SPHERE SYSTEMS

Door-Trol 32

Version 1.461

1 System Overview

1.1   Door-trol32 Access Control System Overview

The Sphere Systems Pty Ltd Door-trol system consists of three main items. The lowest level is the *Doorcom controller*. This is responsible for the actual control of the door or boom. Doorcoms are designed to be located near the door they control. They are mounted by clicking into "snap track". No screws are required for mounting. One Doorcom can control up to 2 doors with up to 16 additional controllable outputs and 16 additional inputs for alarms. Doorcoms are autonomous units containing their own software, real-time clock and battery backup. An inboard battery charger will support a 12-volt DC 7 AH/hr standby battery.
A Doorcom can either be used as a standalone controller or a number of Doorcoms can be connected in a network. A network processor 'DP11' manages the control of the network.
The network controller is connected to a PC. A software package called *Secur32p* running under Microsoft Windows® NT4 – Win95-98 allows the system user to configure the network and to monitor any user, door or point on the network. Access history logging is also implemented through this package.

1.2   Doorcom Controllers DC390

The DC390 controller is the basic unit in the Access system. This board has six universal (analogue or digital) inputs, one door only relay plus an auxiliary door or user definable output. An expansion port on the DC390 allows the addition of additional inputs and outputs. Expansion boards are available for digital inputs and outputs and for tamper proof inputs. Each of these expansion boards has eight inputs or outputs. Up to two of each type of expansion board can be attached to a Doorcom. Thus extra 32 points can increase the initial capacity of the Doorcom. The digital output expansion board has its own on-board relays.) All tamper proof inputs to the access system are 0-10 volts. Two dedicated inputs with RJ45 connectors are designed to handle card reader devices for either entry or exit as a one door controller or 2-entry reader when configured as a two-door controller.

Firmware in the Doorcom controller implements a complex set of control algorithms. Before use, a Doorcom has to be configured. This configuration specifies how the inputs to the Doorcom are to be processed to drive the door outputs. The Doorcom contains a separate lithium battery backed memory, which stores this configuration. Each Doorcom has its own unique serial number. This allows the configuration for that Doorcom to be down loaded from the PC while the Doorcom is connected to a network. The Doorcom control algorithms include standard, switching/windowing on-off functions, logic functions, delay functions and numerous configurable delays and overrides. In addition, a real-time clock and calendar in the Doorcom allow the setting up of time-clocks to control doors. The Doorcom firmware also implements a comprehensive alarm system.   The Doorcom also has the capacity to log all users, digital inputs and outputs internally.
The power supply for the Doorcom is 16 Volt AC transformer
A Doorcom can be used in a stand-alone configuration, where it communicates with a PC using a RS232 interface without the need for a network controller. The Doorcom can also be operated remotely without being connected to a PC. In this case, firmware inside the Doorcom can be set up to automatically dial a Telstra, Link or Hutchinson pager – GSM Phone SMS in the event of an alarm condition.
A number of Doorcoms can also be connected in a single network using the RS485 standard. This allows up to 250 Doorcoms to be networked together. In this case a network DP11 controller is required.

1.3   DP11 Network Controller

This unit connects a network of Doorcom to a PC. The controller operating system is multi-tasking. This unit has built in network diagnostics.

1.4   PC Front-End System

The user interface to the Access system is via a full 32 bit Microsoft Windows® program called *Secur32p*. This program is graphically orientated and can operates in three modes, stand-alone, network and TCP/IP multi-user.   Each of the modes uses a password logon procedure and can be set-up in such a way as to give different operators different access privileges. For example one can limit a user to only being able to monitor doors and users but not change any of the configurations. An in-built diary system allows operators to enter standard messages as reminders for special activities. In addition, network mode allows the configuration of a network of Doorcoms and Liftcoms while the stand-alone mode only a single Doorcom to be controlled. The network mode also requires the use of a DP11 network controller.

TCP/IP mode allows multiple users to access the Doorcom units from multiple PC locations as a Server - Client configuration.

A great deal of attention has been given to making the operation of the Access system as simple as possible for the operator. The front-end software is used to specify a door and user database and to generate the configuration for each Doorcom.

The software allows the user complete control over the Access system. The operator can develop his/her own floor / building drawings and can overlay text, door data, alarms CCTV cameras and input/output points on these drawings. When running on-line, the data will display the actual Doorcom item status and the operator can modify this. Door names can be changed and the operator can incorporate additional points into the system. An operator with the correct privileges an also change the Doorcom configuration and down-load this information to the Doorcom by clicking a single button.

Alarms generated by the Doorcoms(s) are logged automatically to a disk file and are also displayed to the operator.

1.5   Access hardware

DC390 Doorcom	6 (Tamper Proof) inputs, 2 Door outputs, 2 Reader inputs
LC390 Liftcom	1 Lift Shaft up to 64 floors
MC390tamper	8 (Tamper Proof) analogue input expansion module
MC390DI	8 digital input expansion module
MC390DO	8 relay output digital output expansion module
DP11	network processor

1.6   PC requirements

The Frontend software requires the Windows   Win95 NT4 operating system. The **minimum** PC requirements for operation are a Pentium 200 processor with 32 Mb of RAM, TCP/IP network card, sound card and about 1.2 Gbytes of hard disk space.   The minimum system server requirements for satisfactory operation are a 450 Mhz processor with 64 Mbytes of RAM 6 Gb Hard disk, PCI network card with TCP/IP, sound card, PS2 mouse (on motherboard) and a graphics accelerator card.

2 Door-Trol32   System Programming

2.1 General

Programming a Doorcom is unlike programming other Access systems. The programming task does not require any knowledge of a computer programming language. The Doorcom has many control functions built-in. When a Doorcom is programmed the information supplied is used to enable

various internal functions in the Doorcom. The user cannot write "bad code" which will cause the Doorcom to crash.

2.2 Operator System Screens

2.2.1 Operator login

Operators have function permission levels and operator action levels allocated by the system super user.
To log off the system click the System LOGOFF menu items in the logon screen. This will log you off the system but will keep everything else running. No data will be lost whilst you are logged off.

2.2.1 Main screen display
2.2.2.1 Events window
The main screen is mostly taken up the Operator actions and Card accesses windows. You can dynamically change the size of these two windows. Place the cursor somewhere in the operator event window and click the right mouse button. A set of sizing handles will appear around this window. You can now place the cursor over the edge of the window. When its appearance changes to a set of arrows press the left mouse button and while holding the button down drag the window to the desired height and release the mouse button. Note that you cannot shrink either window below one line height. You can further customise the number of events displayed in each of these two windows. Click the System Options menu items and then enter the number of rows for each window. The system will remember the settings you have made and next time you log on the display will revert to the previous settings.

These display windows provide an immediate access to the last few events in the system. You can view all the operator events or select which events to display by clicking the History menu item and then click the Operator history item. You can similarly view card activity using the Access history menu.

2.2.2.2 Status information
Below the event window are 2 panels, one showing where there are any current alarms. The other panel is only displayed in the standalone mode and it shows the door currently being addressed. Note that in the standalone mode of operation you MUST select a door otherwise the system will not communicate. The system will remember the last door you made active and this door will be set as the active door when you reload the program.

2.2.2.3 Status bar
The status bar is located at the bottom of the main screen. It remains visible even when other forms are displayed. It consists of 4 fields. The left-hand field displays status information and is also used to display the most recent alarm in the system. This field changes colour when an alarm is detected. The colour of the text and the background indicates the alarm priority.

The second field displays an icon when an alarm is generated as a result of an operator action. The current alarms, which can occur, are a Trace alarm and a Diary alarm. In the case of a trace alarm a letter A is displayed while for a diary alarm a letter D is displayed.

The third field displays the communication mode currently being used. If this field is blank or says Offline then no communication is possible with the doors in the field. This field changes colour depending on the communication system status. In tcp/ip networks this field also is used to display the status of any remote tcp/ip connections. Place the mouse-pointer over the field and press a button to display a list of the IP addresses of connected clients. The list remains while the mouse-button is held down.

The right hand field displays the current PC time.

2.3.2.2 Standalone operation

In standalone operation, you can only communicate with the currently active door. You set this door by clicking on the Doors Modify menu items. The name of the currently active door is displayed below the Events window.

Operator Actions and Card Access Screen

This screen can be configured to display only one door or the whole system.

When in single door mode the cardholder's photo can be displayed when the card is presented at the reader for positive identification. This screen is the default system entry screen.

2.3 System Menu Commands

2.3.1 Main Operator Menu Map

System

    Super User

        Set as Client

        Clients

            Add clients

            Delete Clients

        Operators

        Doors

        Lifts

        Users

            Assign Users to Tenancies

            Assign All

            User Count

        Reports

            User Details

            Occupants

            Expired Cards

            Access

        Modify

    Operators

    Permissions

    Pager System

        Configure Pager

        Set pager scheduling

        Page a Person

    Diagnostics

        Network Test

        Door Status

    Diary

    Weekly Schedules

    Sticky Memo

    Register

    Options

        Setup

        Drawings

        Identification

        Debugging

        Misc

    About

    LOGOFF

Exit

Comms
Communications
On-line
Remote
Remote Dial-out
Firecom
Set Timeouts
Configure All Doors

Users
User Maintenance
Current Users
Lost & Stolen Cards
Deleted Cards
Card Usage
Import Users
Read Card Details

Doors
Modify
Groups
Status
Group Control
Multilevel Passback
Access Maintenance
User Numbers
Failed Updates & DB Fixes
Configure DP11
Networking

Lifts

Time
Time Schedules
Set PC Time
Public Holidays
Door Times

Inputs
Configure Inputs
Input Status

Outputs
Configure Outputs
Output Status

Drawings

History
Access History
Operator History
Digital In History

Alarms
Current
Ademco

Configure Dialler
Print Alarm List
Define Guard Actions
CCTV Locations
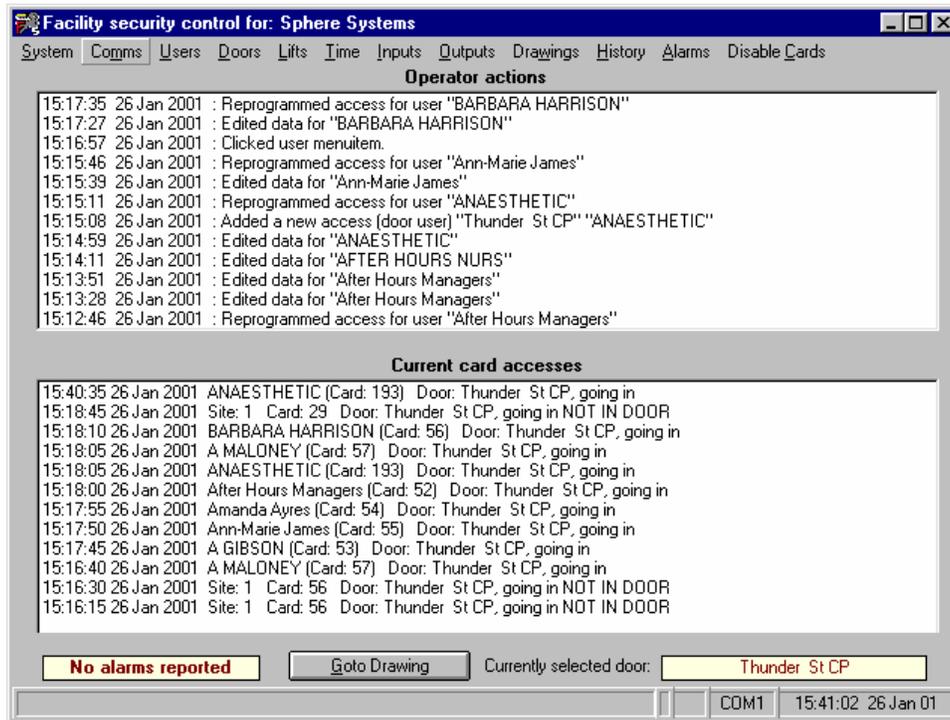
2.3.2 System

2.3.3 Super user
Allows you to configure what is visible to an operator.

NOTE: To change a client configuration you must have global access privilege.
This form allows you to configure what areas an operator can see. The only predefined client is Global and you select this client by clicking the entry in the client list. You cannot delete the global client. To add a new client types in the name of the client in the Name textbox and then click the Add button (or Clients/ Add clients menu item).

You can assign a password for a NEW client by typing the password into the Password box. Passwords must be less than 20 characters and can consist of any mix of alphanumeric (A-z) or numeric characters. You cannot assign a password to an existing client, you must delete the client first and then re-enter it. Once a client has been assigned a password you will not be able to set the global user to appear as that client without supplying the password. Also, you cannot alter a door, operator or a lift floor belonging to that client without supplying the password. You can, however, add new doors, etc to that client without needing the password. Do not forget the client passwords, as they cannot be recovered from the system!

To delete a client, click the name in the table and then click the Delete button. Deleting a client will delete all operators and diary entries for that client and will re-assign all doors, points on doors, and cardholders from that client to the Global client. The history and events for that client will still remain in the database but are not recoverable by the system. To recover this data will require you contacting Sphere Systems Pty Ltd.

Initially any new door, lift or operator inherits the client status of its creator. For example, if you belong to client "ABCD" and you create a new door, then that door also belongs to client "ABCD".

The client status of a door belongs to the door and ignores any groups a door might belong to. If a door belongs to more than one group then that door will have the same client status in both groups. You can have a group where each door belongs to a different client.

To assign doors or lifts to clients click the desired menu item. If you clicked the Door menu you will display a list of all doors in the system. If you clicked the Lifts menu you will get a list of lifts plus a floor list. Click a lift entry to display the list of floors for that lift. To assign a given door or floor as a particular client, click the desired door (or floor) and then click the client who should own this object. Click the Change client button to assign the object to the desired client.

Follow a similar procedure to assign an operator to a client.

You can change the client you are by clicking the desired client in the list of clients and then clicking the Set as client menu item. This is useful in checking what a client can see. Note that the global client (ie the owner) can see everything that exists in the system (provided the operator has access to client passwords (if used). To see doors belonging to a client other than the global client you must set yourself up as the correct client.

When a client wishes to set an access to a door he can choose between any door belonging to him OR any door belonging to the global client. Thus, the front door could be a global access and hence available to all clients while all other doors belong to their clients. A client cannot access the parameters for a door not belonging to him.

The control program implements a multi-tier security access control strategy. You can break a system up into a number of discrete sub-systems and assign these sub-units to different clients. An operator assigned to one group of doors and users will not be able to see anything about another set of doors or users belonging to other clients. This allows the building owner to set up a group of tenancies where each tenant has complete control of their own area but knows nothing of other tenants. There are some global parameters which all tenants (clients) share. All time schedules, public holidays and lifts are global. Doors can also be included as globally accessible. Lift floors can be global or can be assigned to clients. Global parameters can only be changed by the building owner (ie the Global operator). The visibility of different ares is controlled by assigning areas to clients
.

Every operator, door, door group, input, output, variable, logic function, delay function alarm and card has a permission level assigned to it. Any operator has access to any door, input, output or alarm etc where his or her permission level is equal to or higher than the permission level of the object. (Note that a door group can be given a permission level different from the permission levels of the individual doors in a group.) Permission levels start at the highest level (Administrator) and number 8 in total. You assign permission levels using the permission's form. You can further restrict what actions an operator can take by controlling what an operator can or cannot do.

Using permission levels on cards you can control what cards a particular operator can access. Thus it is possible to allow an operator to enter new cards into the system but not change any details on existing cards. The operator is not able to view the details of cards having a higher permission level than his/hers. Nor can the operator view or change the access of any cards having a higher permission level than his. Further, an operator cannot assign or change the access to ANY doors or door groups having a permission level higher than his. In general any operator can add new doors etc and assign any permission level to these objects BUT if the assigned permission level is greater than that of the operator, then he/she will not be able to make changes to the object (including deleting it).

You can view this security access scheme as the client controlling what an operator can see, the operator access controls what functions an individual operator can do and the permission's level determines on what objects the operator can do the actions on and what actions are permitted.

There is a second level of security available and that concerns how the Global client can access other clients. Each client can be given a password by the Global client, when creating the client, and unless

the Global client has access to this password he will not be able to set himself up as that client and consequently he will not be able to access any users, doors etc belonging to that client. Furthermore, although he can see what operators, doors and lift floors belong to the client he cannot change their ownership. He can, however, add new operators and doors to the client.

2.3.4 Operators
Allows you to determine who can use the program.
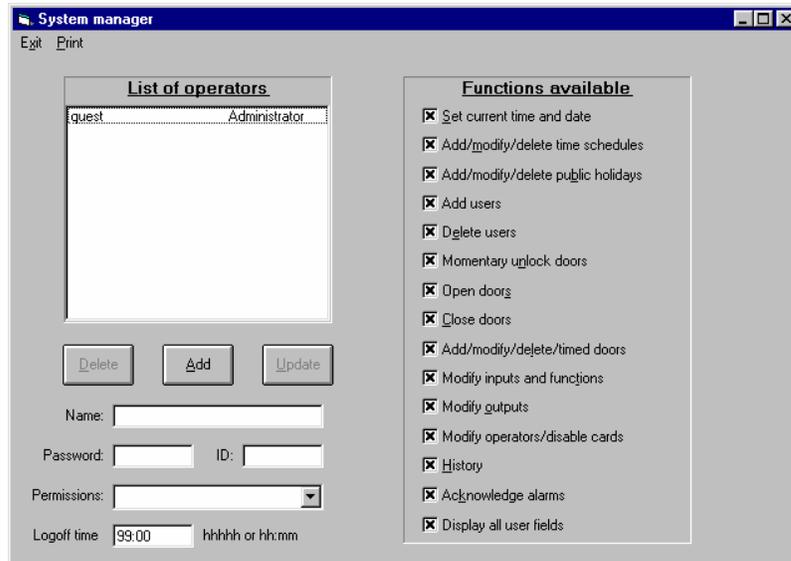
The operator maintenance is accessed from the System menu by clicking the System menu item and then clicking the Operators menu item
To see the details for an existing operator
Click on the desired operator in the displayed list of operators.
You can change the name of an operator or their password by typing in the new data and then click the Update button. Any attempt to enter or modify the data in the ID field will cause the Update button to become greyed out. You can only Add this as a new operator and then delete the old operator.

2.3.4.1 Adding a new operator
Enter the data for the operator in the Name, Password and ID fields and then select which areas of the program the operator can access by clicking on the appropriate checkboxes in the Functions available panel. Click the Add button to save the new data.

2.3.4.2 Deleting an operator
Select the operator in the List of operators panel and then click the Delete button.

2.3.4.3 Changing the allowed access for an operator

Select the operator by clicking the entry in the List of operators panel. Check the desired checkboxes in the Functions available panel and then click the Update button.

2.3.5 Permissions
Allows you to determine what an operator can do.
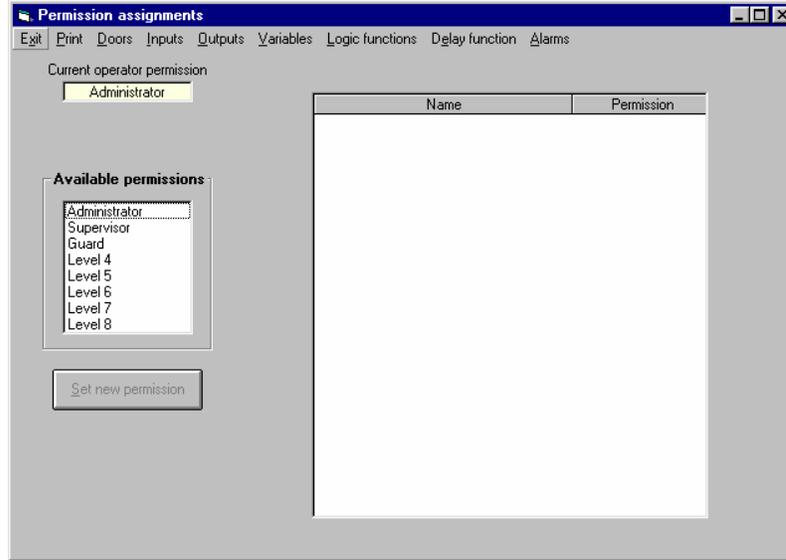
To change the permission level of an object (a door, input, output, logic function, delay, variable or an alarm) click the System Permissions menu items in the main screen. This brings up the Permissions form. The form displays the current operator permission level. This operator can change the permission level of any object whose current permission level is less than or equal to his/her level. The new permission level can be made higher than the operator's current level but once this form is exited the operator will not be able to change the level again!

To change the permission level first bring up the table of objects of the desired type by clicking the desired menu item. Then click the desired object and click the desired permission level and click the Set new permission button.

2.3.6 Pager System

2.3.6.1 Configure Pager
Configure the pager - Sets the modem parameters, phone number and paging details
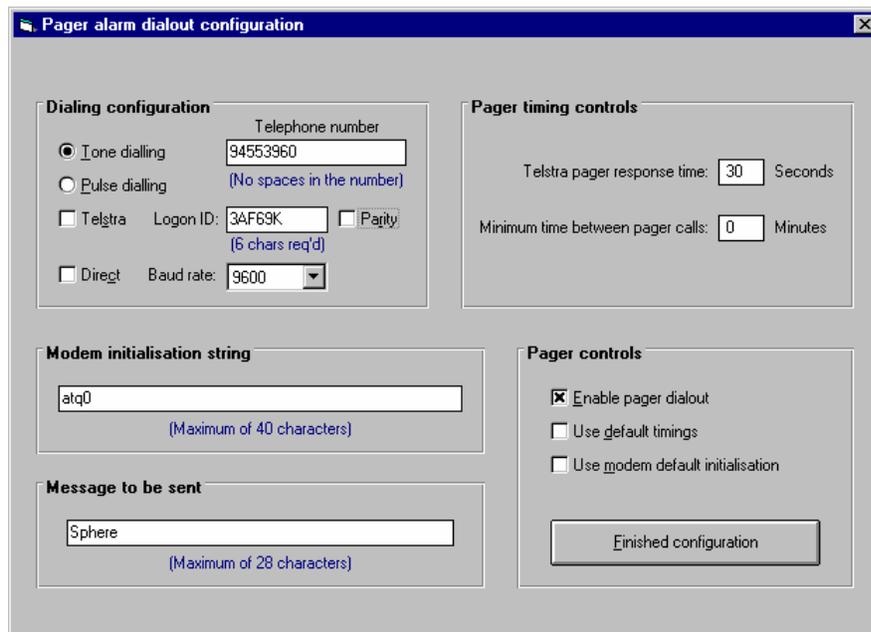
2.3.6.2 Set pager scheduling
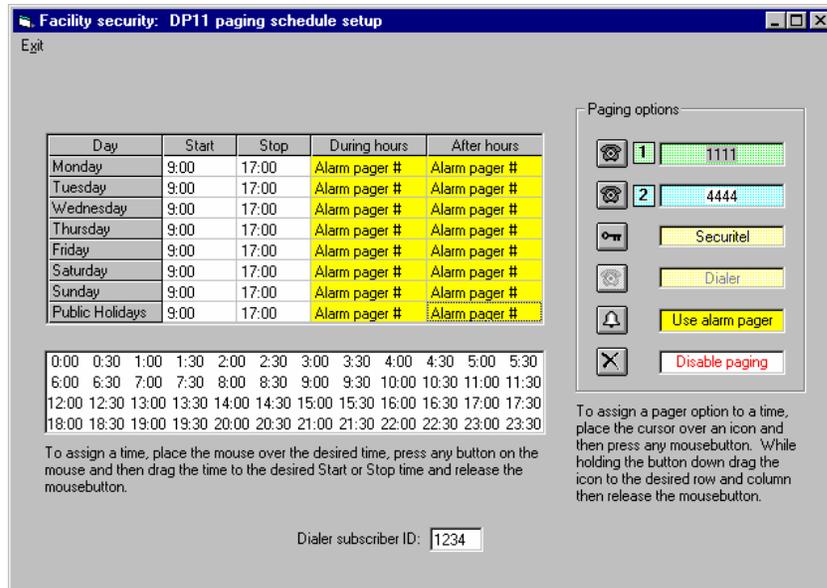
If you are using the paging method of alarm notification, then you have the option of switching the pager number from that assigned to an alarm to either one of two other pager numbers or using Securitel dialouts. You can also disable paging altogether. The control of which pager number to use or disabling paging can be configured separately for each day of the week and for public holidays and you can have 2 different paging options/day. The available paging option for each period can be selected from:

Pager number assigned to each alarm
> Pager number 1
> Pager number 2
> Securitel dialout
> Paging disabled

For example, this system allows you to disable paging during working hours and to alternate between 2 pager numbers on alternate days during non working hours. You could also set the system to use the pager number for each alarm during working hours and to use Securitel dialing after hours.

2.3.7 Diagnostics

2.3.7.1 Network test
Displays the current network state. Also allows diagnostic network testing.

2.3.7.2 Door Status
Displays the current status of all doors. Inputs together with door and d8 status.

2.3.8 Diary

Allows the generation of a Diary message
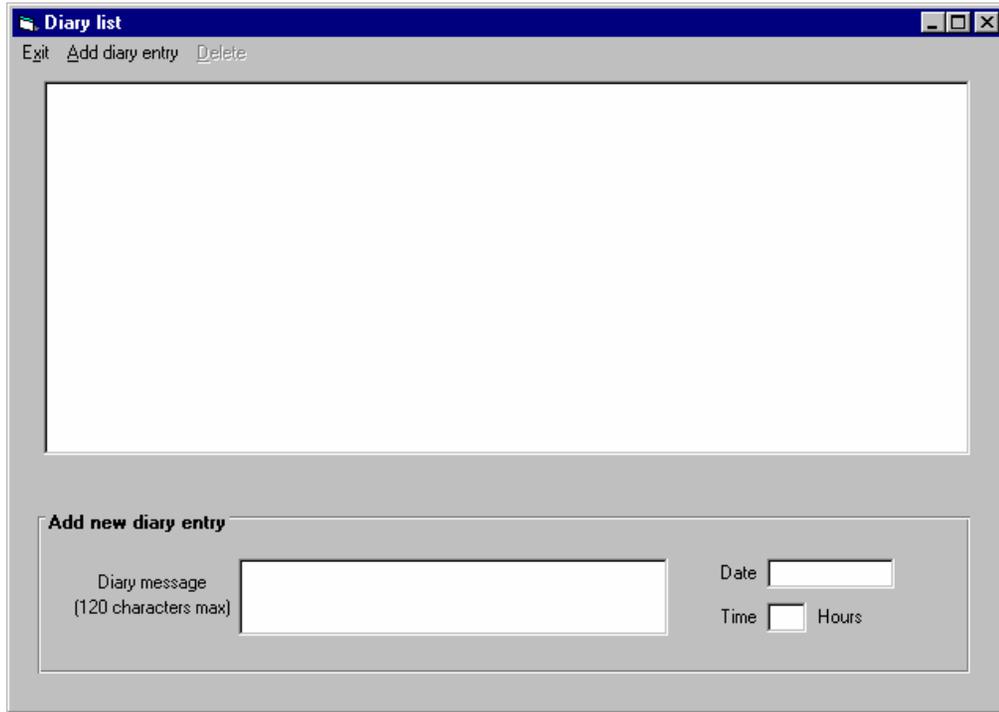
The control program allows you to store messages in a diary. Together with each message you specify a date and time for the message. Once per hour the system will check the diary and if there is a diary entry for that time the system alarm panel (the second item from the left in the main status bar) will show a D and emit a beep. (Note that the system alarm panel is shared with trace alarms so if a trace alarm is present the D might not be displayed). Clicking the panel when the alarm indicator is displayed will bring up the diary form displaying the current diary message(s). You can delete a message by clicking the message and then clicking the Delete menu item.

You set a diary entry by clicking the System Diary menus. The form which appears lists the diary entries. You can delete an entry by clicking on the entry and then clicking the Delete menu. To add a new entry type the message and the date and hour (24 hour clock) for the message and click the Add diary entry menu.

2.3.9 Weekly schedule

Weekly calendar which can also generate alarms

The weekly schedule system allows you to generate messages at preset times during a week. These messages, which can also generate alarms, repeat on a regular weekly basis until deleted. To add or modify the messages click on the System, Weekly schedule menu items in the main screen. This brings up the weekly schedule form.

The weekly schedule form consists of a window with a grid displayed. The top row of the grid is fixed and displays the day of the week. The left hand column displays the times for which you can generate a message. You can alter this time by clicking the Interval menu item and then selecting one of choices listed. Changing the interval will delete all diary entries. You can change the top row displayed by clicking the Top row menu item and then entering a time for the top row. The time can be entered in a number of ways (eg. 12:34, 2 am, 3 pm etc). You can still access earlier times using the vertical scroll bar. You can vary the column and row widths and heights by placing the mouse cursor over the divider line between rows or columns, press the left mouse button and drag the field to the desired position. Then release the mouse button.

If an alarm is set for a particular time then an icon of a bell will be displayed in the grid. When a message generates an alarm the To enter a message you click on the cell where you want to add a message or you can use drag and drop to select a range of cells. Selected cells will change colour. Enter the message to be displayed in the text box in the window below the grid. Check the Set alarm checkbox if you want this message to generate an alarm and then click the Enter button.

If you click on en entry in the table the message will be displayed in the message window.

An alternative way to add messages is to type the message into the message window and then click the Copy button. The legend for this button will change to Paste. You can now click the mouse over any cell where you wish to add this message. If the Set alarm checkbox is checked the message will generate an alarm. Clicking the Paste button will change it back to a Copy button.

System status panel will display a W. Click on this part of the status to display a list of system alarms. You can display the full alarm message by clicking on an entry in this list.

The Clear button is used to clear the message window and thus can be used to clear schedule entries.

2.3.10 Register
Allows you to register this program
The licence is PC specific and registration is required for each PC running the Facility Access control software.

2.3.11 Options
2.3.11.1 Setup
Allows you to configure the way the program operates.
System -> Options -> Setup
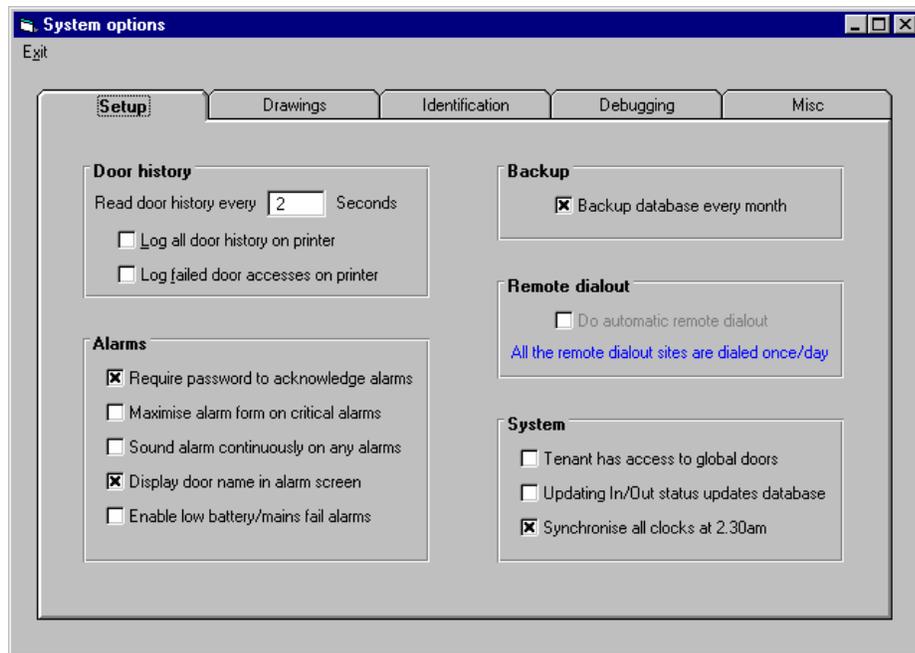
2.3.11.2 Workstation Drawings Setup
Dynamic Drawing Options per Work-station

System -> Options -> Drawings
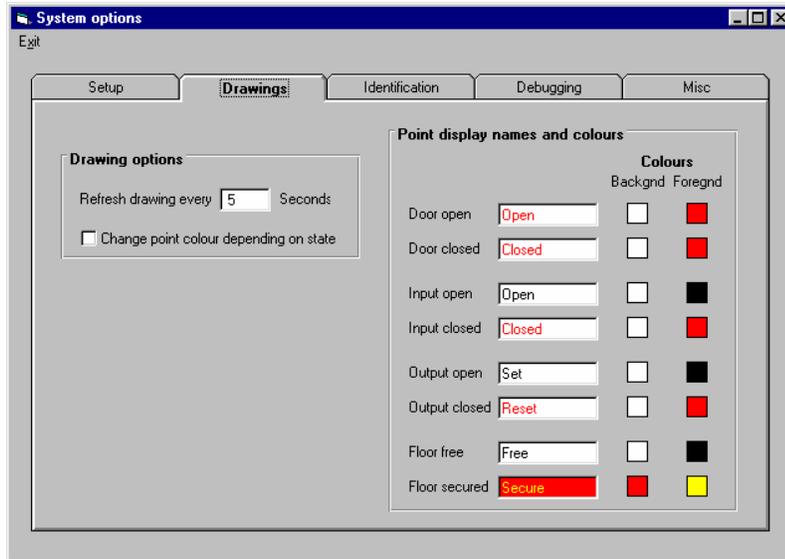
2.3.11.3 Site Identification
System -> Options -> Identification
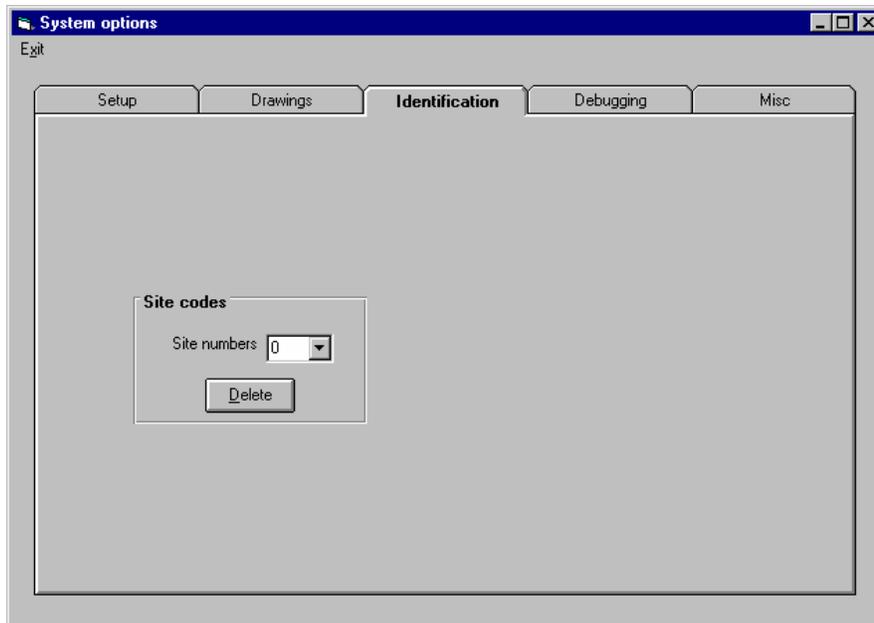
2.3.11.4 Misc
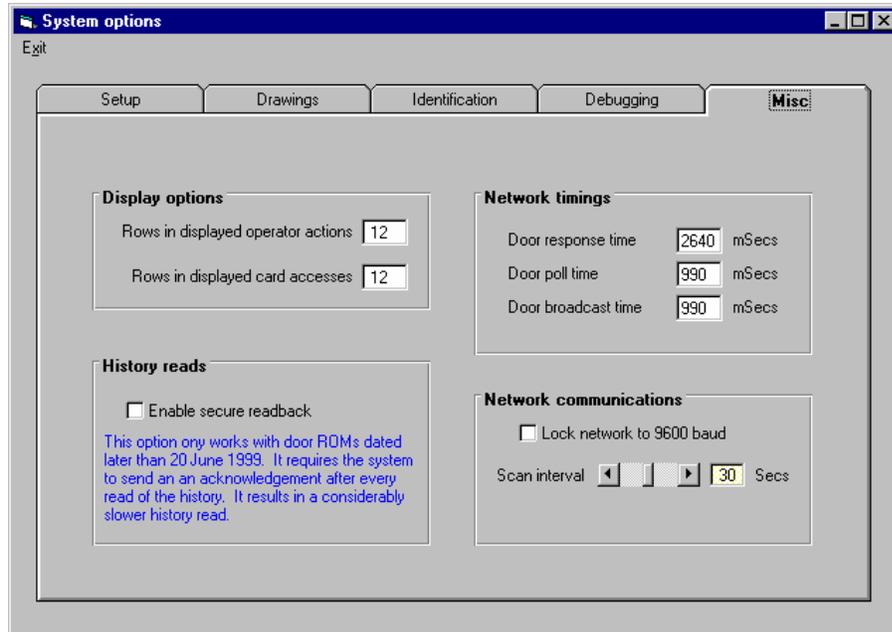
System -> Options -> Misc

2.3.12 About

System information display

2.3.13 LOGOFF

Logs you off the system without closing the system down.

3 Comms Menu Item

3.1 Communications

Allows you to set up how the system communicates to the doors
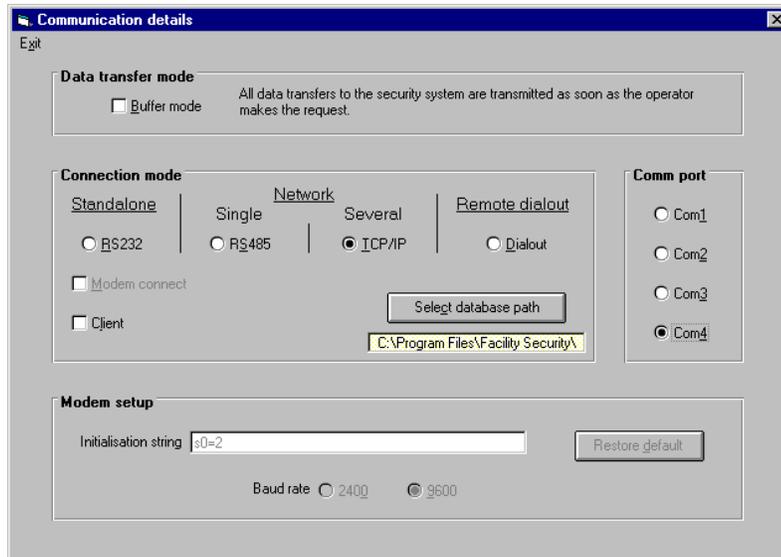
This function controls how the frontend program will communicate to the doors in the field. You configure the communications by clicking on the Comms menu item and then clicking the Communications item. This brings up the Communication details form. Note that you MUST be Offline to be able to change communications settings. To switch the system offline, click the System menu and if the On line entry is ticked click it. You can now click the System Communications menu items.

There are numerous ways in which you can configure the communications and these are discussed below in more detail. The program allows multiple PC's to access a single Doorcom or a network of doorcoms. The PC or program controlling the whole system is called the Server, all other PC's accessing the network are called Clients. The current release of the software only allows a single server but unlimited clients. You MUST have a server you CAN have clients.

You must set the communications up for both clients and the server. For a Server you must tell it how it should communicate to the doorcom(s). You also have to list the clients which can attach to this system and what information they should receive. Clients only require you to specify how the server will talk to the doorcoms. (The clients talk to the doorcoms via the server). You must also set a PC as a server or a client. This is done by checking or un-checking the TCP/IP connect checkbox. Leaving it unchecked forces the program to be a server, checking it causes the program to be a client.

3.1.1 Setting the communications to the doorcom network.

There are 3 basic ways in which you can configure the communications system: The simplest method is just a single doorcom attached toa PC. This is known as the Standalone mode. If you have more than one doorcom in a network, then you need to use a DP11 network processor to handle the communications between the PC running the network and the doorcoms. This is the Single network mode. You can also have multiple single networks each connected to a different PC. This requires a local server program on each PC connected to a network of doorcoms. The entire network is controlled by a single PC designated as the network server. This is the Several networks mode.

 Note that you MUST configure both the server and the clients with the same type of connection mode. The only difference between the server and a client is that the client has the TCP/IP connect checkbox checked whereas the server does not.

3.1.2 Standalone mode

Uses RS232 communications directly to a single Doorcom controller. You can use this mode to communicate with a single door even if the door is part of a network. You must, however, configure the door controller for RS232 mode. You can also use this mode to configure a number of standalone doors sharing a common database. You select the door to control by clicking the Doors Modify menu items and then clicking on the desired door in the table. The currently selected door is displayed towards the bottom of the main screen.

3.1.3 Single network..

Uses RS485 communications to communicate between several Doorcom controllers. This requires a DP11 network controller connected to a PC via RS232 communications. The Doorcom controllers talk to the DP11 controller via RS485 communications.

Several networks uses TCP/IP communications between PC's. Each PC can have a DP11 network controller connected to it. Each PC can communicate with any door in the system and all PC's can share a common database. For each PC connected to a DP11 processor, you need to run a copy of the Sphere Systems Facility Server program. This runs as a background task on a PC running Windows 3.11 or higher and acts as a local server for the network connected to that PC. It accepts information packets from the network server and handles the communications between the PC and the doorcom network connected to it. This mode of operation still requires you to nominate a single PC as the network server but this can be any PC in the network and it need not even have a doorcom network attached to it. Note that the Facility server program (facserve.exe) runs as a background task but because of the way Windows works on PC's it is not advisable to run any other software on a machine running this program other than the programs supplied by Sphere Systems as part of the building management/access control systems as other programs can hog the PC and not allow communications to occur.

Note that the several networks mode uses Windows networking to access remote databases (ie a database not located on your machine). This relies on attaching a directory (folder) on another machine to your machine. This is not supported by networks such as the Internet which means that you must have local copies of all databases and files that the program requires if you wish to connect over a non-Windows type of network.

For both Standalone and single network modes you must tell the program which serial port it should use to communicate with the doorcoms. You select the port by selecting one of the options in the Comm port panel. Clients do not require this selection and it will be ignored.

You can also use a modem to isolate the Server PC from a single Doorcom controller or a network of controllers. In this way the PC can be located remotely from the doors, however you cannot use a modem to communicate with several networks of doors; They must all be interconnected by a TCP/IP network.

You select the mode of operation for the server by selecting one of the options in the Connection mode panel. You can select the modem connection mode by checking the Modem connect checkbox. For a server you MUST leave TCP/IP connect checkbox unchecked. Checking this box forces the program to be a client.

3.1.4 Database selection

The Server expects to find all the database and configuration files in the directory (or folder) where the program is stored. Clients have the option of using a database and associated files from any directory or folder on the local machine or from any other machine on the network. As a client you MUST select a path for the system database. To select the desired path click the Select database path button and choose the desired database from the popup dialogue box. The selected path will be displayed in the panel below the button.

In addition, you can set the system to work in a normal or a buffered mode of operation depending on the Data transfer mode you select.

3.1.5 Data transfer mode

The Data transfer mode allows you to determine whether communications with doors are made in realtime (Buffer mode unchecked) or delayed. If you check Buffer mode, the program will behave as if it is online even if it is not connected to the field. All operator actions which send commands to the doors in the field will have those commands saved by the program. When you do eventually switch the program online, the program will immediately send all buffered commands to the field, in the order in which they were initiated, and will then read back all the history for each of the doors in the field. If you have selected the buffered mode of operation the word buffer will appear in the status bar while running offline.

The connection details for buffered and un-buffered communications are identical for RS232 and single network systems. Buffered communications are not possible for TCP/IP networks. For multiple networks the TCP/IP mode becomes a Multiple DP's mode and it uses modem access to connect you to a single network at a time. You can specify a different telephone number for each network. The building you assigned to each door determines which network a door is connected to. Click the Configure button to display the Building telephone number setup form. This form displays each DP processor and the corresponding building name and telephone number. You add or edit the telephone number by clicking on an entry in the table, typing in the telephone number and then clicking the Update button. You can choose a DP number as well. This has to be a number between 1 and 250. If you assign the same DP numbers to different buildings then the system will automatically assign the same telephone number to each building. What you have done is to allow the use of the building field to specify separate groups on the one DP processor.

3.1.6 Modem setup

This panel allows you to configure the modem for correct operation. You can either connect at 2400 or 9600 baud depending on which option you click. You can set the initialisation string the modem uses for communications in this panel. The default string should work for most Hayes compatible modems.

3.2 On line

Connects/disconnects the PC from the door network

3.3 Remote .

Only applicable if this is a server system. Allows configuration of remote logons
Note that this section only applies to the PC acting as the system server.
The remote PC setup is used to enable remote computers to gain access to the doorcom network. You configure remote PC's for logon by clicking the System Remote menu items to bring up the Remote access setup screen. Note: you must be the network server to be able to configure remote access logons. This screen displays a table listing the remote computers (by name) which are authorised to gain access to the server, their connected status and what information will be passed to them.

To enter a new computer start by clicking the Add menu item. You then enter the name of the remote computer and its IP address in dot notation.

You now have to select what information should be sent to the remote PC. Check the appropriate box to display the information, keep it clear to disable updating on the remote PC. Click the Save button to add this PC to the remote PC list.

You can delete a PC from the list by clicking on the entry and then clicking the Delete menu item.

You can edit an entry by clicking the entry, making any changes that you want and then click the Update button.

The Connect column indicates the current status of each remote PC in the list. You can disconnect a remote client by clicking the appropriate entry in the table and then clicking the Disconnect menu item. Disconnecting a client is only a temporary step as the remote client can reconnect and there is nothing you can do to stop this other than removing the client from the table.

Note that the remote access logon procedure will check any new connection from a remote client against the information in this table and will also verify the remote user's logon id and password before allowing a connection to be made. If any of this information is invalid the remote termination will be terminated.

If there is a remote client connected to the server then the communication mode field in the system status bar will change from a grey to a green background.

4 Users

User maintenance - Allows adding, modifying and deleting cards to the system
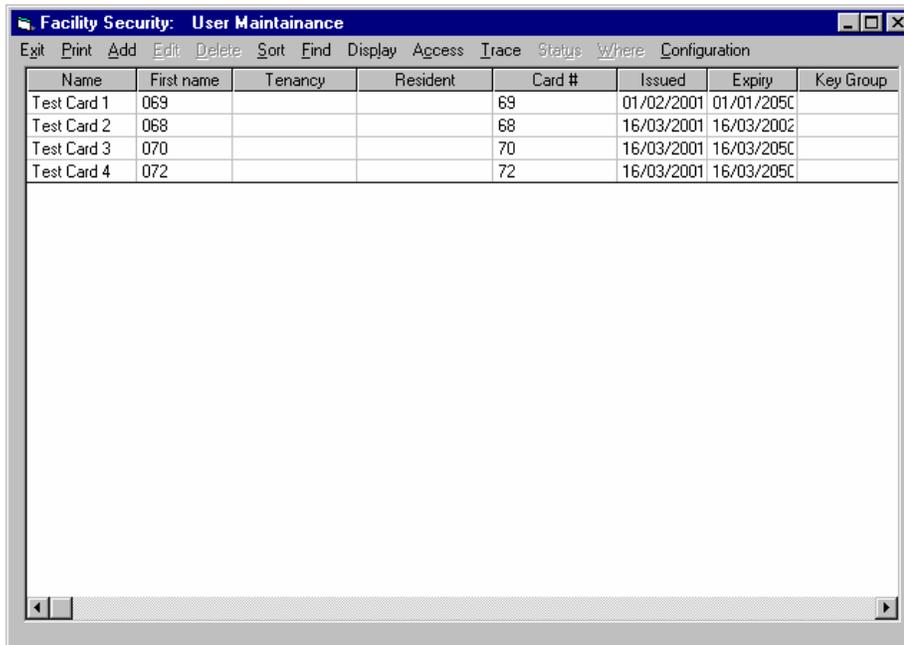
Name	First name	Tenancy	Resident	Card #	Issued	Expiry	Key Group
Test Card 1	069			69	01/02/2001	01/01/2050	
Test Card 2	068			68	16/03/2001	16/03/2002	
Test Card 3	070			70	16/03/2001	16/03/2050	
Test Card 4	072			72	16/03/2001	16/03/2050	

4.1 User maintenance

4.1.1 To add a new user
Click the Add menu item to bring up the User data entry form.

```
Facility Security:  User data entry                          [_][□][X]
Exit  Photo  Stolen card  Lost card
┌─ Personal details ──────────────────────┐  ┌─ Card access details ──────────────────┐
         Name  [Test Card 1           ] *           □ Button/Barcode/ Prox36
    First name  [069               ] *              Card #  [69          ] *
      Tenancy  [                 ] *                 Issued  [01/02/2001 ] *
      Resident  [            ▼] *─[Update]           Expiry  [01/01/2050 ] *
       Mr/Mrs  [    ]   PIN number  [      ]     Site number:  [1       ▼]
    Key Group  [          ] *  User □          Zone access:  [Zone 1   ▼]
     Car reg 1  [      ]   Car reg 2  [      ]     □ First use      □ Long access
      Phone #  [               ]
     Join Year  [              ]─[Update]       ┌──────────┐   [  Add new  ]
      Address  [               ]               │          │
       Suburb  [               ]               │          │   [  Status   ]
   Next of kin  [               ]               │          │
       User 1  [               ]               │          │   [  Cancel   ]
       User 2  [          ] [Memo]              └──────────┘
    User text  [                  ]               Permission       [  Update   ]
                                                 [Level 8   ▼]
```

4.1.2 To edit the data for an existing user

Click the desired entry in the table and then click the Edit menu item to bring up the User data entry form. You can also achieve the same result by double clicking a user. NOTE that if your permission level is less than that of the card user you will not be able to edit or view the cardholder's details.

4.1.3 To delete an existing user

Click the desired entry in the table and then click the Delete menu item. You cannot delete a cardholder whose permission level is greater than yours.

4.1.4 Sorting the display

Clicking the Sort menu item gives you a choice of fields on which to sort the display list. Click on the desired entry to redisplay the table sorted by this field. You can also sort the display by clicking the various column headers.

4.1.5 Finding a table entry

Clicking the Find menu item gives a choice of fields in which you can look for a text string. Click on of the entries and a dialogue box will appear. Type the text to be looked for into this box and click OK to do the search or click Cancel to abort the search. Note that the search will only find an entry starting with the text string you have entered. You cannot find a string embedded in the middle of an entry.

4.1.6 Creating a subset of the users

This menu item allows you to display a subset of the users. Clicking the Select
menu item brings up the Field selection criteria form. You type the text string or data into this field of a table entry. An asterisk in an entry means include all data from this field. You do not need to type the full name in a field. An asterisk placed before a text string will include all data where the text string is at the end of an entry. An asterisk placed at the end of a string will include all data where the text string starts the entry. An asterisk placed at both the start and the end of a text string will find all entries including the string anywhere within the entry.

For example:
Abc   - will only include entries whose full text is Abc
*abc   - will include all entries ending in abc
abc*   - will include all entries starting with abc
abc - will include all entries having the string abc anywhere within the entry
*   - will include all entries in the list

Using this form you can find any desired subset of entries very easily. Click OK
to do the search or click Cancel to abort the search.

Clicking the menu item will display the complete list of table entries and will reset all the selection fields to a *.

Changing the status of a cardholder
Click the desired user in the list and then click the Status menu item.

4.1.7 Setting the accesses for a cardholder
Click the Set Access button in the User data entry form or select the user in the list and then click the Access menu item. This will display the Access assignments form. You cannot assign an access (or view the accesses) for a cardholder whose permission level is greater than yours.

4.2 Current users

Displays the list of current occupants.

4.3 Lost & Stolen Cards

Displays the list of lost and stolen cards..

4.4 Deleted Cards

Displays the list of deleted cards..

4.5 Card Usage

4.6 Importing data

You can import a list of users, card numbers and other details from a data file or an Excel spreadsheet. The data file format consists of one line of data per user with commas delimiting the data in each line. To generate the data file using Excel you must save the Excel spreadsheet as a *.csv file with no column or row headings. The data fields imported must be in the following order:

First name, Surname, Card number, Site number, Department, Manager, Address, Suburb

Only the first 2 fields are required. If you do not want to put data in a field the field must still exist. For example, to omit card and site numbers the entry for a line should look like:

Firstname, Surname,,,Department,Manager,Address, Suburb

If you do not want to include fields at the end of the line (eg the Suburb field then just leave it and the comma before it out. For example:

Firstname,Surname,,,Department

This will import just those 3 fields.

4.7 Read Card Details
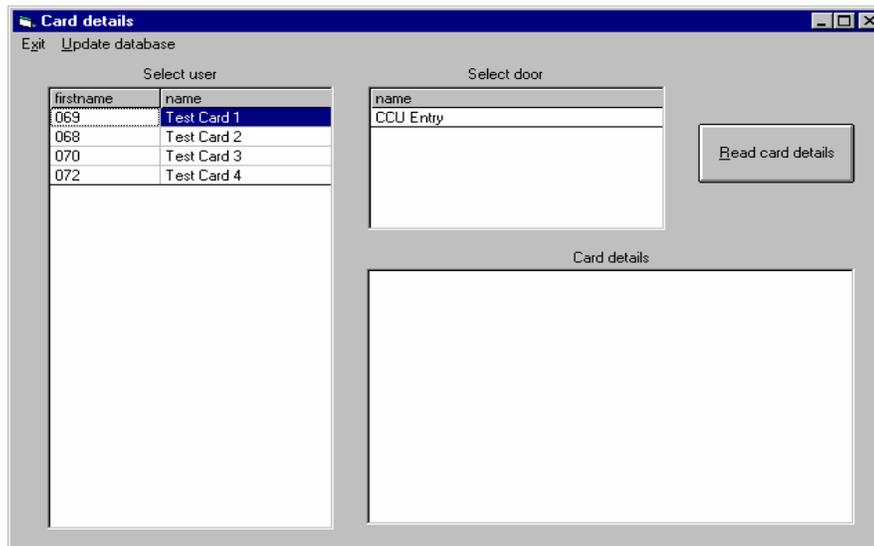
5 Doors

5.1 Modify - Add

Allows you to define new doors or change existing door details

5.1.1 Configuring a door parameters

To define a new door, click the Doors menu item in the main screen and then click the Modify menu

item. This will bring up a form labelled: Facility Security: Door/reader definitions. You can change the name of the Building, Floor and Room fields by clicking on the name.

You select a door to configure by clicking on an entry in the displayed list. For stand-alone operation this determines which door is currently set to be active. All communications to other doors will be inhibited. Thus you can use a single database to store information about a number of doors and still only configure one door at a time in the stand-alone mode of operation.

Readers are assigned to doors. Each door can have one or two readers assigned to it. If two readers are assigned to a door then the door is set for anti-passback operation or for exit reader operation or for dual-door operation. You assign a mode to a door by selecting the desired option in the Exit type listbox. You can also select how the door is to be opened from the non-reader side in a single reader system. If you select the Dig In 6 option in the Exit type listbox then activating I6 on the door controller will operate the lock. This allows you to use a pushbutton on the inside to open the door. Note that DI6 can also be controlled by a timeclock. If you select the None option then there is no provision made for opening the lock other than by the reader. If the None option is selected then the form will display the total number of accesses made through this reader. If any other option is chosen then the total number of people remaining inside the controlled door is displayed. You can reset this number to zero using the Functions, Set room unoccupied menu item.

You specify how long the door should remain open by entering this time in the Open time field. Each door has the capability of being opened for an extended time to allow wheelchair access etc. You can specify this extended time by clicking the Configure button and entering the desired extended time in the Extended open time panel. The activation of the extended opening is controlled by the cards used to activate the door.

There are several advanced options available:

You have the option of qualifying a card access with a digital input, variable or output before a door will open. This option is used, for example, in carpark control where a loop under the car must detect a car otherwise the gate will not open.
> The Exit reader operation can also be qualified with a digital input, variable or output.
> You can also change the operation of the Exit reader so that it controls D8 rather than DR. This option is useful in cases where there are separate entry and exit gates, each with their own reader. When activated, D8 will open for the same time as the Door. You can manually control the D8 relay, or control it using a timeclock, as it still behaves in all other respects as a normal digital output.

Dual authority requires 2 card accesses within a certain time to allow the door to open. To set dual authority you must check the Dual authority check box and also set the maximum time allowed between the 2 cards being detected.
> PIN codes allow you add further security when using Wiegand type cards.

You access these options by clicking the Configure button to bring up the Door status/relay configure form. Check the desired checkboxes and options. Note that unless you have enabled Passback you will not be able to change the Exit reader configuration. Note that you cannot change the assignment of which input is used with which reader.

NOTE: After you have defined a new door you must click the Update button to save the configuration. This also makes entries for the points (inputs, outputs etc) belonging to that door in the database. Until you have saved the door there will be no inputs available for that door.

You can also use any digital input to operate the lock by linking the digital input to the DO8 output relay and then parallelling the Door and DO8 relays. Note that you cannot use any relays other than those on the main controller board as these relays actually switch 12 volts. All other relays have voltage-free contacts!

A door/reader is assigned to a 3 level index system comprised of the building, floor and room fields. The contents of these 3 fields is up to the user to define. The floor and room fields are only used by the system to make it easier for the user to find a particular door. The Building field is used in much the same way, however this field also allows you have networks of doors in different areas or even different buildings. Using the TCP/IP communication mode these buildings can be at remote sites on the other side of the world if you so desire.

For simple systems, you can leave the floor and room fields blank however you MUST enter a building and name for each door.

For each door in the network you have the option of specifying what type of access control is used. This can be Wiegand or proximity cards or buttons. The type of access you select is determined by the communications protocol of the reader attached to the door controller. The Wiegand item is the normal communications protocol for both 26 bit Wiegand and proximity readers. To select the type of access required click on the down arrow and then select the desired entry in the displayed list by clicking it. The Prox36 selection allows you to read 36 bit proximity cards. The Proximity selection uses standard 37 bit proximity cards.

Each door has as standard 6 inputs and one output associated with it. This can be expanded by an additional 16 inputs and outputs. If you have additional inputs and outputs you have to let the program know how the door is configured. After clicking a table entry click the Configure button to bring up the Door status/relay configuration form. Select the appropriate input and output configurations and click the Save configuration button.

5.1.2 Door/reader details

5.1.2.1 Adding a new door/reader
Click the Add button and then fill out the various fields. You can always come back and edit fields later if you do not know what to enter into all the fields. Then click the Update button to save the data.

5.1.2.2 Deleting an existing door/reader
Click the entry in the table and then click the Delete menu item. Note that deleting a door will delete all user accesses to that door as well.

5.1.2.3 Sorting the displayed list
You can sort the displayed list in several ways. Click the Sort menu item and then click one of the displayed items to perform the sort.

5.1.2.4 Finding an existing door/reader
You can find a particular door by clicking the Find name menu item and then entering the full name for the door and clicking the OK button. You cannot seek for part of a name.

5.1.2.5 Programming a door
This menu item is only enabled after you click on a table entry and the system is switched to on-line. When you click on this menu item the system will down-load all the time schedules and user details for this door. You use this menu item after you have installed a new door.
Note that using this menu item will erase all the history for the door.

5.1.2.6 Assigning a time schedule to a door
You can assign a time schedule to a door by clicking the Set timed control button to bring up the Time schedule form. You can now define a new time schedule or a time group if you wish. To assign a time schedule to a door double click on an entry in either of the 2 panels.

5.1.2.7 Deleting a time schedule from a door.
Click on the door entry in the table and then click the Clear timed button.

5.1.2.8 Controlling doors
When you are running on-line you can control the operation of a door. Click the button in the Door
control panel corresponding to the function you wish to perform.

5.2.1 Functions
5.2.1.1 Inputs

Configure inputs - Allows the configuration of digital inputs for the door controllers
Input status - Displays the state of digital inputs
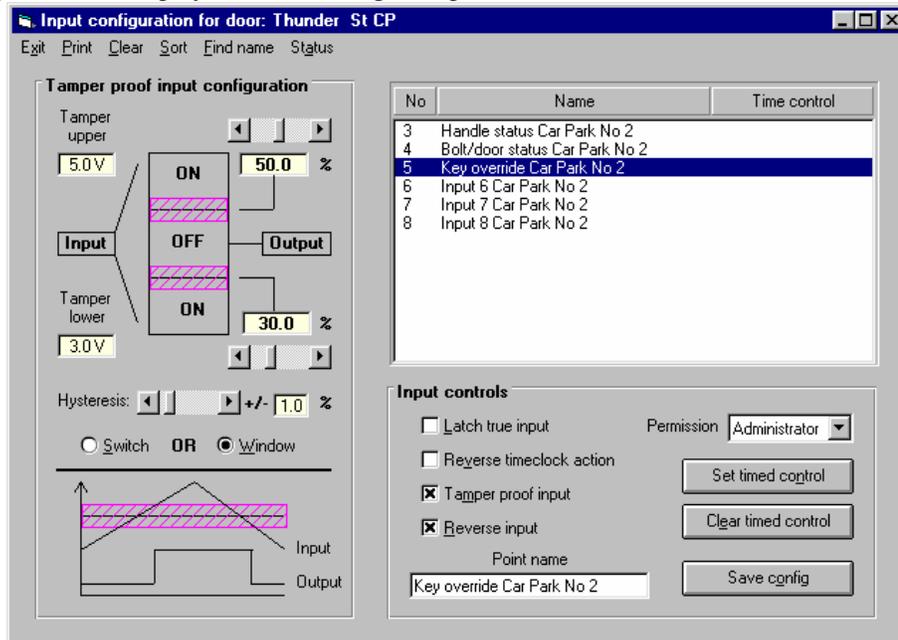
5.2.1.2 Outputs
Configure outputs - Allow configuration and control of digital outputs
Output status - Displays the status of digital outputs
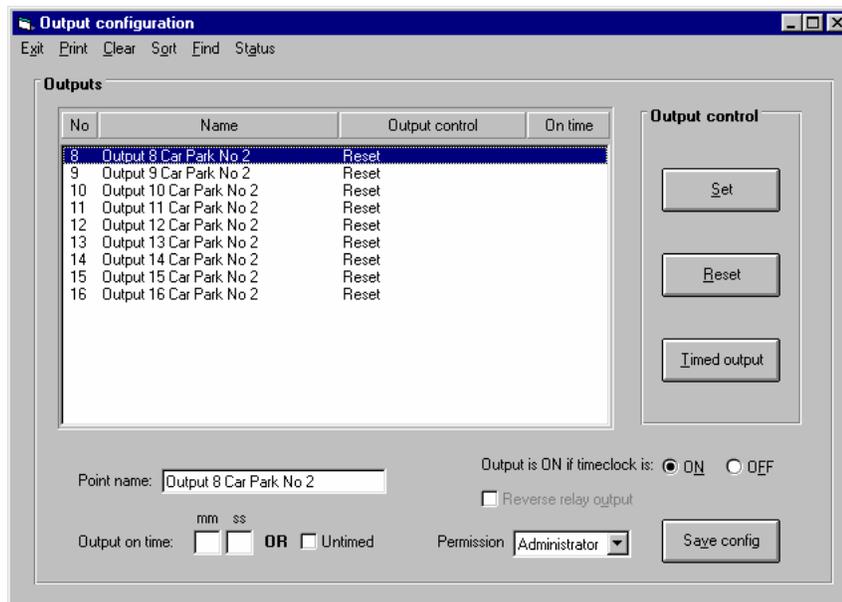
5.2.1.3 Configuring an alarm

An alarm can be generated from a digital input, variable or output or a tamper input. You can select the time the source has to be valid for before an alarm is generated. You can generate an alarm on the source being True or False. You select the source for the alarm using the controls in the Source panel and the conditions under which an alarm should occur in the Alarm conditions panel.

An alarm can also control a digital variable or output. You can configure the output to be True or False when an alarm exists. If you wish to display the alarm on a dynamic drawing you MUST set an output for the alarm.

The Inhibit panel allows you to use another digital input, variable or output to inhibit the generation of an alarm. If the inhibit value is in the selected state then even if all other criteria for generating an alarm are met the alarm will not occur.

Associated with each alarm is a message. You can select from a user generated list of messages or type your own message into the bottom panel on the form. You can delete messages provided they are not being used by an alarm.

You can give an alarm one of 4 priorities: Critical, High, Medium, Low. You do this be selecting the desired priority in the Alarm priority panel. The various priorities are indicated by the background colour in the system status panel.

Critical alarms display as yellow text on a red background
High alarms display as red text on a yellow background
Medium alarms display as red text on a green background
Low alarms display as yellow text on a blue background

5.2.1.4 Logic Function Block Setup [AND – OR]
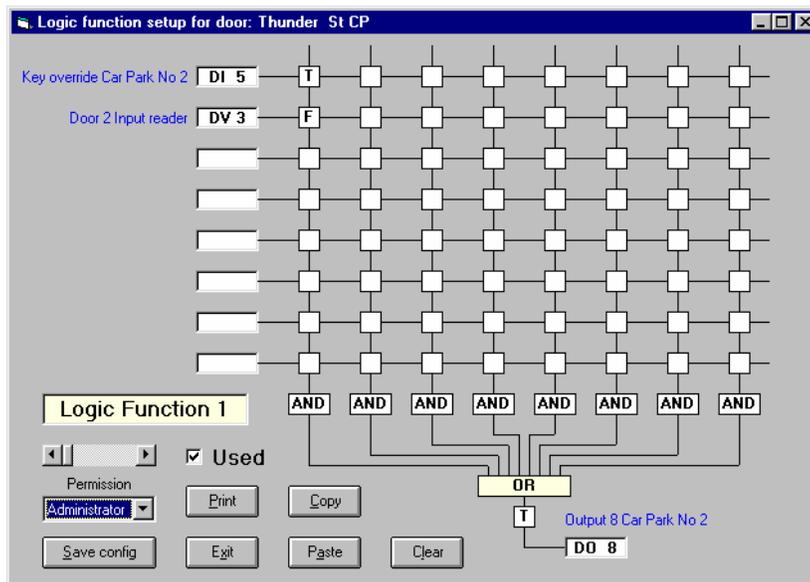
A logic function accepts up to 8 inputs. Each of these 8 inputs can be included in an AND function using either the input or its complement. You can have up to 8 of these functions which are all OR'd together to provide the function output. You can also invert the function output. You can see the state of the logic function when you are monitoring the door status.

The logic form displays 8 input boxes arranged in a vertical row on the left side of the form. From each input box there is a horizontal line indicating the input. There are 8 vertical lines each crossing each input line and each ending in a box labelled AND. These lines represent the inputs to each AND function. There is a square box (the input enable box) at each intersection of the horizontal and vertical lines. To connect an input to an AND function click on the intersecting box. If this box displays the letter T then that input to the AND function is the true value of the input. If the box displays the letter F then the complement of the input is the input to the AND function. If the box is blank then that input is not connected to the AND function. Repeatedly clicking the box cycles through the 3 possible states. (You can also double click this box to change the states 2 at a time.)

To select an input click on the rectangular box representing an input. This will change the background colour of the box and open up a panel labelled Select input. Click on the arrow in this box to display a choice of input sources and then use the scroll bar to choose the channel number. The input box will display the selected input and the name associated with that input will also be displayed. You can choose another input without clicking the OK button. Note that selecting an input as unused will set all input enable boxes for that input to the clear state.

To select the output of the function click on the output box and follow the same procedure as listed for selecting an input. You do not have to click the OK button until you have finished selecting all used inputs and outputs.

For example, assume that input number 1 is to be set to digital variable 7 (DV 7), input number 2 is unused and input number 3 is digital output 15 (DO 15). The output of the function is to go to digital variable 22 (DV 22). The output of the function is to be true when DV 7 is true and DO 15 is false. Assume that no inputs or outputs have been set for this function.

Click on any one of the left input boxes.

Click on the down arrow in the Select input panel and then click on the entry labelled Digital variable. The coloured input box will display DV 1.

Slide the scroll bar until the input box reads DV 7.

Now click on any other input box. The highlight colour will change to this box. Repeat the previous procedure to set this input to DO 15.

Now click on the output box. Its background colour will change and the selection panel will now read Select output.

Click on the down arrow and then click on the entry labelled Digital variable.

Use the scroll bar to set the output of the function to DV 22.

Click the OK button to close the panel.

Now click the input enable box where any of the 8 vertical lines crosses the horizontal line corresponding to the input box DV 7. This selection box should display a T.

Now double click the input enable box in the same vertical row where the horizontal line corresponding to input DO 15 crosses it. This box should display a F.

Clicking the Clear button will clear all input enable boxes.

Clicking the Save config button will save the configuration while clicking Cancel will not. Clicking the Save config button will also cause the Used checkbox to become checked thus enabling the function. To disable the function click on the Used checkbox to clear it. This will clear all inputs, the output and all input enable boxes.

The scroll bar can be used to select the function number. The Exit button will close the form.

If running in the on-line mode the logic function data will be downloaded to the doorcom when the Save config button is clicked.

5.2.1.5 Time Delay Function Block Setup
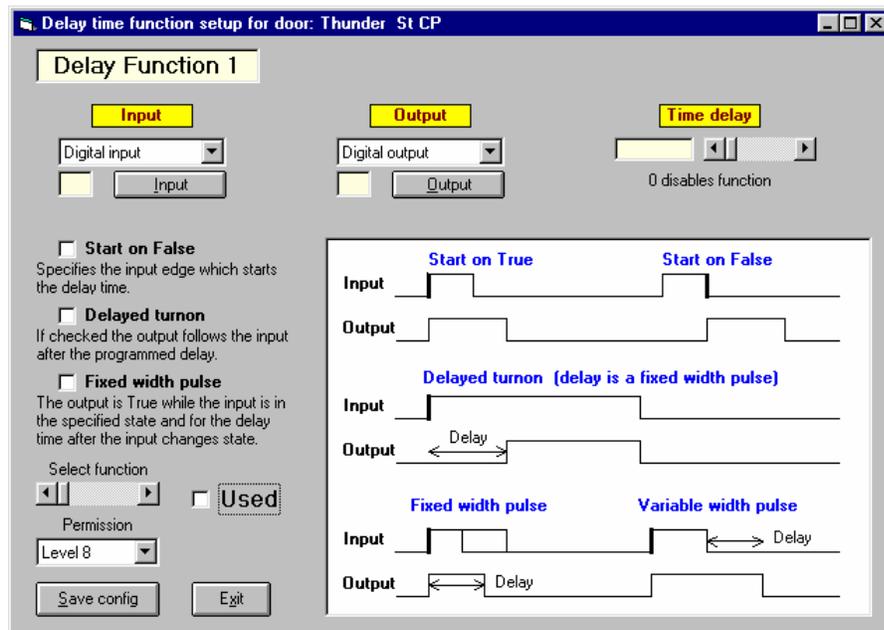
A delay function is used to provide a time delay which can be used to provide a fixed length pulse or stretch an input pulse or for many other purposes.

The first step in creating a delay function is to describe where the input of the function comes from. Click on the down pointing arrow to display the available choice of inputs and then click on the desired input to select it. The channel number for the input can be selected by using the button underneath the input label. (The input of a delay function can be from a digital input, output or variable). If there is a name assigned to the channel then that name will appear below the scroll bar and channel number.

Normally the function would be activated when the selected input becomes true, however, you can make the function become activated when the input becomes false by checking the checkbox below the input channel scroll bar.
Click the Fixed width pulse checkbox if you wish to generate a single, fixed width pulse (equal to the delay time) from the delay function. Leave this box unchecked if you wish to generate a pulse whose width equals the input pulse width plus the delay time.

The next step in creating a delay function is to describe where the output of the function goes. Click on the down pointing arrow to display the available choice of outputs and then click on the desired output to select it. The channel number for the output can be selected by using the button beneath the output label. (The output of a delay function can go to a digital variable, a digital output or it can be used to control an analogue output).
The final step in creating a delay function is to set the desired delay time. Use the scroll bar to set the time. The delay time is displayed in hours, minutes and seconds next to the scroll bar. A click on the arrow box at either end of the scroll bar will change the time by 1 second while a click to either side of the scroll button will change the time by 1 minute.

Clicking the Save config button will save the configuration in the configuration data file while clicking Cancel will not. The Used checkbox will become checked if the time delay is set to a non-zero value. You can also mark the function as used by clicking the Used checkbox, but this should not be necessary.
The scroll bar can be used to select the function. The Exit button will close the form.

If running in the on-line mode the delay function data will be downloaded to the doorcom provided that the Used checkbox is checked.

5.3 Groups

Allows you group doors into groups

5.3.1 Door Groups

As for time schedules, you can combine a number of doors to form a door group. You can use this group in place of a single door when defining the access for a cardholder. To access the form allowing you to define door groups, click the Doors menu item followed by the Groups menu item. This will open up the Facility Security: Define groups form. The right hand panel lists all the doors defined.

5.3.2 To view the doors in an existing group

Click the arrow in the Defined groups box to display a list of all the groups defined. Then click the desired entry and the doors in that group will be displayed in the list below. The name of each door (limited to the first 20 characters) is displayed together with the permission level for that door. The current permission level for the group will be shown in the Permissions box.

5.3.3 To add a new group

1.   Select the doors you wish to add into the group in the right hand panel.

2.   Type a new name for the group in the Defined groups box.
3.   Press the Enter key to save this name.
4.   Click the Add button to add the selected doors to this group.

5.3.4 To delete doors from a group

Click the name of the door in the list of doors in a group. Then click the Delete button to remove that door from the group.

5.3.5 To delete an existing group

Remove all doors from a group as per the paragraph above and then click the Delete group menu item. This will delete the group whose name appears in the Defined groups box.
Note: you cannot delete a group while there is still a door defined in the group.

5.3.6 To assign a permission level to a group

Select the group you want to assign a permission level to. Select the permission level for that group. This can be different from the permission levels of the individual doors making up the group. Then click the Assign button.

5.4 Status

Displays the status of each door in the network
Group control - Allows the opening, closing and assigning time schedules to all doors in a group.

5.5 Multilevel Passback

38
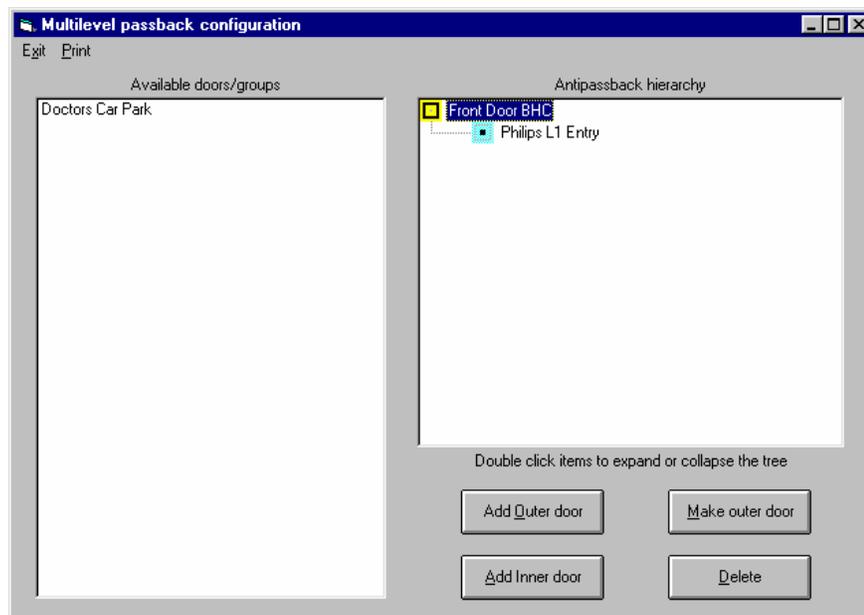
5.6 Access Maintenance

5.6.1 User Numbers
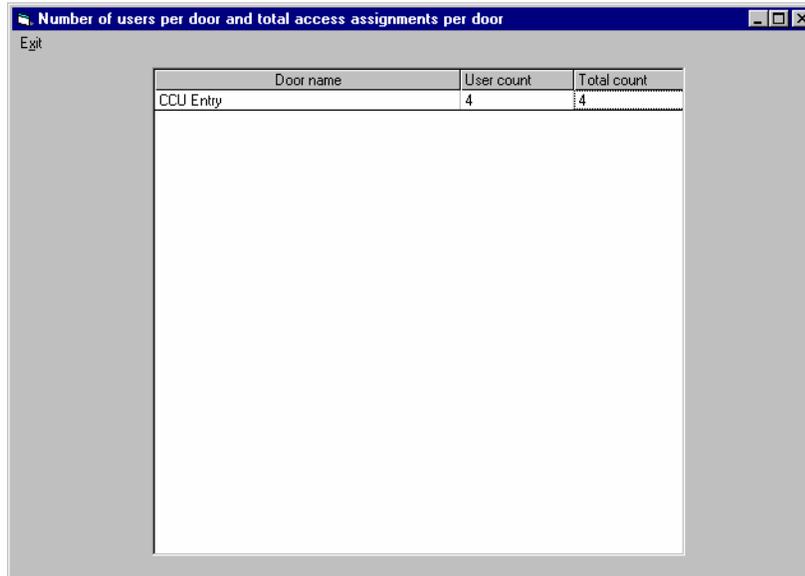
5.6.2 Failed Updates & Data Base Fixes

6 Lifts

6.1 Lifts

Clicking the Lift menu item will open up the Lift definitions form. This form displays a list of the lift controllers in the network. There is one entry for every lift car in the network. You can change the name of the Building field by clicking on the label.

Lift cars are assigned in groups. All the cars with the same Name, Building and Shaft details are assumed to be in the same group. When you configure any lift in this group you can also automatically have the same configuration details applied to all the other cars in this group. Note that the Building field is used in exactly the same way as for doors.

As for doors, each lift car has a serial number and an access time. The access time specifies how long the user will have after swiping his card to finish pushing the button for the desired floor. After the access time has expired all floors are locked out. You can set an access time from 1 to 255 seconds.

The Number of floors field tells the controller the maximum number of floors that the lift has. This includes floors where the lift cannot stop. All cars in the same group MUST have the same number of floors. If you assign more floors to one car than any other, these floors may not be accessible on any

lift! If you have one car in a group which has a different number of floors then you must assign a different shaft to this car or you must let all lifts have this number of floors and then permanently lock out those floors on cars which cannot reach them. If some cars cannot stop at one or more floors then you must still include those floors in the field. You do not need to include the hardware to control those floors so there is no cost penalty in this operation.

Each lift controller comes standard with two uncommitted digital outputs and 6 digital inputs. These are programmed exactly like the door inputs and outputs.
The names assigned to the digital inputs map to the connections on the controller as follows:

Input 3	HND
Input 4	BLT
Input 5	KEY
Input 6	I6
Input 7	I7
Input 8	I8

The digital outputs map to the connections on the controller as follows:

Output 7	DR
Output 8	D8

You can add two more blocks of 8 digital inputs to a controller. Click the appropriate option button to specify the number of inputs on the controller. Additional inputs are numbered from 9 upwards.

6.2 Adding a new lift

Click the Add menu item and then enter the lift details into the various fields. Then click the Update button to save the data in the database. Note that after adding a new lift the fields are not cleared. Note that clicking the Update button DOES NOT transfer any information to the lift controller.

6.3 Editing an table entry

To edit a table entry, click the desired entry, edit the desired fields and then click the Update button. Note that this operation DOES NOT transfer any information to the lift controller.

6.4 Deleting a lift

To delete a lift, click the desired entry in the table and then click the Delete menu item. Note that deleting a lift will also delete all user accesses to that lift.

6.5 Sorting the displayed list

You can sort the displayed list in several ways. Click on the Sort menu item and then click one of the displayed items to perform the sort.

6.6 Finding an existing lift name

You can find the name associated with a particular lift by clicking the Find name menu item and then entering any part of the name for the lift. Click the OK button to search for the name.

6.7 Configuring a lift

You can configure the lift controller for a single car or a group of cars by clicking any member of the group and then clicking the Configure lift menu item. This will open the Lift floor controls form. The

top of the form shows the Building and Shaft names assigned to the lift group. You have the choice of configuring all cars in the group or just the single car you have selected. You select the option desired by checking or un-checking the For all cars in this group checkbox. If you are only configuring a single car then the car number will be shown.

In general, you will start by configuring all cars in a group together. You might then need to change some access provisions for one car separately.

The table lists each floor in the lift group. You can set a time schedule for any floor or secure or un-secure a floor. You can also change the name of a floor. To perform any operation on a floor click the floor entry in the table. If the floor has a time schedule associated with it then the schedule details will be displayed in the top right hand panel.

6.8 To change the name of the floor

Click the appropriate table entry. The floor name is displayed in the bottom right hand panel. Edit this name as desired and when you have finished press the Enter key. Note that the cursor does not have to be at the end of the entry.

6.9 To secure or un-secure a floor

Click the desired floor entry in the table and then click the Secure floor or Free floor button. This will immediately download the information to the lift controller.

6.10 To assign a time schedule to a floor

Click the desired floor entry in the table and then click the Set timed control button. This will open up the Time schedules form. You can assign a time schedule or a time schedule group to the lift floor by double clicking on an entry in either of the two tables in this form. You can also define a new time schedule if you wish.

6.11 Programming a lift

You can transfer the lift configuration to the lift controller by selecting the lift in the table and then clicking the Program lift menu item. This will completely configure the lift car. All existing information in the car controller will be destroyed. The time schedules, the floor access levels and the user details will all be transferred. Note that you MUST DO THIS operation after you have initially added a new lift otherwise you will not be able to communicate with the lift. You should not have to perform this programming operation thereafter as the floor data is transferred immediately as you secure or un-secure a floor.
High level and low level elevator interfaces available.

7 Time

7.1 Time schedules

Allows the definition of time schedules and time schedule groups
To define time schedules click the Time menu item in the main screen, then click the Time schedules menu item. This will bring up a form labeled : Facility Security: Time Schedules.
Time schedules are displayed in the top panel of the form. **All times are based on a 24 hour clock.**
Note: You are allowed a maximum of 16 different time schedules.

7.1.1 Adding a new time schedule

You can add new time schedules by entering a name for the time period and the times and days when this schedule should be active. The time is active from the hours and minutes typed in the From boxes until the hour and minute set in the To boxes. The clock will be active on the days where a check mark appears. When you are happy with the settings click the OK button. This will enter the time period in the panel above.

7.1.2 Editing an existing time schedule

Click on the time schedule in the top panel. This will transfer the details of that period to the Edit time schedule panel. You can now change the data and then either click OK to update the entry or click Cancel to leave the entry unchanged.

7.1.4 Sorting time schedules

The Sort menu item allows you to display the time schedules sorted by the Name, From or To times. Just click the desired menu item to display the resorted list.

7.1.5 Finding a particular time schedule

You can find a particular time schedule by clicking the Find name menu item. This opens a dialogue box. Type the name of the time schedule in this box and then click OK. If the time schedule can be found it the list be re-arranged to display this entry within the displayed list.

7.1.6 Creating more complex time schedules

You can create more complex time schedules by combining time periods into groups.
You are allowed a maximum of 16 time period groups.

7.1.7 Adding a time period group

Click on the time periods in the top panel which you wish to combine into a time period group. The highlighted periods will be combined into a group. Successive toggling of an entry will change its highlight. When you have finished with your selection, click the Paste button. A new panel will open asking you to enter a name for the group. Enter a name and click the OK button to save the new group, or click the Cancel button to abort.

7.1.8 Deleting a time period group

Click the desired group in the lower panel and then click the Cut button. Note that you cannot edit a group you must delete the group and re-enter it to make any changes.

7.2 Set PC time

Allows setting of the PC clock and resets all DC390 clocks.

7.3 Public Holiday Entry Schedule

To set public holidays click on the Time menu item and then click the Public holidays menu item. This will open up a form called facility Security: Public holidays.
To add a public holiday to the list of holidays click on the date. This will change the date colour and cause a new line to be added to the list of public holidays displayed on the right side of the form.
You can give a name to a public holiday. Click on the public holiday in the displayed list and then type in the name for this day. When you press the Enter key the name will be attached to the holiday. You can change the name of an existing holiday the same way.

To change the month or the year click on the appropriate down pointing arrow to display a list of choices. If a scroll bar appears you can use this to show more choices. Click on the chosen item to select it. The calendar will change as well. You can add up to 16 public holidays.
To delete a public holiday either click on the coloured date in the calendar, or click on the entry in the holiday list to select it and then click on the Delete button to delete the selected item.

Clicking the OK button will close the form. If running in the online mode then the holiday list will be downloaded to the Doorcom.

7.4 Door times

Displays the current time and date stored in each door
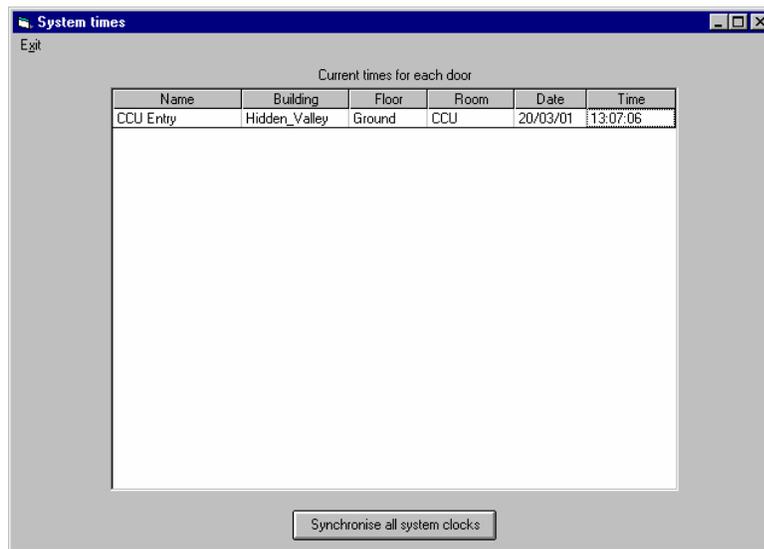
8 Inputs

The standard Doorcom controller has 6 digital inputs. Although these 6 inputs can be used for any purpose, the names of the first 3 inputs default to specialised inputs relevant to the door status. These are the handle, bolt and key status's. When you add additional boards, the inputs of these new channels become input 9, 10 etc. You can change the name of any input by clicking on the entry in the table and then typing the new name in the Point name field. Either press Enter or click the Save config button to save the new name. There are two type on input available on the system: A normal digital input and an analogue type input which can be used for tamper monitoring. There are also a number of options available for inputs.
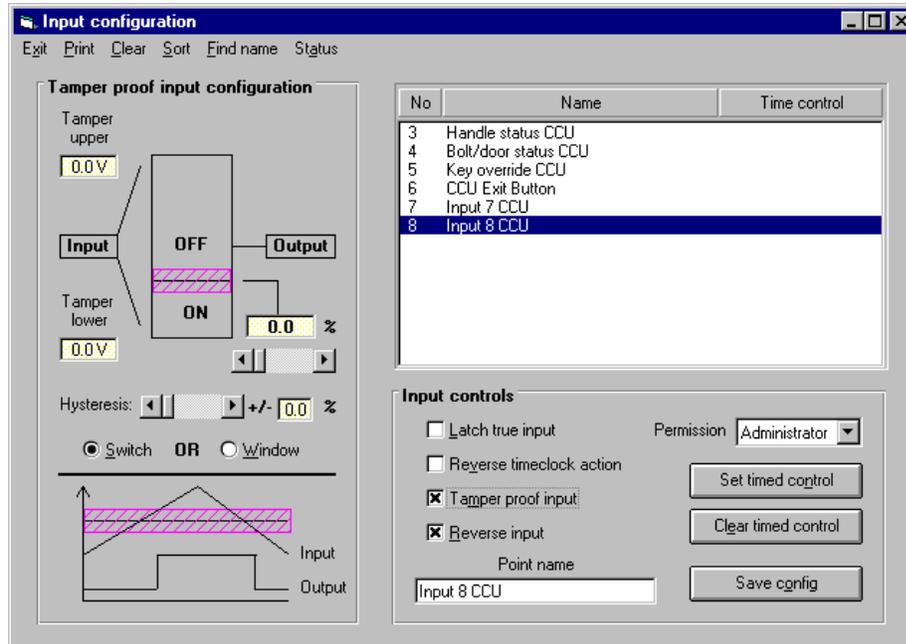
8.1 Options for inputs

Reversing an input state
An input normally is True when it is shorted to ground. All inputs can have their operation reversed. i.e they are True when open and False when closed. You reverse the operation of a digital input by clicking the Reverse checkbox. This also works for tamper inputs but in a slightly different way.

8.2 Reversing the operation of a timeclock

Each digital input can be set up to be controlled by a timeclock. Normally when the timeclock is on (True) the digital input is held to the False logical state independent of what happens in the real world. (Note that this is taken AFTER any input reversal). By checking the Reverse timeclock checkbox you force the input False when the timeclock is off (False).

8.3 Latching an input

Normally the logical state of an input follows the state of the physical input attached to it. This is not satisfactory for security operations. By checking the Latch checkbox you capture a momentary True state of an input. Thus while the physical input is held False the logical state, as seen by the doorcom, is also False. Once the physical input becomes True the logical state also becomes True. It remains True even if the physical input is removed. You can only clear a latched input using the input status form

8.4 Tamper proof inputs

Tamper proof inputs use an analogue-to-digital converter to measure a voltage level and then convert this measured value to a digital value. You can also use a tamper input to measure other things such as room temperature. Associated with each tamper input are two level functions. You can either use a simple threshold or a window function to convert the input to a digital value. Tamper proof inputs normally work by having a fixed resistor at the end of the line and then shorting this out with a second

46

resistor when a switch closes. Thus the voltage on the line switches between two voltage levels. Changing a switch from the open to closed position usually causes a decrease in the voltage at the input thus the reverse checkbox becomes checked when you initially select a tamper proof input. The system also detects for the presence of an open and shorted line and these conditions set a tampered input state as well as the switch state. The voltage levels at which the tamper is detected are fixed at 1Volt and 3.5Volts. For a tamper proof input you should select a Switch function and set the switch threshold at halfway between the open and closed voltage levels.

A threshold works by comparing the input to a fixed (user set) value. If the input is above the level the output is True otherwise it is False.

A window works in a similar way but now the input has to be between a low level and a high level for the output to be True.

Because there can be problems with noise on an analogue input there has to be some means to prevent an input continually causing a change in the output state if it is almost at a threshold level. This noise rejection is done by providing a hysteresis band around each threshold value. If the input is below the low threshold minus the hysteresis the output is False. It remains false until the input rises above the threshold plus the hysteresis. When the input falls it has to fall below the threshold minus the hysteresis to again become False.

You select the type of function, the lower and upper thresholds and the hysteresis level (the same value applies to each threshold) by using the controls in the Tamper proof input configuration panel.

8.5 Sorting the displayed list of inputs

You can sort the displayed list of inputs either by Name or Door. Just click on the appropriate entry in the Sort menu item.

8.6 Finding a particular entry

You can find a particular entry in the table by clicking on the Find name menu item. This will open a dialogue box. Type the name, or part of the name, in the textbox and click the OK button. The program will start searching from the current point in the list down towards the end of the list and the first matching occurrence of the string will be highlighted. Repeating this procedure will find the next matching occurrence of the string. If no matches are found there will be no change to the display.

8.7 Clearing all the data for an input

Clicking the Clear menu item will clear all data for the selected output.

8.8 Controlling inputs with a timeclock

Like doors, inputs can be controlled by timeclocks.

To set a timeclock to control an input, click on an input in the table and then click the Timed control button to bring up the Time schedule form. If necessary, you can define a new time period now. Doubleclick on a time period or a time period group to set the timeclock for the input. Click Save config to save the data.

To delete a timeclock from controlling an input, click the desired input in the table and then click the Clear timed ctl button and then the Save config button.

8.9 Displaying the status of the inputs

You can click on the Status menu item to display the status of the various inputs.

9 Outputs

To configure outputs you click on the Output menu item and then click Configure outputs. This brings up the Output configuration form. The standard Doorcom controller has a single output, in addition to the door it controls, but this can be extended by up to 16 additional outputs. You can change the name of any output by clicking on the entry in the table and then typing the new name in the Point name field. Either press Enter or click the Save config button to save the new name.

9.1 Set and Reset

The terms Set and Reset are deliberately chosen to avoid misunderstanding between Open and Closed. When talking about controlling the outputs we are talking about opening and closing relays. Typically when a relay is closed the controlled device, say a door, is opened and vice versa. Using the terms Open and Closed when talking about the on-board relays could be confusing. When an output is Set then it is on and the corresponding relay contacts are closed. When Reset the output is off and the contacts are open. When an output is set then no other function can change its states. When an output is reset then it is not actuated and any other function can activate the output. Thus when an output is controlled by a timeclock, when the timeclock is off then an input card read can open the door as can a pushbutton but when the timeclock is on the output is on and cannot be turned off.

9.2 Reversing relay operation

In most cases the normal relay operation is suitable but there can be occasions, especially involving relay state in a power down condition, where it is necessary to reverse the operation of a relay. By checking the Reverse relay output checkbox you logically invert the operation of a relay. (i.e. an OFF state will close the relay contacts). Note that this function operates directly on the relay and is not to

be confused with a logical output of the system. The system should still be configured for a logical True and False output, you use this function convert the logical output to the desired physical output.

9.2 Timeclock control of relays

Outputs can be turned on or off or controlled by a timeclock. You can also make an output turn on for a predetermined time. You can also reverse the way a timeclock drives an output by clicking the On or OFF option buttons.

9.3 Sorting the displayed list of inputs

You can sort the displayed list of inputs either by Name or Door. Just click on the appropriate entry in the Sort menu item.

9.4 Finding a particular entry

You can find a particular entry in the table by clicking on the Find name menu item. This will open a dialogue box. Type the name, or part of the name, in the textbox and click the OK button. The program will start searching from the current point in the list down towards the end of the list and the first matching occurrence of the string will be highlighted. Repeating this procedure will find the next matching occurrence of the string. If no matches are found there will be no change to the display.

9.5 Clearing all the data for an output

Clicking the Clear menu item will clear all data for the selected output.

9.6 Setting the length of time an output should be on for

Select the output in the displayed list and then either check the Untimed checkbox or set the time in minutes and seconds the output should be on for and click the Save config button. Each time the output becomes set it will turn on for the time selected. Note that if the output is turned on by a timeclock it will remain ON while the timeclock is active irrespective of any other settings made.

9.7 Controlling an output

You can turn an output on or off by selecting an output in the displayed list and then clicking the Set or Reset buttons. You do not need to click the Save config button.

You can set an output to be controlled by a timeclock by selecting the output and clicking the Timed output button. This will bring up the Time schedule form. If you wish you can enter a new time period or create a new time group. Doubleclick on an entry in either of the two panels to assign a timeclock to the output. The name of the timeclock will appear in the list of outputs.

9.8 Displaying the status of the outputs

You can click on the Status menu item to display the status of the various outputs.

10 Drawings

10.1 Generating Real Time Dynamic Drawings

You can only develop system diagrams and data displays while the doorcom is **offline**. To generate a system drawing click on the Drawing menu item in the main screen. This will result in the display of a new form. Drawings are placed in groups. The selection of a drawing is a two step procedure. First click on the drawing group in the left hand box. This will display a list of drawings in that group in the right hand list. Then click on the desired drawing name.

To generate a new group click on the Add button and then type the group name in the text box. Click on the Group option button and then click on Enter data. The new group name will appear in the group list panel. You can add as many groups as you like. The Group option button will remember its last setting.
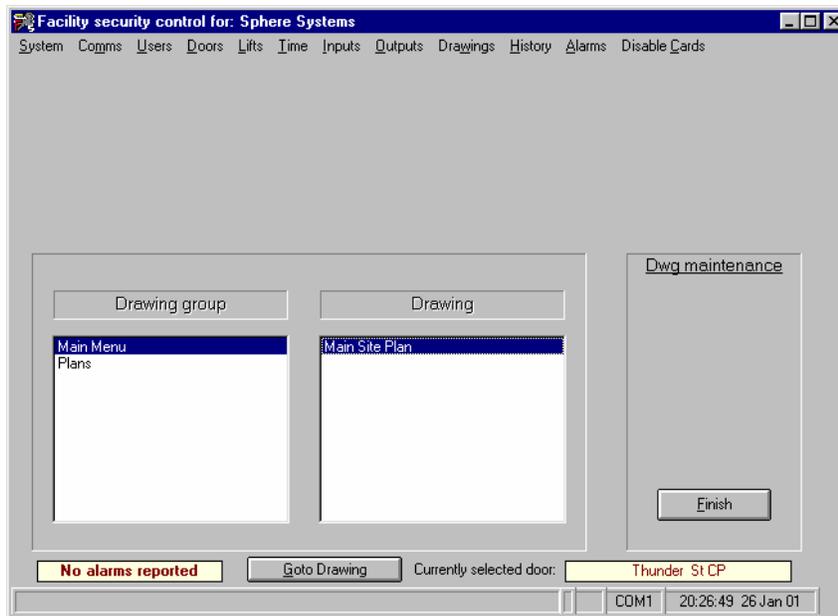
To enter a new drawing repeat the above procedure but click the Drawing option button before clicking the Enter data button. The blank drawing screen will appear and then proceed to produce the drawing as detailed in the manual.

You can delete a drawing by selecting the drawing group and the drawing (both lists must have one item highlighted) and then click the Delete button.
You can move a drawing from one group to another. Select the drawing as before and then click the right mouse button over the selected drawing. The highlight colour will change to a green background. Now select the desired group in the left hand panel. When you click on this group the drawing name will disappear from the drawing list and the highlight colour will return to its normal value. Note that the list of drawings in the right hand panel does not match the selected group displayed. You must click the group entry again to update the display. Alternatively you can select a new drawing to move.
You can delete a drawing group but only when there are no drawings in that group. To delete a drawing group click on the group name and then move all drawings in that group to other groups or

delete them one by one. When there are no drawings left in the group and there is no highlight displayed in the drawing list, you can delete the group by clicking the Delete button.
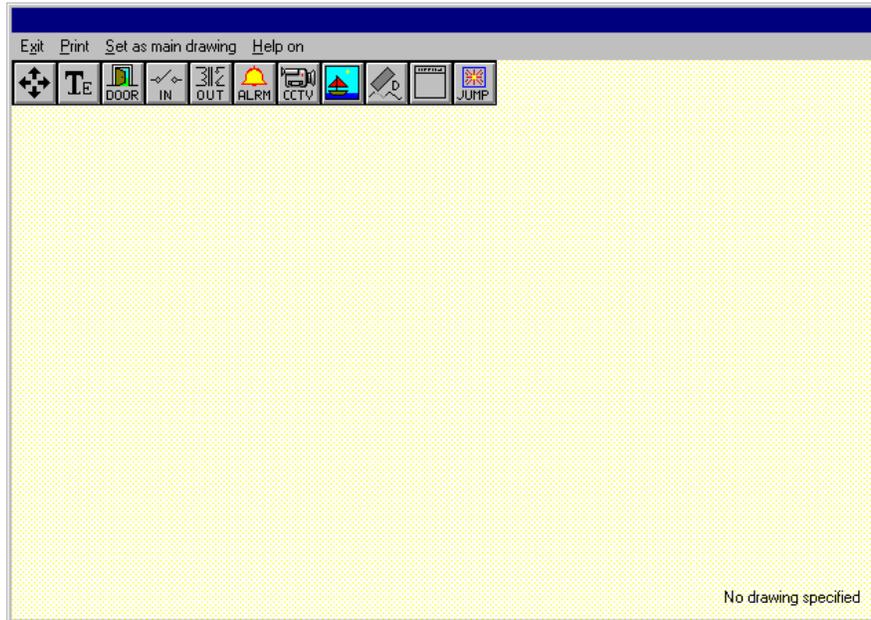
When you either add a new drawing or edit an existing drawing a new form will appear. This form contains a toolbar at the top and several buttons at the bottom. The toolbar icons allow you to develop the drawing. Online help is available by clicking the Help on button. When the cursor is positioned over a toolbar icon a brief description of how to use the icon appears. The toolbar icons are as follows:
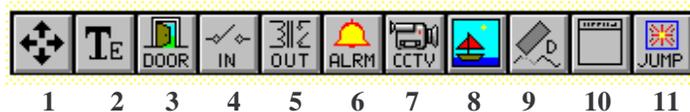
(1) This icon is used to move the toolbar. Position the cursor over the icon and hold the left mouse button down. While holding the button down drag the toolbar to where you want it and then release the button.

(2) This icon is used to insert text into the drawing. Position the cursor over the icon and hold the left mouse button down. While holding the button down drag the mouse to where you want the text to be located. A small rectangle will be attached to the cursor. When you have positioned the cursor where you want the centre of the text to be release the mouse button. A dialog box will open. Type your text in the text box in the Text panel. You can change the size of the font and also bold and underline it by checking the various checkboxes in the Font style panel. When you are happy with your selection click the OK button and the text will appear on the drawing.

(3, 4, 5 & 6) These 4 icons are used to insert a doors, inputs, outputs or alarms into the drawing. The point will display the current status read from the doorcom every few seconds when the drawing is loaded in the online mode. To insert a point proceed as for text insertion as above. When the dialog box opens display the list of possible items by clicking the Show points button. To select a point either double click on the point in the table or click once on the point to highlight it then click the Select button. The point name will appear in the textbox in the Point name panel. The name of the point will also be displayed on the drawing. You can choose to hide this name by unchecking the

Show name checkbox. As for the text insertion above, you can modify the text style for the point name. When you click the OK button the point name will appear in the drawing in a box. The point name will be replaced by the actual point data when the doorcom is running online. Note that the only alarms that you will be able to place on a drawing are those where the output of the alarm is configured to drive a digital variable or a digital output.

You can specify how the text will be aligned on the screen. As the data changes the size of the displayed box changes. Left aligned keeps the left hand side of the box fixed at the position specified when constructing the drawing. Centre keeps the centre fixed while right aligned keeps the right hand side fixed.

(7) The camera button is used to place the controls for a CCTV camera onto a drawing. To insert a camera control icon, drag the icon from the toolbar and drop it on the desired spot on the screen. When you drop the control a form will open listing all CCTV cameras available. Select a camera either by double clicking an entry in the list or by single clicking and then clicking the Select button.

 (8) The picture icon is used to insert a picture in the drawing. Click on the icon to open a file selection dialog box. You can select any Windows metafile (*.wmf) , Windows bitmap (*.bmp) file .gif and jpg Windows metafiles will be automatically scaled to fit the drawing area. This could result in distortion of the drawing if the aspect ratio is not the same as the display aspect ratio. Windows Bitmap files are cropped to fit the display area. Thus a bitmap which is, say, wider than the display area but the same height will have its right hand side cropped to fit the display area. You can replace the current drawing with another drawing by clicking again on this button.

(9) The 'D' button is used to delete labels and points in a drawing. To use this button click on it. A help message displays on the bottom of the screen. To delete a point or label just double click on it. The label or point will not be deleted immediately but will change colour and will be deleted when the drawing is saved.

(10) This button is used to place a heading on the drawing. Clicking this button to open a dialog box. Proceed as for the text icon above. You can change font characteristics if desired. When the OK button is pressed the name you have chosen will have replaced the heading of the form. You can replace this heading as often as you wish.

(11) The jump button is used to insert hotspot jumps into a drawing. A hotspot jump allows you to assign a drawing to a region of the display so that when the user clicks on that region the screen will show the new drawing. You can insert invisible hotspots or hotspots surrounded by a blue border. You also have the option of creating a hotspot showing a line of text or even showing another drawing. If desired you can build complex menus consisting of pictures which the user can click on to display that drawing. Note that points displayed in drawings used as hotspots do not update. To insert a hotspot click to show the procedure. You can move text and points after you have dropped them. Simply position the cursor over the item to move and hold the left mouse button down. Then drag the item to where it should go and release the mouse button. If you attempt to move the item over an illegal area then the mouse cursor will change to a white circle with a diagonal white line. You can still drop the item if you wish but it might not move.

The Print button will draw the form on the current Windows printer.
The Exit button will close the form and save the drawing to disk.

10.2 Displaying Dynamic Drawings

Drawings created when offline become active when you are running in the **online** mode. This means that the data in the drawing is updated every few seconds from the field. The dynamic data also shows whether a an alarm has been triggered by this point. You can also change the state of doors and turn outputs on and off. In addition, you can set or clear timed controls for inputs, outputs and doors. To change the state of a door or output or to set or clear a timed control, place the mouse cursor over the state of the point and click the mouse button. This will bring up a pop up menu. Click on the desired menu item to make the change you desire.
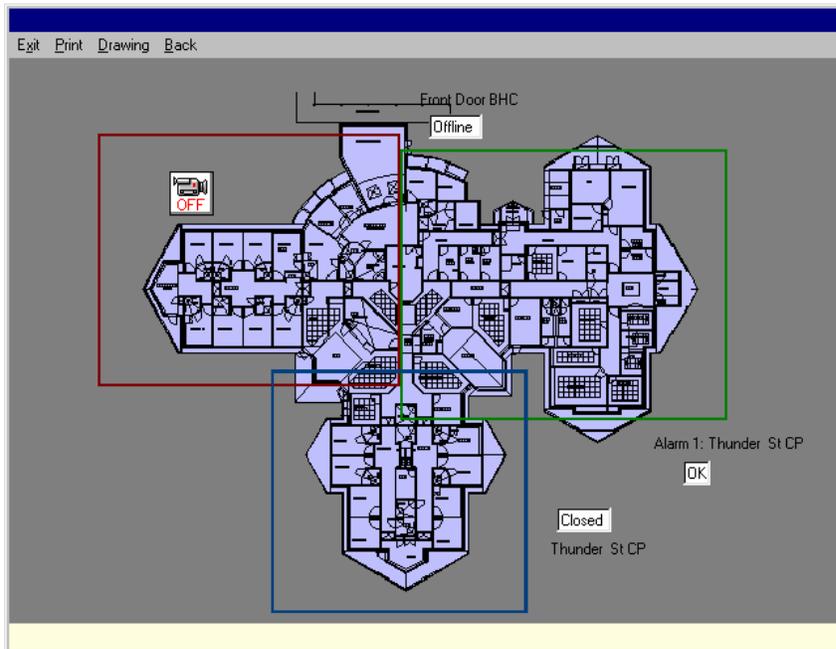
The data for a door can be preceded by one or more letters. These letters have the following meanings:

C - The door has been activated by a card. This applies to doors set as first card activation
     T - The door is set for timed control.

You can change to display a new drawing by clicking the Drawing menu item. This will bring up the drawing and drawing group selection panels. Alternatively, you can use the drawing jump system to construct a menu of drawings.

Clicking a CCTV camera button will activate the relevant camera and bring up its picture on the screen.

The drawing options in the Options form (System, Options menu items) allows you to change the time between drawing updates. Keep this time reasonably long as otherwise you will consume a lot of network bandwidth to the detriment of keeping track of the door history. For a drawing of about 20 points an update interval of 10 seconds should be adequate.

10.3 Dynamic Drawing Options per Workstation

Refer to section 2.3.11.2   System – Options - Drawings

11 History

11.1 Access history

Displays the history of the network
To display the history of operator actions, click the History menu item and then the Operator history menu item. This will result in the display of the Access history form. The list of entries is initially blank. To display the operator actions you have to click the Show menu item.

You can select what part of the history to display by changing the selections in the Selection criteria panel. The operation of the controls is fairly straightforward and the effect of the choices is best learned by some experimentation. The More options button gives you an expanded selection mode. You can select to display the history for a single user or a group of users. The group can be selected using either the department or manager fields. You can choose to see the history for a single door or a group of doors. The time selection can be based on hours and minutes as well as days.

Note: For the display to work properly you MUST set the Date formats in the System control panel to be of the form dd-MMM-yy, with the day of the month preceding the month. If you leave the system set to the American default of mm/dd/yy the sorting process will not work properly.

You can delete history from the stored list by using the same selection criterion you use to display history. Click the Purge button to delete records. All the access history is written to a data file (FAmmyyyy.log - where mm is the current month and yyyy is the current year) as well as being saved in the system database. You cannot delete records from the access history log file only from the system database. It is recommended that you periodically purge records from the database as otherwise the database will become very large and this will slow down accesses to the database. The log file is a plain text file and can be viewed with any standard text editor. You can use the search facility of the text editor to find records. Spaces are used as delimiters between fields so you can also import this file into a spreadsheet.

11.2 Operator history

Displays the history of operator actions
To display the history of operator actions, click the History menu item and then the Operator history menu item. This will result in the display of the Operator history form. The list of entries is initially blank. To display the operator actions you have to click the Show menu item.

You can select what part of the history to display by changing the selections in the Selection criteria panel. The operation of the controls is fairly straightforward and the effect of the choices is best learned by some experimentation. The String to search for box allows you to seek only those entries where there is a user defined message as part of the history message. User defined messages appear between double quotes ("). You only need to enter part of the string to look for, there is no need to enter asterisks before or after the string, the program will find any occurrence of the string appearing between double quotes. If you don't want to include this feature in a search then leave this field blank.

Note: For the display to work properly you MUST set the Date formats in the System control panel to be of the form dd-MMM-yy, with the day of the month preceding the month. If you leave the system set to the American default of mm/dd/yy the sorting process will not work properly.

You can delete history from the stored list by using the same selection criterion you use to display history. Click the Purge button to delete records. All the operator history is written to a data file (event.log) as well as being saved in the system database. You cannot delete records from the operator history log file only from the system database. It is recommended that you periodically purge records from the database as otherwise the database will become very large and this will slow down accesses to the database. The event.log file is a plain text file and can be viewed with any standard text editor. You can use the search facility of the text editor to find records.   Spaces are used as delimiters between fields so you can also import this file into a spreadsheet.

The system also maintains a file of the overall system logon/logoffs. This file is called user.log.

12 Alarms

12.1 Current Alarms

The latest system alarm is displayed in the System status bar. You can display a full list of alarms by clicking the Alarm menu item in the main screen. This will bring up the Alarms form. You can see the alarm pager message for an alarm by clicking on the alarm in the list.

You acknowledge an alarm by selecting the alarm and then clicking the Acknowledge menu item. You will be prompted to type a text message into the Operator acknowledge message panel and then press the Enter key to complete the alarm acknowledgement. Depending on the system options you might have to enter your password before being able to acknowledge an alarm. The time of acknowledgment and the operator who is currently logged in will be displayed in the panel. An alarm can only be cleared when the alarm is cleared in the field.

To display the action to be taken in response to an alarm, click the alarm and the action required will be displayed in the panel at the bottom of the screen.

If there is a recorded message for this alarm then when you click the Play message menu the message will be played.

You can display the location of an alarm in a graphic screen by selecting the alarm and then clicking the Show where menu. This will bring up a graphic screen containing the alarm. If the alarm appears on more than one graphic screen then only the first occurrence will be displayed.

You can display all alarms or only alarms of a particular priority by clicking the Display menu item and then clicking one of the submenu items.

12.2 Ademco

Configures the system to use Ademco contact ID dialing (Not Supported)
Securitel , SMS or paging is the preferred method for alarm notification.

12.3 Configure Dialer

Allows the linking of alarms to a Securitel monitored line
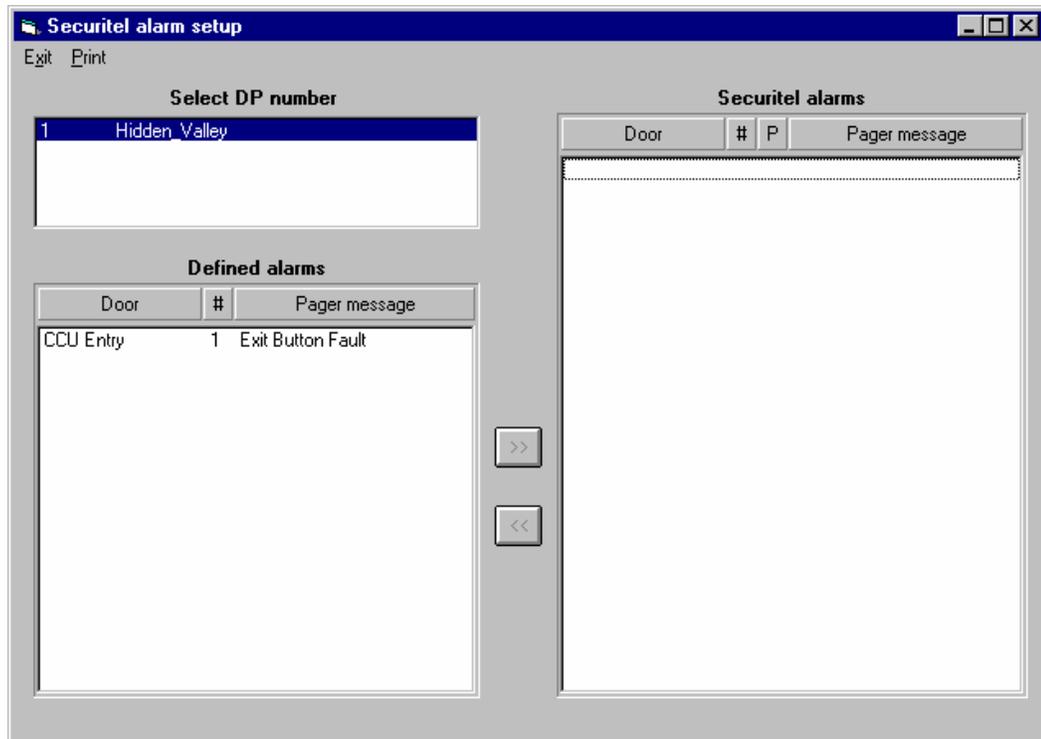
12.3.1 Securitel Configuration

Each alarm can be configured to either just display on the screen, display and print or also page out. If you wish to page an alarm then you must enter the pager id number and a message of up to 24 characters to be sent. The pager message may be preceded by another system generated message.

You can control how the system responds when it detects an alarm. The Options menu item in the System menu allows the system to automatically display the alarm screen when a critical alarm is detected. You can also enable an audible warning to sound every few seconds when one or more alarms are present and unacknowledged. Normally when an alarm is acknowledged the operator must type in his password to enable him to acknowledge the alarm. You can disable this requirement.

You MUST click the Save menu item to save an alarm. When an alarm is saved it is automatically sent to the doorcom. A deleted alarm is disabled in the doorcom.

You can change the default pager dialout to connect to a Securitel monitored line. Securitel monitoring can only handle 255 alarms in 4 priority ranges. The system allows you to select which alarms will be monitored. The securitel interface is connected directly to a DP11 network controller and as such can only send alarms for the doors connected to that DP11. If you have a multiple DP11 network then you need a separate securitel interface for each DP11.
To access the securitel alarm setup screen you need to select the Alarms, Securitel setup menu items in the main screen.

Select a DP11 processor from the list in the top left hand box. This will bring up a list of all alarms for all doors connected to that DP11.

To add an alarm to securitel monitoring click the alarm and then click the >> button. This will transfer the alarm to the right hand list.

To delete an alarm from the monitoring list click the desired alarm and then click the << button. This will transfer the alarm to the lefthand list.

To enable securitel monitoring you must enter the Client ID number given to you by the monitoring station. You enter this number by selecting the System Options menu items in the main screen. Enter the client ID number in the appropriate text box. Note that Securitel numbers must be a 4 digit hexadecimal number in the range or 0001 to FEFF.

To disable Securitel monitoring delete the Client ID number.

Note that you MUST reconfigure the network (ie all doors) to either turn on or turn off Securitel monitoring.

You can print the list of Securitel alarms by clicking the Print menu item.

12.4 Print alarm list

Prints the list of alarms

12.5 Define guard actions

For each alarm in the system you can define up to a 5 step sequence of operations that should be preformed when an alarm occurs. To assign an action to an alarm click the Define guard actions item in the Alarms menu in the main screen. This brings up the Alarms action form.

The drop down list box in the Defined actions panel will display the first step of all actions currently available. You can display the full steps by clicking an item in the box.

To add a new action click the Add new button and enter the details for the various steps and then click

the Save button.

To delete an action select the action and then click the Delete button. You cannot delete an action if it is assigned to an alarm.

The main panel of the form displays a list of all alarms in the system. To view the action currently assigned to an alarm click the alarm.

To assign an action to an alarm, click the desired alarm and then select the desired action and click the Set as action button.

To delete an action from an alarm, select the alarm and then click the Clear action button.

12.6 CCTV locations

Define the location of CCTV cameras, communication port and video card driver.
Interfaces to **Pacom** CCTV system.
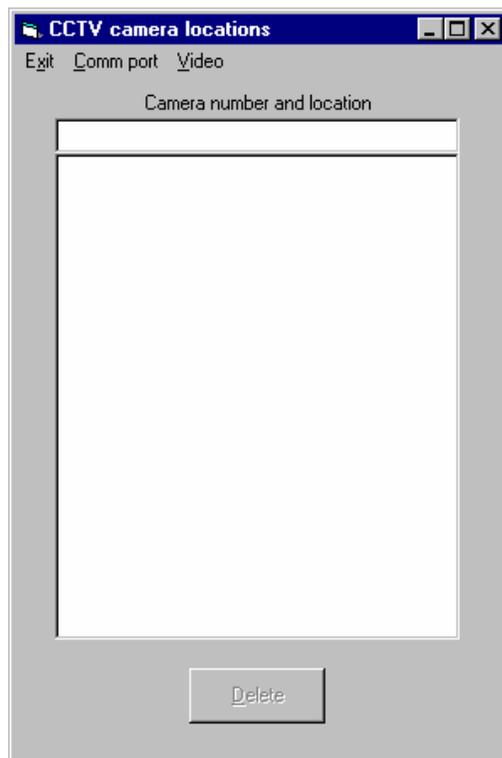
13 Disable cards

Allows the global disabling and enabling of ALL cards. Only available at administrator level.

14 TCP/IP Configuration

14.1 Server – Client Setup

The Access system can be networked using PCs running Windows 9x or Windows NT4 (service pack 3 or greater) fitted with Ethernet cards and configured with standard Microsoft TCI/IP protocol . Each PC must have an individual IP address and sub-mask; not the automatic selection. The IP address and sub-mask is allocated by the system network administrator. If this is a small network which has been established for the Access system then this information may not exist.

To establish a small, self-contained network we recommend an IP address of 192.168.100.n where n is a separate number for each computer. This IP address is one of a number set aside internationally for internal networks not connected to the Internet under the RFC 1918 recommendations. The sub-net mask would be 255.255.255.0. If TCP/IP is not installed on the computers then it would be advisable to have a qualified person to install and configure the networking system.

Once the TCP/IP protocol has been installed, the Facility software can be installed on each machine that is to access the Access system. Each PC must be individually registered by forwarding the registration form to Sphere Systems. PC registration numbers apply only to the PC for which it is generated.

The directory where facility is installed on the server machine is to be shared with full control access and each client must map this directory as a local drive.

Check that the server program (facserv32.exe) exists in the Facility Security directory. The directory "Facility Security" is expected to be located in c:\Program Files.

14.2 Option 1 – PC Server - DP11 connected to server

This is the recommended installation option.

- From the Comms -> Communications menu select Single RS485 Tick box Value.

- Tick the TCP/IP connect Box.

- Insert the server IP address.

- Do not tick the client box as the PC is being setup as the Server.

- Select the Database Path button and select – open the security.mdb file in the server PC facility security directory.

    This will open the TCP/IP connection window.

This will open the TCP/IP connection window.
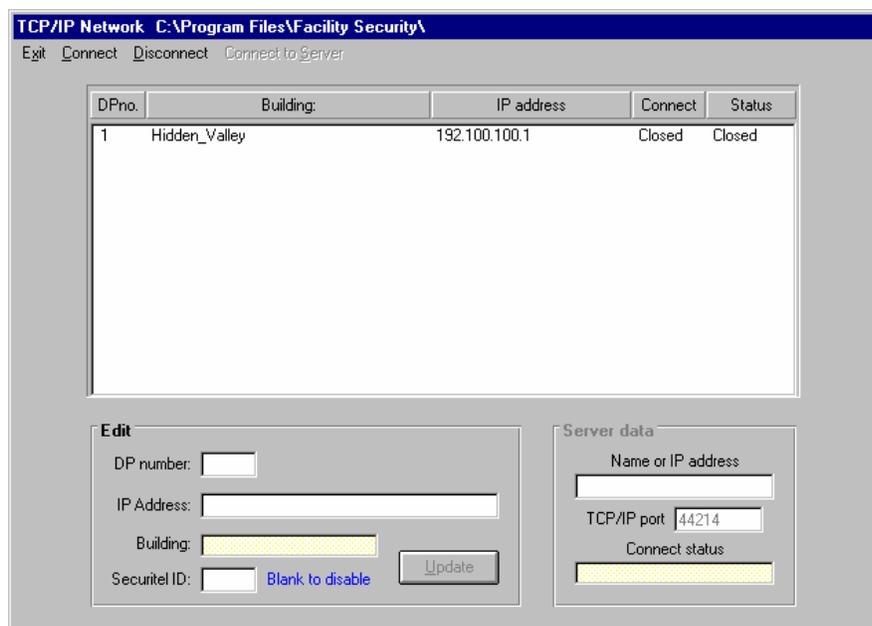
Each DP11 is to have its respective PC's TCPIP address entered

- After completing the entries exit from the screen and the communication details screen.

- Close the program down so as to save the new settings and the re-start.

- The system will then automatically start a program called facserve32 is the PC is set as a server

14.3 Configuring facserv32

These changes will cause the facserv32 TCP/IP program to start automatically when Security is launched. When facserv32 starts for the first time, it is necessary to configure it to use the correct communication port. Click on the DP11 Server entry on the Start bar to restore the facserv32 window. Select the correct communication port that is used by the DP11 (Doorcom) is attached and click Select Port.

Other facser32 configuration settings and information windows
Active sockets, TCP/IP address
Queue
Net timeout – this defaults to 5 seconds to accommodate delays over busy TCP/IP networks. It may need to be longer under some circumstances. If Facility Security reports network errors or doorcoms off-line, increase the net timeout value.
Transactions
Last TCP/IP Error
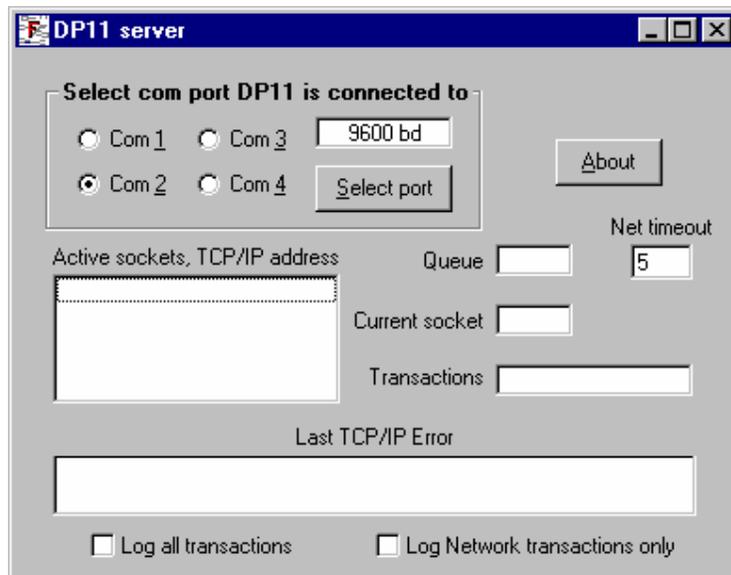Log all transactions
Log Network transactions only
Baud Rate – the Baud rate displays the current communication rate between the PC and the DP11. This is normally 9600 Baud for non-TCP/IP operation and 19200 Baud for TCP/IP operation.

- Close (do not just minimise) facserv32.

- Close Security.

- Restart Security again and facserve32 should automatically start and Security go on line as a TCP/IP Server.

Facserv32 if maximised will indicate a IP connection.

14.4 Option 2 –Client PC - DP11 connected to server

Client Connections.

Start Security on the server   PC as an Administrator.
Under Comms -> Remote
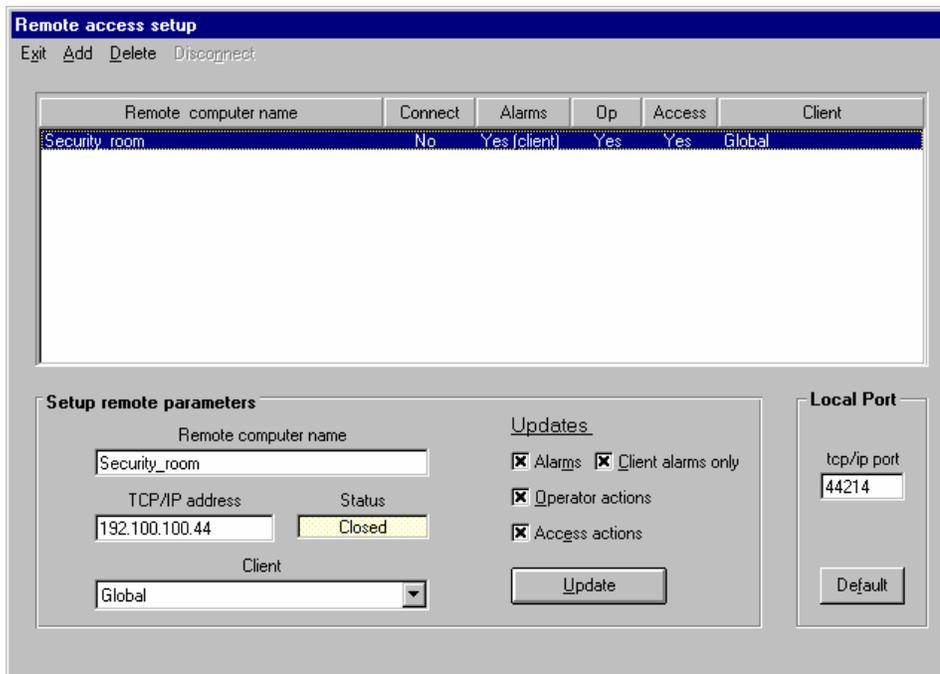
Enter the proposed client PC TCP/IP details and update data request. This is the server client permission's list and a client PC will be refused connection unless it appears in this table.

- Start the Client PC Security program
- From the Comms -> Communications menu select TCP/IP Tick box Value
- Tick the client box .
- When the Client is selected a box will appear requesting the Server Nane or IP address.
- Select the Database Path button and select – open the security.mdb file in the server PC facility security directory.

  This will open the TCP/IP connection window.

Each DP11 is to have its respective PC's TCPIP address entered

After completing the entries exit from the screen and the communication details screen.

Close the program down so as to save the new settings and then re-start Security.

Go to the TCP/IP form and click on the connect entry on the top line. An OPEN status should appear instead of the closed statements. This may not work the first time and under these circumstances exit the TCP/IP form, close facility down to save the new settings. Restart Security and go to the TCP/IP form and click on the DP11 entry the select connect. An OPEN status should appear against the Connect and Status columns.
Exit from this form and go On-Line

TCP/IP Client should be displayed on the bottom status line.
Any number of Client PC can be connected at once and will show any updated information entered from any other PC.

15 RS485 Communications

15.1 Introduction

The RS485 communications standard has been widely adopted for network communications in industrial and scientific applications. It is a very robust system when installed correctly. There are constraints which must be observed during installation to ensure satisfactory network performance. This document describes how to install an RS485 network.

15.2 Cabling

15.2.1 Cabling Specifications

RS485 communication cable is a constant impedance, shielded, twisted pair cable. Many cable manufacturers supply cable meeting the RS485 standard. The characteristic impedance is generally close to 120 Ohms although other impedances are sometimes available. The lower impedance limit is set by the drive capability of the RS485 chips. The driver chips used by Sphere are sourced from Maxim, National Semiconductor and Texas Instruments (SN75176/DS75176) and can drive impedances down to approximately 50ohms
Other cabling media such as telephone cable, coaxial cable and non-constant impedance cables such as shielded wire, multi-core wires, building wire and wet string will prove problematical and not provide satisfactory performance.

A typical cable specification is:

1. Cable Code	DCK4702
2. Cable Description	2 pair 7/0.2tcw (24AWG) polyethylene insulated aluminium polyester tape screened including a 7/0.2 TCW drain. TCW braided PVC sheathed. EIS RS485 Data Cable. Low voltage, not for mains connection.
3. Construction	
3.1 Conductor	7 strands of 0.2mm tinned annealed copper to AS1125, drawn from Class 11A "Electrolytic tough pitch copper" to AS 1574. Max DC conductor resistance at 20C 89.0 Ω/km
3.2 Insulation	Coloured polyethylene to AS1049 Nominal Diameter 1.7mm Nominal Wall 0.5mm
3.3 Lay Up	2 pairs twisted PAIR 1 Black + White PAIR 2 Red + Green
3.4 Screen	Aluminium/Polyester tape over layup plus 7/0.2 TCW Drain
3.4 Braid	Tinned annealed copper wire braid to 80% cover
3.5 Sheath	Coloured 4V75 PVC to AS3191 Nominal diameter 7.0mm Nominal wall 0.76mm
3.6 Typical Electrical Properties	Nominal impedance 120Ω Nominal capacitance 42pF/m cond to cond Velocity of Propagation 66%

This cable is manufactured by Tycab and distributed by AIM.

15.2.2 Topology

RS485 allows multiple network nodes to be connected to a single cable. The cable must be installed to pass close by each node. Stubs (cables joining the node to the cable) or stars (multiple cable segments brought back to a single point) are not permitted.

If stubs or stars are required then a repeater must be installed to drive the stub or star segment.

15.2.3 Cable Length

The maximum length of a single cable run is 1200 metres.

15.2.4 Termination

The cable must be terminated at each end with a terminating resistor equal to the characteristic impedance of the cable. This is to prevent reflections which would disrupt communications. A cable with a 120 Ohm characteristic impedance must have a 120 Ohm resistor at each end. A power rating of ¼ Watt is adequate. The terminating resistors should be carbon composition or carbon or metal film. Wire-wound resistors have substantial inductance and should not be used.

The characteristic impedance of the cable is published by the cable manufacturer as part of the cable specifications.

15.3 Repeaters

Sphere supplies repeater types for different applications.

The standard repeater is used to connect to a stub or to extend cable length

An optically-isolated repeater is used to maintain electrical isolation between cable runs in separate buildings. Note: Electrical isolation is required where separate MEN grounds are installed but are desirable for any data link between buildings.

15.4 Cable Isolation

The communication cable must not be run in cable trays carrying power wiring nor in close proximity to power wiring. Current surges in power wiring due to high equipment starting currents or to faults can disrupt communications and may cause damage to Sphere equipment.

15.5 Ground and Earth Connections

The grounding and earthing connections in RS485 provide two separate functions. The first is related to safety and the second to establish a reference voltage.

15.6 Safety

The RS485 cable screen must be bonded to the protective earth system of a building at one point only. The cable screen must be electrically continuous throughout the entire cable run.

15.7 Voltage Reference

The screen of the RS485 cable establishes a ground reference voltage for the RS485 signal conductors. For this reason the cable shield must be connected to the ground reference for each node on the network.

It is not acceptable practice to tie the node ground reference to the building protective earth as this will introduce electrical noise into the system and may lead to equipment damage in the event of electrical fault currents.

15.8 Installation throughout Multiple Buildings

There are two separate installation procedures depending on the type of electrical earthing system.

15.8.1 MEN System at one building
In this case the installation may be made as though it exists in a single building. The cable shield will be continuous throughout the installation.

15.8.2 MEN System in each building
In this case there must be electrical isolation between buildings with different MEN systems. Each building is wired as a separate and complete installation with the cable shield tied to the building protective earth at one point.
Optically isolated repeaters or optical fibre must be used to connect the communications network between buildings.

15.9 Wiring Details

Figure 1 shows how the RS485 network should be wired between various network nodes. The essential features to note are:
1. All the cable shields are tied together and are tied to a Ground connection (GD or Shield) on EACH node. Without the cable shield connected there will be no ground reference voltage established for the RS485 drivers and receivers. Reliable communications will not be achieved.
2. The cable shield is connected to a building protective earth at ONE POINT. Any point along the shielded cable can be used to attach this protective earth. This earthing is required to ensure that the network cabling cannot float to dangerous voltages.
3. The DP11, or in fact any other node, can be connected at any point along the cable. It does not need to be at one end.
4. Termination resistors must be connected at each end of the cable. The nominal resistance is 120Ω. These resistors make it appear that the cable continues indefinitely and hence eliminate reflections from the end of the cable. These resistors can be ¼ or ½ Watt resistors.
5. The polarity of the cable is important. For ease of installation and maintenance it is recommended that a consistent colour code be adopted throughout the network. An acceptable scheme may be Blur for COM- and White for COM+.
6. Beyond any repeater the cable must be 2-pair with one pair connecting the COM terminals and the second pair connecting the TRX terminals. In figure 2 the 2-pair cable as shown as fatter lines
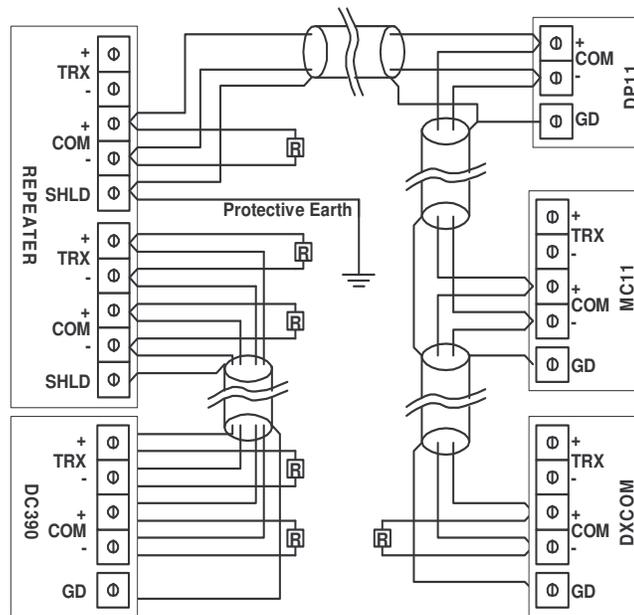
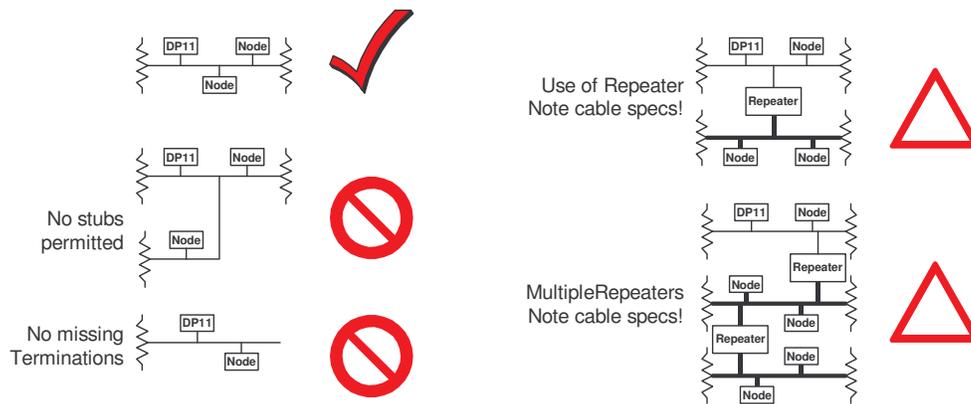Figure 1 Wiring Details for RS485 Network

Figure 2 RS 485 Cabling Topologies

15.10 References

TIA/EIA-485 ELECTRICAL CHARACTERISTICS OF GENERATORS & RECEIVERS FOR USE IN BALANCED DIGITAL MULTIPOINT SYSTEMS (http://global.ihs.com/)
AUSTEL Customer Premises Cabling Manual. (http://www.standards.com.au/)

16 System Backups

16.1 Backing up Facility Security

Backups are extremely important. Please read the following information very carefully and if you do not understand the procedures described, call Sphere Systems support for assistance.

Backups should be stored remotely from the live data. Ideally backups should be stored off site. Multiple copies of backups are recommended with each copy stored in a separate place. The physical security of backups is important as backup files can be read by Access, giving the bad guys sensitive and useful information if they can get the backup files. Backup media is also prone to physical damage and must be stored in locations where they will not be damaged by heat, fire(!), water or other influences. It is very desirable to regularly read the backups to ensure that they are readable and will allow the data to be recovered.

In the event of data loss it is unlikely that Sphere Systems can help very much in recovering data. Any files we have will not be current.

Although Microsoft promote Access as a multi-user database, it appears that the database cannot be backed-up unless all remote users have disconnected. This requirement presents an operational problem for multi-user sites as it means that all clients must disconnect to allow backups to be performed. It appears that the database can be copied and this copy will probably be OK, but the chance exists that the copy took place at a time when the database was being updated by the Jet engine and is in an inconsistent state. It is recommended that a periodic time be established when clients disconnect briefly to allow a backup to be initiated at the server. These backups should be carried out on a regular basis dependent upon the importance of the data.

16.2 Security.mdb Backups

The security.mdb file is critical to the operation of the system. It contain the total configuration of the system and if this is lost all data for the entire site will need to be re-entered manually. This includes but is not limited to the card data stored for each person, access rights to all doors and all time schedules. **TREAT THIS FILE AS MISSION CRITICAL.**

When the server is started it will attempt to create a backup of the security.mdb file which will be called security.bak. This may fail due to Microsoft Access prohibiting the operation. The reason will be displayed in a dialog box. The most likely reason is that client programs are still connected to the Access database. To successfully perform the backup, all client programs must disconnect from the Access database. This is achieved by closing all client programs.

If security.bak exists in the same directory as the security.mdb file, the creation of a new backup will not take place. Thus when a security.bak file is created it should be moved to a backup directory and renamed in a way which will facilitate recovery.

16.3 Sechist.mdb Backups

Automatic backups of this file can be enabled through the System->Options Setup tab, check box Backup database each month. The backup file is called secmmmyy.mdb, where mmm is the previous month in the format jan, feb etc, and yy is the least significant two digits of the year.
If this box is checked when the server is started, a dialog box asking for backup confirmation will be displayed under the following circumstances:

it is the first day of the month, or
a backup for the previous month does not exist and it is later than the seventh day of the month.

If the backup is requested, the security.mdb file will copied to the backup file. All data for the previous month is deleted from the security.mdb file. A dialog will be displayed indicating success or failure of the backup operation.

Note: Due to undocumented features of Microsoft Access, it is not recommended that the automatic backup mechanism be relied upon for backing up your database when your site has client connections.

16.4 Manual Backups

All clients and the server must be shut down so that no active connections to the access databases exist. It is recommended that a time each week or each month be nominated where all clients are disconnected to enable the backups to take place. The following files must then be copied manually to a backup directory, assigning names that facilitate data recovery:

Database and history files:
security.mdb   (main configuration database)
group.mdb   (remote dial-out database)
sechist.mdb   (card access history)
alarm.txt   (alarm history) a text backup file of the alarm history

        SECMmmyy.mdb   (Monthly history database)
        Mmm = month in for Jan, Feb etc)
        yy = year

The alarm.txt and the sechist.mdb files are recreated automatically if they do not exist

16.5 Invalid Database Format Messages

A feature of Access is its ability to track proper closure of the database file. When Access (or the Jet engine) closes a file it sets a bit indicating proper shutdown. An improper shutdown could be caused by an operating system crash or the power failing. When it attempts to open database Access checks this bit.

If the data base was previously shut down correctly then the open proceeds and the bit is cleared.

If on opening the bit is clear, it is interpreted as an improper shutdown and Access reports this as "Invalid Database Format". This does not indicate that the database has been corrupted (although if the shutdown occurred during a critical database updating phase it may be) and can usually be corrected by using the Access Repair Database tool.

16.6 Database Access with version of Microsoft Access other than 97.

The database file created and manipulated by the Facility Security server and client programs use a version of the Jet database engine which is **ONLY** compatible with Access 97. If later versions of Access are used to open the database files the files will be converted and **WILL NO LONGER BE USEABLE** by Facility Security. This behaviour is a feature of updating Microsoft applications and is out of our control. Once a database file has been updated it probably cannot be reconverted back to the original format. In any case, we do not know how to do it and we do not maintain several versions of

Microsoft Access to allow us to even look at the problem. Our advise is "**DO NOT DO IT**". If you accidentally upgrade a database file your only recourse is to reload your data from a backup file.