Access Control System

Capabilities & Outline Proposal

20-26 High Street | Greenhithe | KENT | DA9 9NN | United Kingdom | Tel +44 (0) 1322 370777 | Fax +44 (0) 1322 370076 | www.xplan.com

Contents

INTRODUCTION **4**

The PLAN system **4**

References **5**

WINPLAN-640 ACCESS CONTROL/ALARM MONITORING SYSTEM **5**

Access Control - General System Description **5**
System Architecture 5
Operation of a Card Controlled Door (Gate/Turnstile/Vehicle Barrier) 6
Optional Asset Protection 6

System Features - Detailed Description **7**
Field Equipment Status Monitoring 7
Redundant Path Communications Module 7
Programming and Operation 8
Operator Log-on Security 8
Remote Locking Facility 8
Event Mask 8
Guard Tour 9
Reporting and listing facilities 9
The Event Monitor Screen 9
Roll Call Listing 10
IN-OUT status panel 10
Quick Search 11
History Analysis 12
Audit Trail 13
Enhanced Time Keeping listing options… 14
General Staff management reports… 16
General Database listing features 19
Anti-Passback 19
General System & Extended Alarms 19
MS Windows 2000 20

Remote Site Networking **20**
Direct Connection. 20
PSTN Dial-up Connection. 20
Leased Line Connection. 21
Existing Client Multiplexor 21
Existing Client :LAN/WAN 21
Other options… 22

Operator Training **22**
Typical Training Schedule 22

WinPLAN-640 Access Control System Data **23**

Integrated PLAN-640 Photo-ID Software **27**
General Description 27

WinPLAN Virtual Control Room Software **28**

General Description 28

VisiPLAN Visitor ID badging and registration software 29
General Description 29

Access Control System - Equipment overview 29
Central Control Equipment 29
Optional PLAN-640 Administration Workstation (ID Badging Station) 30
ILS-400 Intelligent Loop Supervisor 30
Field Control Equipment 31
Microprocessor Controlled Field Panels - PLAN-400's 31
Enclosures 31
PSU's 31
Card Reading Equipment. 32
Locking Equipment 32
Break Glass Units 32
Fire Alarm Door Override Input 32
EMC 33
BS EN 50133- part 1 33

Introduction

This document contains an outline specification and overview for an integrated Access Control, Alarm Monitoring & Security Management System based on the PLAN range products. Once deployed, such a scheme will offer the benefit of a flexible solution - expandable to meet the future local and wide area needs of almost any size of organisation, without compromising the integrity or simplicity of the system in the process.

The PLAN system

The PLAN range of Access Control equipment is a UK manufactured range of products aimed at the large scale, high security requirements of major European corporate, educational and financial institutions. The system was launched in 1987 to meet the specific needs of the security industry for a high integrity (fully distributed intelligence) system with technical support in the UK.

Due to its integrity and resilience, the system has been implemented in a wide range of applications in HQ buildings, cash and data centres within the Banking arena. However, in today's demanding and competitive security systems marketplace, the PLAN product range takes it's place as a high end product suited to the 'large scale' enterprise-wide needs of leading companies across all commercial sectors.

The PLAN system is appropriate for any application where an organisation has one or a number of mission critical facilities to secure.

<u>Key features of the proposed system are;-</u>

Integrated Photo-ID Badging capability.

Real Time Event and Alarm Monitoring.

Multiple Workstation/Multi-Site administration.

Asset Tagging and Surveillance Facility.

Fully Auditable Password Protection for Software features.

Extensive Transaction Analysis.

Real Time Guard Tour Processing.

Remote Locking Control.

Graphical Alarm Display and Touch Screen Integration.

Automated Visitor Badging.

Distributed Intelligence.

Anti-Passback (local 'True' and Global).

Support for multiple reader technologies.

Personnel Tracking Facility.

‘VisiPLAN’ Visitor registration and Badging

Roll Call Listing (inc. automatic printing).

WinShifts T&A Processing.

Multiple Printer support.

References

The PLAN product range has one of the most impressive client lists in the security business – PLAN systems have been deployed in over 15% of companies listed in the FTSE100. As a supplier of a leading 'large scale' access control system, we are confident that we will have no problems providing any necessary references, however, we respect the confidentiality of our customer contacts and propose to submit a list of client references - on request - if the PLAN product selected to proceed to the next stage of the selection process.

WinPLAN-640 Access Control/Alarm Monitoring System

Access Control - General System Description

The PLAN640 Access Control System is a programmable Windows based (Win'95-98, NT4.0, Win2K or XPpro) fully featured high integrity distributed intelligence Card Access System - the primary purpose of which is to control and record (for future analysis) the movement of personnel around the site. This will be achieved using a network of up to 1024 xPLAN400 distributed intelligence access control units connected to up to 4,096 proximity card readers (fitted adjacent to each controlled door, gate or turnstile). To gain access through a restricted door, the system will require an authorised card (or optionally Card + PIN) to be presented to a reader and validated by the local controller.

The system is modular in design and can be expanded by the addition of extra field panels or software modules.

System Architecture

The Control System shall comprise of a WinPLAN-640 CCU complete with optional Graphics Display (WinPLAN Virtual Control Room Software) located the nominated security control room. An Intelligent Loop Supervisor (ILS400) will provide the link between the Central Control Unit and the xPLAN-400 local controllers.

Additional WinPLAN640 admin. PC's can be provided to provide general day to day administration facilities at a number of separate locations. These PC's will be connected to the 'main' system in the Security Room by means of an Ethernet network utilising an industry standard network protocol (TCP/IP). This network connection will make use of the existing client Local/Wide Area Network and/or a dedicated security LAN.

The xPLAN-400 "Distributed Intelligence" local controllers ensure that the integrity of the installed system is maintained even if the central control unit (CCU) is unable to communicate with its network.

The system has the capacity to monitor alarm inputs from third party equipment (such as Door contacts, Perimeter detection, PIR's etc.) by use of the 16 supervised alarm inputs provided within each xPLAN400.

Up to four readers are connected to each PLAN400 control unit, which will report events via the communications network to the CCU. When a PLAN-400 local control unit detects an event, such as a card read or alarm, the controller sends a message to the PLAN-640 CCU which then displays an event message or alarm indication - in the latter case, the operator uses the facilities of the PLAN-640 software to assess the cause of the alarm and to acknowledge it.

Operation of a Card Controlled Door (Gate/Turnstile/Vehicle Barrier)

Operation of the access control system from a users point of view shall require them to perform the following sequence of events:-

1) A card is presented to the access control reader by placing the card within the detection range of the reader. If the card is invalid the system will generate an "Invalid Card" message at the CCU and the Reader LED will stay Red.

2) If the card is valid the system will unlock the door and start the programmable door unlock timer. The reader will display a Green LED for the duration of the unlock time. The time required to unlock the door from the time when the card is read shall normally be less than 0.1 seconds.

3) If the unlock time expires before the door is opened the system shall re-lock the door.

4) When the door is opened, a programmable door open timer should start. If the timer expires before the door is closed the system shall also generate a "Door Open" alarm.

Note 1:- If a door is opened without a valid access or exit request a "Door Open" alarm should be generated. The alarm can be set to clear when the door is closed or latch until an alarm acknowledgment code is entered at the CCU.

Note 2:- Where Card plus PIN readers are installed the card holder will be prompted to enter their PIN at the appropriate time.

Note 3:- The PLAN system is compatible with the majority of available Biometric Verification options. In this case, after a valid card is swiped, the user must scan their finger/palm/iris before the door will be released.

Optional Asset Protection

The PLAN system features and advanced level of Asset protection utilising a dedicated version of the xPLAN400 panel - developed specifically for this purpose. This solution benefits significantly over competitive systems which do not have the advantage of an embedded asset controller which allows the local verification of Assets with any of their allocated owners (up to 16 owners per asset) instantaneously with no PC or central control involvement.

Effective Asset tracking requires a reading technology which is capable of detecting multiple cards, on the move, at long range. PLAN system users can elect to use long range readers throughout their organisation, or only at building exit points.

By adding the P103-TC2 and TC3 uniquely coded asset tags to high value (or mission critical) equipment, the Access Control System can be used to track these assets as they move around and between protected buildings.

'Asset Matching' is a technique which allows tagged equipment to be 'owned' by selected Staff and verified dynamically as both Asset and Owner pass through the detection zone.

Uniquely, the PLAN-400ax, 4-port, Asset Matching controller provides high speed, dynamic processing, of both Asset and Personnel Tags for system managers who want to give teeth to their passive (paper based) Asset Tracking Systems.

In operation, whenever an asset is detected, the system interrogates a 2½ second 'cache' memory to establish whether an authorised carrier for this asset has been seen at the reader. At this point, regardless of the search results, the controller raises an 'asset detected' warning at the panel and at the PLAN-640 main P.C. If an owner for this asset has been seen at this reader within the 2½ seconds, then an asset verified status will be sent to the PC and the Asset Detected indication will be cleared. If no owner has matched the asset after the time delay, then an Asset Alarm will be indicated at the Panel and reported to the PC.

The asset detected signal can be used to prime third party equipment for an alarm, (by panning cameras into place) or to discreetly alert nearby staff to the fact that an asset is in the detection zone. If the situation develops into a full Asset Alarm, the output can be used to close doors, sound an alert or enable video monitoring/recording of the incident.

Because of the dedicated mode of operation for these panels, up to 48 Tags within the detection area can be processed simultaneously.

System Features - Detailed Description

Field Equipment Status Monitoring

The PLAN-640 CCU will supervise the communications network - which can support an unlimited number of card records, 4,096 access control readers and 16,000 additional alarm inputs, with the option to expand (by the addition further network supervisor units and field equipment). The system features continuous polling of the field panels to ensure notification in the event of a network cable break.

The central processor will monitor the health of the field panels and report failures immediately upon detection as system alarms. Detectable failures include - Alarm polling response failure, Event Message failures, and failure of the local watch dog health checks by the PLAN-400's.

If a PLAN-400 field panel fails to respond to polling messages sent by the CCU, a communications error message is displayed on the Event monitor screen to indicate which outstation has failed to respond.

The PLAN-640 CCU polls the network for any reader/alarm events and stores these on the system hard disk for future transaction analysis.

Redundant Path Communications Module

For additional network integrity the PLAN400's can be cabled in a redundant path configuration. Using the xPLAN400 redundant path communications module (RPC) in the event of a cable break or short circuit, the system will automatically negotiate a healthy return path back to the WinPLAN640 in the event of a cable break.

Furthermore, using the RPC module, the system will display an alarm message which will indicate where the cable fault has occurred and panel. An attending engineer will proceed directly to the panels connected to the faulty cable, where the system will provide additional diagnostic information such as whether the fault is an open or short circuit. Despite the fault(s), the system will maintain full communications function whilst the problem is investigated and repaired.

Programming and Operation

All programming operations can be carried out using the WinPLAN-640 software at the PLAN-640 CCU (or at one of the optional networked Admin. PC's). The software is designed so that day to day operation does not require the user to be familiar with computers. Selection of menu options is controlled by a single 'click' using a mouse and field data is, as far as possible, selected from pre-defined drop-down lists - with the QWERTY keys used only for logging on to the system and for the entry of free text information.

Password controlled menu access to the editing functions is restricted to those options defined within the operators individual password record (see below). For clarity, when a new user logs in to the system, they will only be presented with the options in each editor, for which they have authority. For example, if an operator has no 'editing' rights in card records, then the 'Edit' button is removed from view when the menu option is accessed.

Operator Log-on Security

Using the Password Editor, each operator is given a unique User ID/Name and Password which will identify him/her to the system when logging on. The system is capable of identifying 64 different operators each of which will have his/her own record in the system database. Each record will identify to what level the user is authorised & will only allow editing in pre-selected areas of the software.

For maximum integrity, each operator, regardless of their level of authority, is able to change their own password on an ad-hoc basis. A dedicated 'button' is used for this to eliminate the need to give 'limited' access to the actual password editor where additional information may be seen.

Remote Locking Facility

The Remote Locking facility will allow an operator with an authorised password to remotely control an individual door, e.g. toggle between- Locked (No Access or Egress), Unlocked (Free Access, No Alarms) or Normal (Valid Card Only). Also, in the event of a security alert or similar emergency, the operator is able to Open or Lock all doors (or pre-selected groups) at once with a simple key combination.

Note: when a door is set to "Locked" mode all functions for that door are disabled except emergency exit.

Event Mask

All events detected by the field equipment will be reported to the WinPLAN640 CCU. However, an Event Mask facility is provided to filter the messages reported in real time to the event monitor screen to only those of specific interest to the operators e.g. Alarm data and Card Read exceptions (cards used outside of allowed areas/time etc). This, password controlled,

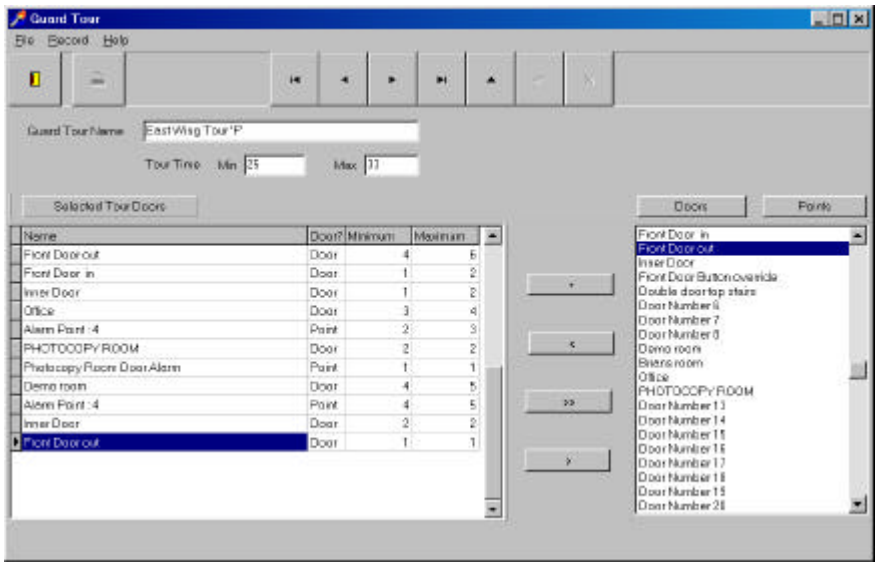
facility is accessed from the Event Monitor Commands menu, where the operator will be prompted to select the types of event to be masked.

Note: Events which are masked from real-time view, will still be recorded and displayed in subsequent History reporting.

Guard Tour

Up to 64 user defined guard tours can be defined using the guard tour editor. Each tour can feature up to 256 'way-points' which must be visited within the minimum and maximum times allowed by the tour definition. An exception will be generated in real time if a guard takes too long between way points or visits a point out of sequence.

A typical tour is shown below…



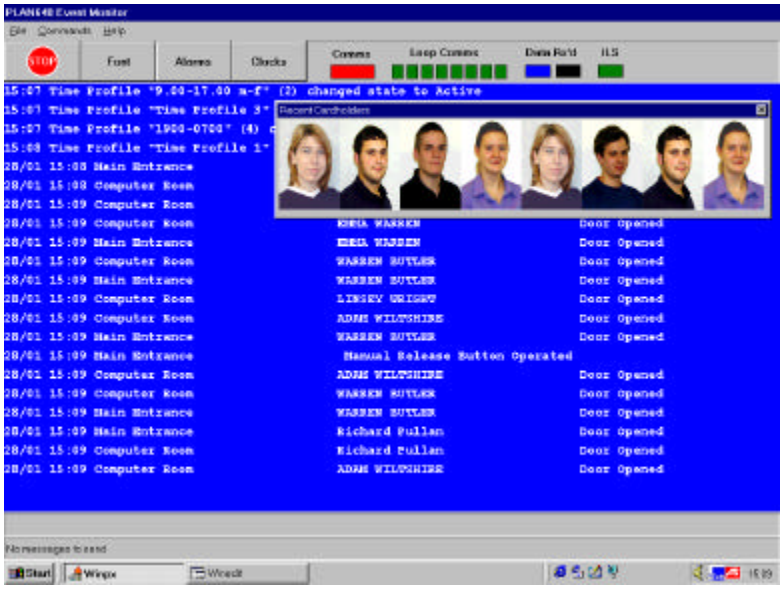
It can be seen above that both alarm points and card readers can be set up as way points… this means that PIR's and door contacts that fall on the rout of the tour can be programmed as well as card readers.

For additional security, tours can be activated by a tour scheduler which can be set up to randomly select from groups of similar tours at the set times.

Reporting and listing facilities

The Event Monitor Screen

The WinPLAN640 Event Monitor Screen comprises a full screen display of all events as they occur. In addition to the scrolling display of card reads and textual alarm and system data, the event monitor screen supports a thumbnail viewer for the display of cardholder images as cards are read.



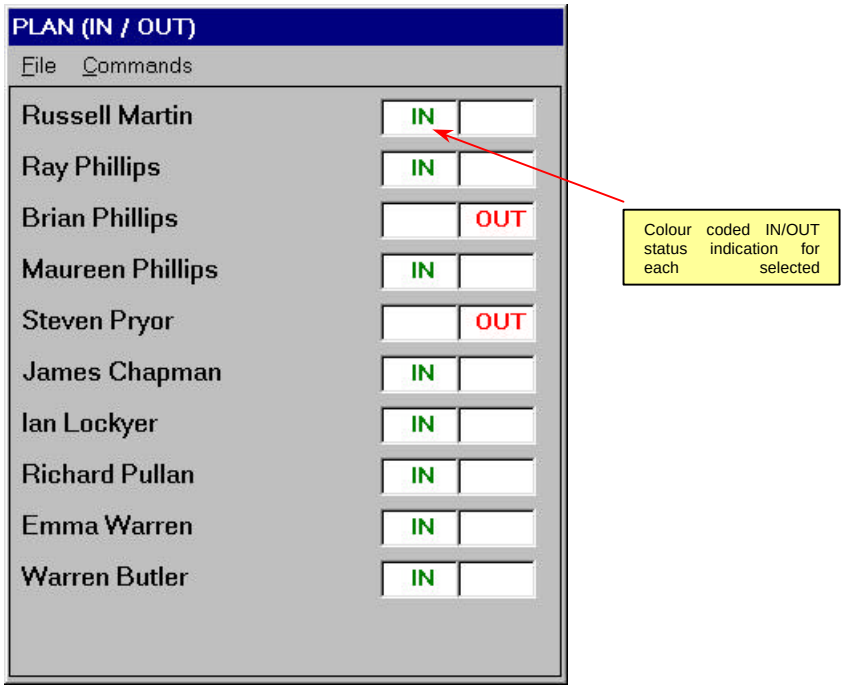
For the busiest sites, an Event Mask facility is provided to filter the messages reported in real time to the event monitor screen to only those of specific interest to the operators e.g. Alarm data and Card Read exceptions (e.g. cards used outside of allowed areas/times etc). Events that are masked from real-time view, will still be recorded and displayed in subsequent History reporting.

Roll Call Listing

A roll call feature is provided to allow, in the event of an emergency, a list of every card holder still inside the building. Listings can be sorted by Name, Card No., or any of the user defined fields as the search/sort criteria. For ease of distribution to a number of muster/assembly locations, the system will allow listings to be optionally set to include a page break between each 'group'. A Roll call can be automatically started on an external trigger event (such as a Fire Alarm) and directed to a dedicated printer.

IN-OUT status panel

The PLAN system ‘IN-OUT status panel’ allows the operator to select a list of key staff (such as ‘First-aiders’, ‘Fire Marshals’ or Managers) for who it is critical that attendance (or not) can easily be identified. Furthermore, a minimum ‘safe’ level for each type of staff can be set. When the number of staff belonging to the target group reaches the minimum value, a warning message is displayed… For example, on a site where the company safety policy states that there shall never be less than 3 First-aiders available, a warning can be set to alert site management as soon as the number reaches the minimum level.



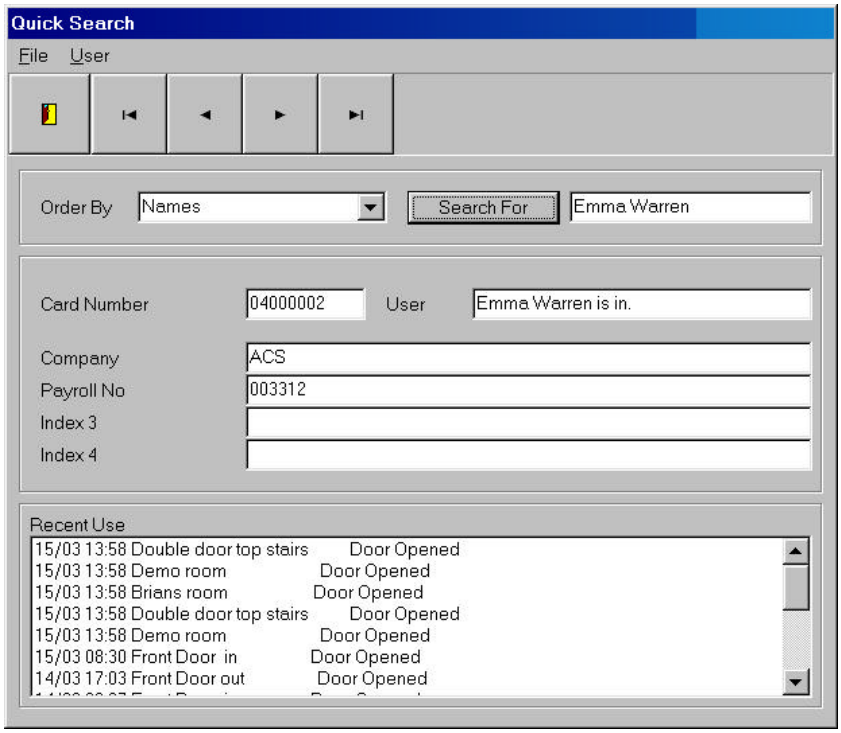
Quick Search

Using the "Quick Search" facility it is easy to locate any member of staff within the building and to indicate their last known position. The information displayed includes; the cardholders name followed by their current status (IN or OUT), as well as selected fields from their personal card record. In addition, a scrolling list of the last 16 events for that card is displayed.

This utility is particularly useful to telephone and visitor reception staff alike, who require the combined ability to locate a member of staff and to be presented with personal details about the person they are looking for.

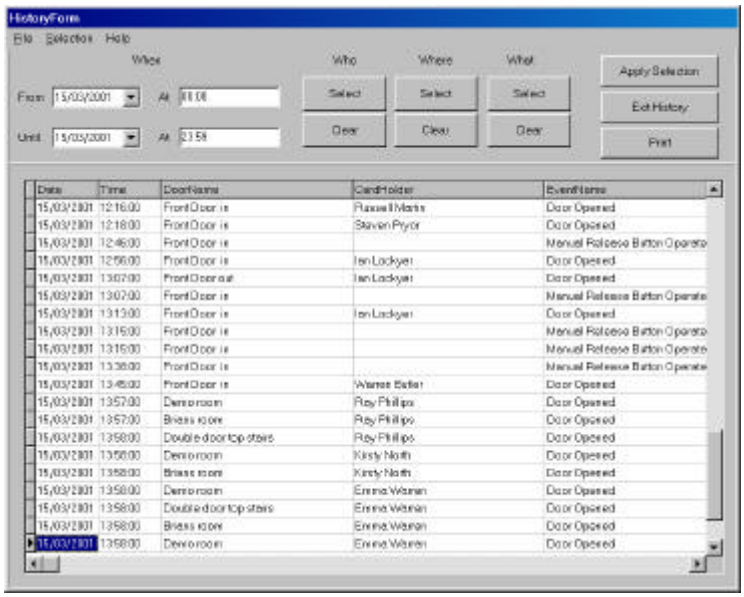
For example, a caller may simply request ‘extension 1234’. In this case, the operator can perform a quick search for the specified extension number and respond to the caller with the exact whereabouts of the named member of staff. The ability to present an operator with additional details about the searched for person, (such as ‘Sales department’) will allow them to offer an alternative representative if the requested person is not available.

The record below shows a typical Quick search display…

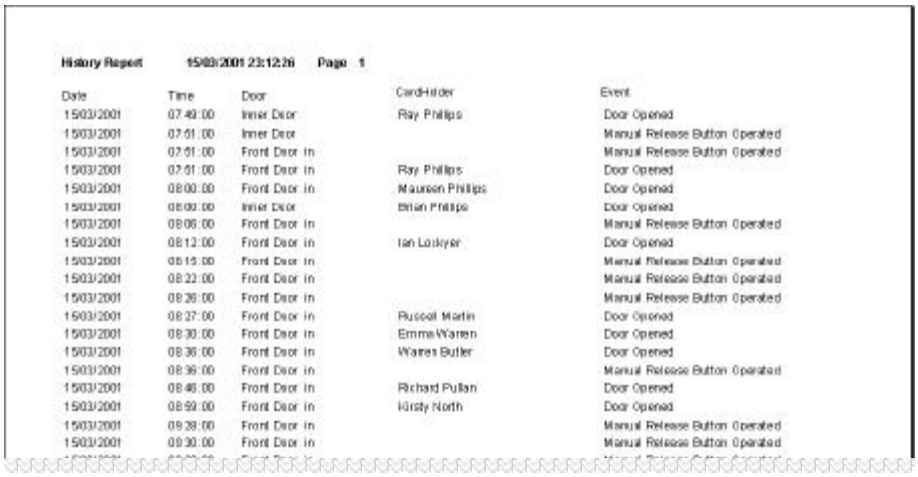


History Analysis

The History analysis feature allows a suitably authorised operator to create on screen or printed listing report which include past events on the system. For speed of operation and ease of use the PLAN system History analysis feature uses 'point and click' selection of the information which is to be included in the report. Operators are able to specify 'When', 'What', 'Where' and 'Who' should be included in the listing. All of these can be selected from lists accessible from within the History analysis screen (as shown below).



As can be seen above, the history editor screen allows the operator to 'preview' the listing before committing to the printer. When the Print Button is selected, a printed report as shown below is generated.



History Report 15/03/2001 23:12:26 Page 1

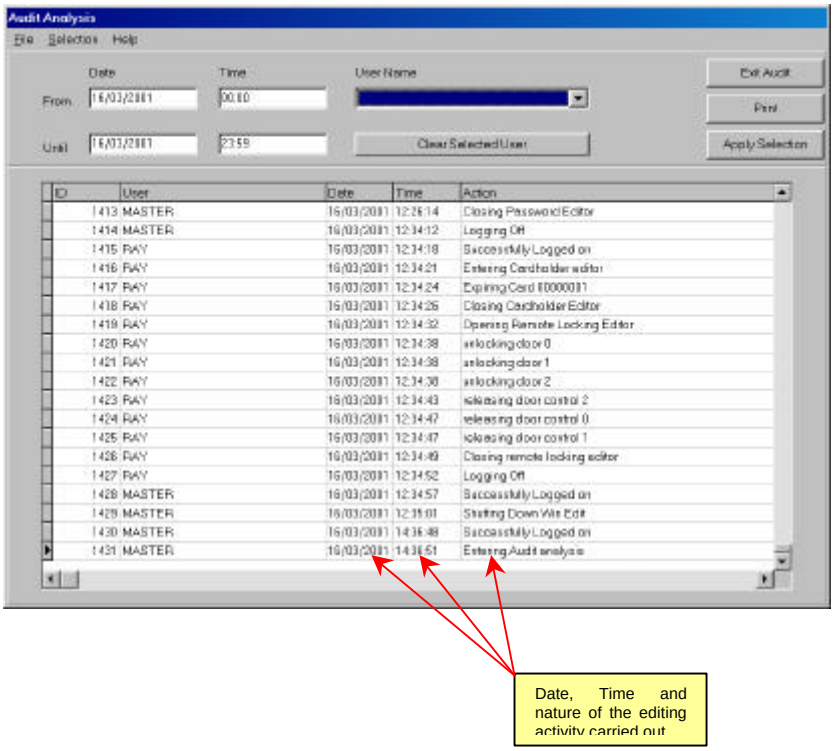
Date	Time	Door	CardHolder	Event
15/03/2001	07:49:00	Inner Door	Ray Phillips	Door Opened
15/03/2001	07:51:00	Inner Door		Manual Release Button Operated
15/03/2001	07:51:00	Front Door In		Manual Release Button Operated
15/03/2001	07:51:00	Front Door In	Ray Phillips	Door Opened
15/03/2001	08:00:00	Front Door In	Maureen Phillips	Door Opened
15/03/2001	08:00:00	Inner Door	Brian Phillips	Door Opened
15/03/2001	08:06:00	Front Door In		Manual Release Button Operated
15/03/2001	08:12:00	Front Door In	Ian Lockyer	Door Opened
15/03/2001	08:15:00	Front Door In		Manual Release Button Operated
15/03/2001	08:22:00	Front Door In		Manual Release Button Operated
15/03/2001	08:26:00	Front Door In		Manual Release Button Operated
15/03/2001	08:27:00	Front Door In	Russell Martin	Door Opened
15/03/2001	08:30:00	Front Door In	Emma Warren	Door Opened
15/03/2001	08:36:00	Front Door In	Warren Butler	Door Opened
15/03/2001	08:36:00	Front Door In		Manual Release Button Operated
15/03/2001	08:46:00	Front Door In	Richard Pullan	Door Opened
15/03/2001	08:59:00	Front Door In	Kirsty North	Door Opened
15/03/2001	09:28:00	Front Door In		Manual Release Button Operated
15/03/2001	09:30:00	Front Door In		Manual Release Button Operated

The event log The event history log is stored on the WinPLAN640 fixed disk and is sized to record a minimum of 10,000,000 events.

Audit Trail

In much the same manner as the History analysis option allows the operator to review cardholder activity around the site, using the Audit Trail viewer, it is possible to view an analysis of system operator functions. Information included in the listing are… the identity of the operator, times 'logged on', menu functions selected and editing actions carried out. The Audit trail facility allows an operator to produce a listing which can be limited to a selected date range or specific user (selected from a drop-down list). All of the information is available for preview 'on-screen', sorted according to requirements before the list is printed.

The Audit report shown below indicates that users 'Master' and 'Ray' have been active recently. Between them, they have been making changes to the password editor, editing card records and carrying out remote lock override functions.



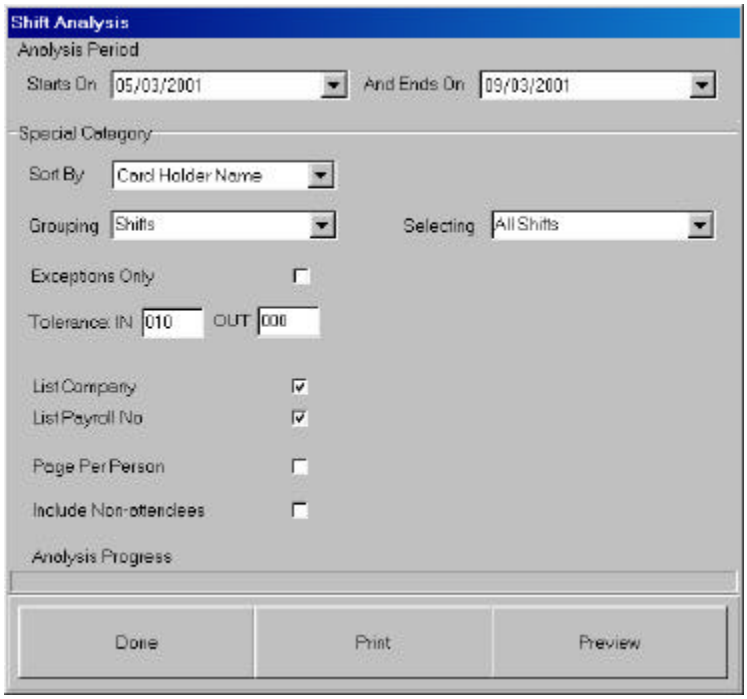
Enhanced Time Keeping listing options…

In addition to the previously described history analysis feature (which will faithfully reproduce the archived event history with no post processing applied) the WinPLAN640 system is available with a Time and Attendance utility called 'WinShifts'.

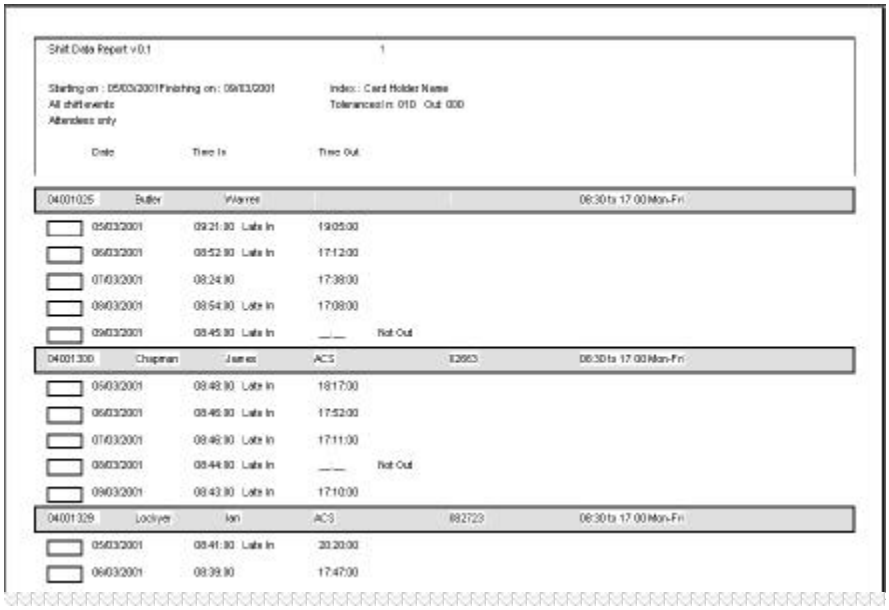
Using the WinShifts feature, a range of listing parameters can be selected which will dictate the results of the report. For example, a 'tolerance' can be selected for the beginning and end of each shift, which will allow the selected number of minutes 'grace' to staff who are 'late in' or 'early leaving'. The actual event data is compared to the expected times based on the selected shift pattern and the tolerance for each member of staff in order to create an accurate report.

Clients who wish to use the shift analysis feature, but, who do not operate a shift system of working, can simply set all records to belong to a common shift pattern which reflects the business hours of the company.

The shift analysis form is shown below to indicate the listing options available…



The above settings would result in a listing for the period 05/03/2001 to 09/03/2001, sorted by Name and grouped by Shift which allows staff 10 minutes of tolerance on entry and 0 minutes of tolerance on exit. The listing will include an entry for every day in the period selected for each member of staff who attended on that day (e.g. Non-attendees are omitted). The option to break the list up into one page per person has not been selected, neither, has the option to list only those staff who failed to swipe in on time. Additional fields that have been selected to be included within the listing are; 'Payroll No.' and 'Company name' from the personnel record.



The print listing shown above indicates how exceptions are reported by the system. Comments such as 'Late in' or 'Early out' are self explanatory. 'Not in' or 'Not out' indicate that the card holder did not use their card for access or egress within the allowable time windows.

In the case of the staff shown above, 'James Chapman' was recorded as late every day and that he failed to swipe on leaving on the 8th March. 'Warren Butler' managed an exception free day on the 7th March.

Additionally, a listing can be set to include the running total of hours worked accumulated over the period of the report.

A 'real' data set would not produce as many exceptions as shown above, however, the empty box on the left hand side of each entry, allows the Pay-roll department or local manager to enter an exception code to explain the problem… For example... B = Out on Business, S = Sickness etc. The key for these codes can be included at the bottom of each page in the listing in the absence code footer.

General Staff management reports…

The Staff database listing option features a range of reporting tools which are designed to aide the administration and management of the system.

Dormant cards - Available from a menu within the staff database editor. This listing allows the system administrator to keep track of cards which have not been used recently. The operator is prompted to specify the adjustable time period in 'days or weeks' – or by selecting a specified date (since which cards should have been used). The resulting report shown below, will include the card number, name and last use of the relevant cards. It will then be up to the system administrator to decide if these cards should remain as valid on the system, or be deleted.

Infrequently Used Cards 15/03/2001 14:53:58

Cards not used since 12/03/2001

Card	Card Holder	Last Use	
04101816	spare ACCESS CARD	23/12 12:21 Front Door in	Door Opened
04001300	James Chapman	12/03 13:03 Front Door in	Door Opened
04100515	bob nightshift	12/01 10:24 Front Door out	Door Opened
04100235	test card No 235	31/01 14:04 Inner Door	Card not recognised

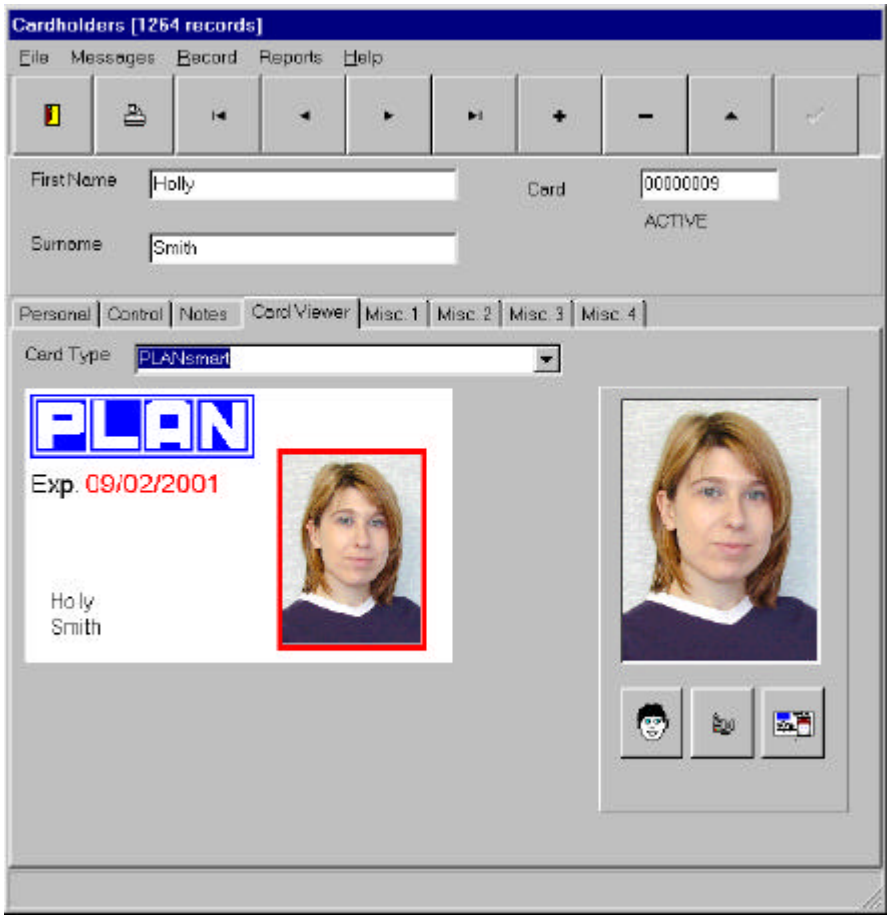
Soon to expire cards – Another management listing, selected from within the staff editor, this option allows an operator to create a report containing only those card records which will be expiring in a user definable time period (selected in 'days or weeks') or on a specific date. The listing shown below indicates that there will be 4 'expired' cards on the system on the 16/06/2001. In this case the listing further indicates that these cards are already expired.

Soon To Expire Cards 16/03/2001 16:25:58

Cards due to expire on or before 16/06/2001

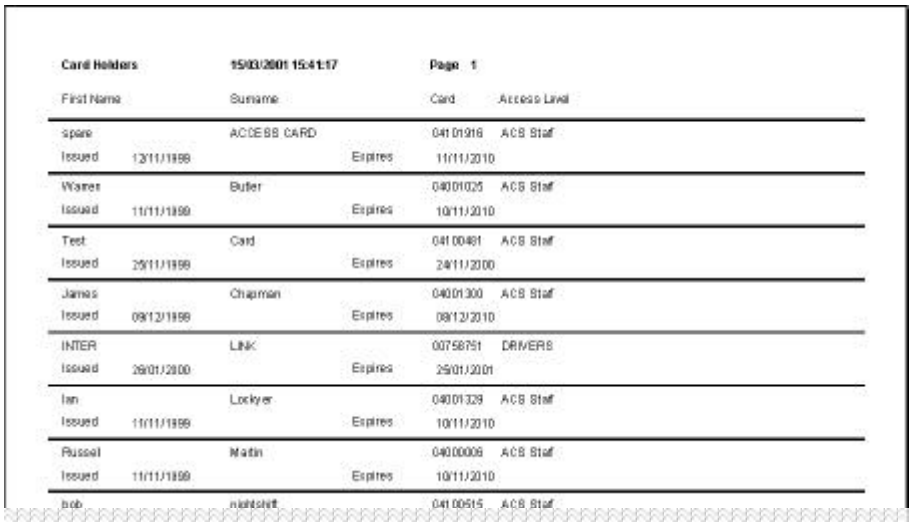
Card	Card Holder	Expires
04100481	Test Card	24/11/2000
00758751	INTER LINK	29/01/2001
04100235	test card No 235	28/11/2000
00800001	Fred Smith	10/11/2000

Staff Record listing options - In addition to the above specialised listing facilities found within the staff editor, there is, of course the facility to view on screen and list the actual staff database….. A typical staff record is shown below…



Access to additional stored information is by means of the tabs for 'Personal', 'Control' and 'Notes' etc. Simply clicking on one of these tabs will reveal the relevant information.

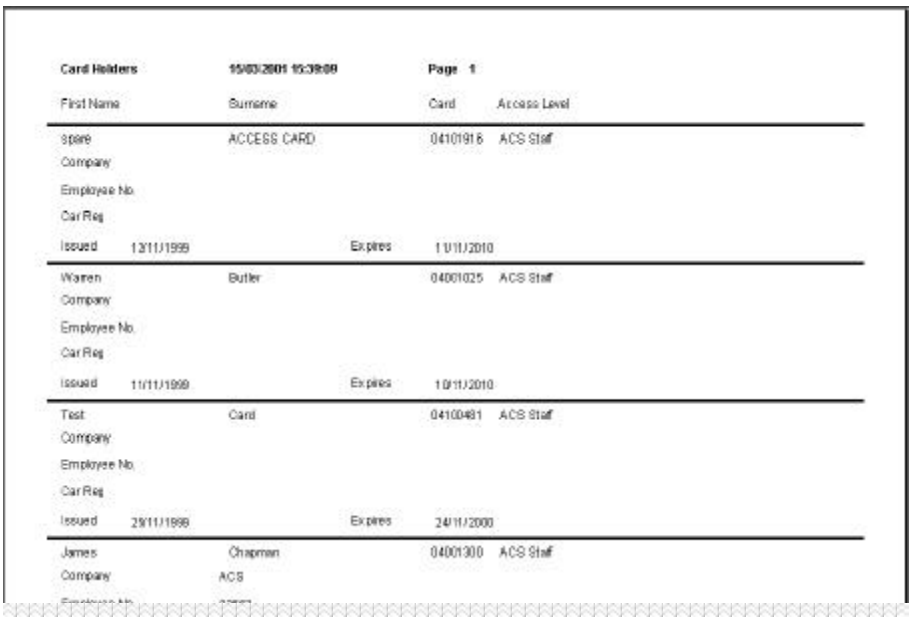
A staff listing can be generated which includes as much or as little of the staff data as required….



Card Holders **15/03/2001 15:41:17** **Page 1**

First Name	Surname	Card	Access Level
spare	ACCESS CARD	04101916	ACS Staf
Issued 12/11/1999	Expires 11/11/2010		
Warren	Butler	04001025	ACS Staf
Issued 11/11/1999	Expires 10/11/2010		
Test	Card	04100481	ACS Staf
Issued 25/11/1999	Expires 24/11/2000		
James	Chapman	04001300	ACS Staf
Issued 09/12/1999	Expires 09/12/2010		
INTER	LINK	00758751	DRIVERS
Issued 26/01/2000	Expires 25/01/2001		
Ian	Lockyer	04001329	ACS Staf
Issued 11/11/1999	Expires 10/11/2010		
Russel	Martin	04000009	ACS Staf
Issued 11/11/1999	Expires 10/11/2010		
bob	nightshift	04100515	ACS Staf

The above list has been configured to include only the basic cardholder information, whereas the figure below, includes slightly more information on each card holder…



Card Holders **15/03/2001 15:39:09** **Page 1**

First Name	Surname	Card	Access Level
spare	ACCESS CARD	04101916	ACS Staf
Company			
Employee No.			
Car Reg			
Issued 12/11/1999	Expires 11/11/2010		
Warren	Butler	04001025	ACS Staf
Company			
Employee No.			
Car Reg			
Issued 11/11/1999	Expires 10/11/2010		
Test	Card	04100481	ACS Staf
Company			
Employee No.			
Car Reg			
Issued 25/11/1999	Expires 24/11/2000		
James	Chapman	04001300	ACS Staf
Company	ACS		

Access Rights – A listing utility which allows an operator to select a range of door locations in order to produce a list of staff who have access authority to these doors. The operator can select the listing criteria to include staff who have access to **any** or **all** of the selected doors. The Access Rights utility is useful for security audits.

Head-count – An occupancy (total number of people on site) report can be generated in real time and either displayed on screen or stored to a log file

for future analysis. The Head-count feature can be configured to base it's report on the Global occupancy of the building, and/or specified zoned areas (or multiple sites). The head count display is used where managers wish to keep a tack on the total number of cardholders in a building or zone (for example a canteen area or car park).

General Database listing features

A listing option similar to the standard staff listing facility, is provided in each of the database editors (Doors, Time Profiles, Access Levels etc) to allow printing of the information stored on the system. Each listing option is available for preview on screen before committing to the printer.

Because the WinPLAN640 system is a multi-user net-workable software package. It is possible for many of the above described utilities and listings to be used by more than one person in more than one location at the same time.

Additionally, the open architecture of the database information and History storage allows a wide range of customer specified reports to be created as menu items. A CSV export utility allows the user to commission bespoke listings & reports from the manufacturers or third party developers.

Anti-Passback

The system supports "True" Anti-Passback (as distinct from "Timed"). When operating in this mode a designated "Entry" reader will not accept cards as valid until they have been used at an "Exit" reader. Passback violations are reported to the CCU as exceptions. To maintain off-line integrity, "True" anti-passback requires that passback zones must operate entirely under the control of an individual out-station.

Anti-Passback is enforced by denying access when a violation occurs and generating an exception at the PLAN-640 CCU.

The PLAN system supports Global and Multi-site Global Anti-Passback zones, which can be defined in order to account for Entry and Exit doors which are connected to different PLAN-400's, however, this feature will revert to local control if the connection between the P400's and the CCU is lost.

General System & Extended Alarms

All alarms within the access control system report to the PLAN-640 CCU. Each extended alarm record shall allow a user selected 'sound' to be attached to the alarm activation).

1) Door Forced
2) Door Left Open
3) Invalid Card Use
4) Attempted Passback
5) Use of emergency exit device (Door Forced)
6) Activation of an extended alarm input unit
7) Asset Detected (if asset readers are fitted)
8) Unauthorised Asset Alarm (if asset readers are fitted)

Alarm information can be displayed both as a colour coded text message on the PLAN-640 system VDU and Graphically on the 'Virtual' Control Room Graphics Alarm Display. The features of the Graphics Workstation (described in detail below) will allow certain alarms to cause the desired CCTV camera to display on a selected monitor (subject to the compatibility of the CCTV system and the presence of a camera in the vicinity of the alarm).

Each new occurrence of an alarm shall cause the PLAN-640 CCU to go into alarm. It shall be silenced when the alarm is acknowledged. Alarms can be displayed in a scrolling window so that off screen alarms may be accessed.

MS Windows 2000

The WinPLAN640 software application has been tested for operation on PC's hosted by Windows 2000 Professional and Advanced Server. The software is also compatible with Windows 95,98,ME, NT4.0 (SP4 or later) and XP pro.

Remote Site Networking

As and when the need arises to Link the system to other sites, the Communications options for linking additional P400's in one or more remote buildings are detailed below…

Direct Connection.

The simplest and cheapest option, allows additional PLAN400's to be connected onto any client owned direct cable connection. The cables must be minimum 2 twisted pairs, with a maximum length of 3000'.

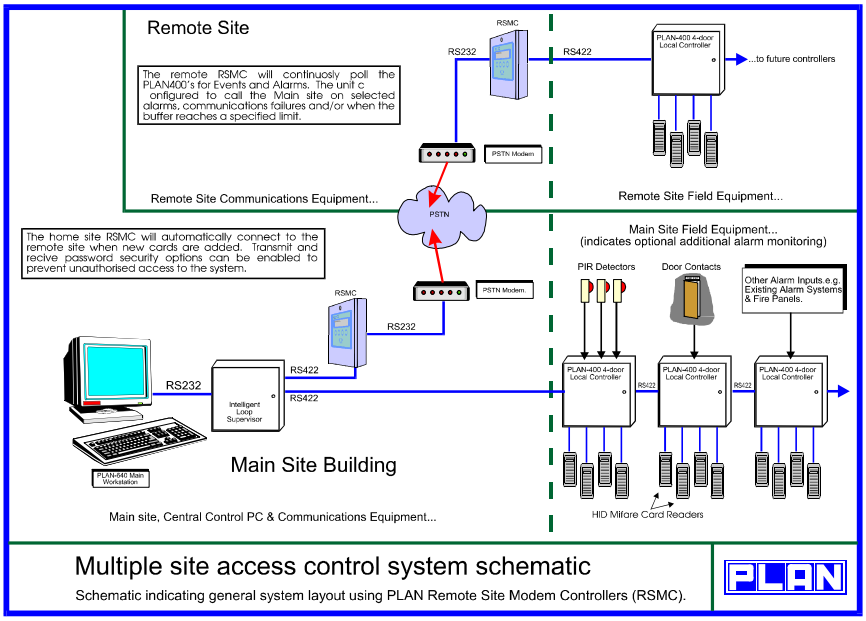
Additional hardware required: No additional hardware is required.

PSTN Dial-up Connection.

Using the Remote site modem controller (RSMC) a standard PSTN line can be used to connect small sites into the main system. An RSMC is installed at both the home and remote sites to create a transparent link between the 'main' system and PLAN400's installed in a remote location. Links can be within a building, local area or international.

The home site RSMC will automatically connect to the remote site whenever new cards are added or edited. The remote RSMC will continuously poll the PLAN400's for Events and Alarms. The unit can be configured to call the Main site on selected alarms, communications failures and/or when the buffer reaches a specified limit. If either unit fails to make a connection, an alarm can be raised at either end of the link.

Password security options can be enabled to prevent Unauthorised access to the system. When enabled the RSMC will only communicate with a unit which has been programmed with the correct password.



Leased Line Connection.

If a dedicated leased line is installed, additional controllers can be connected at a remote location further than 3000'.

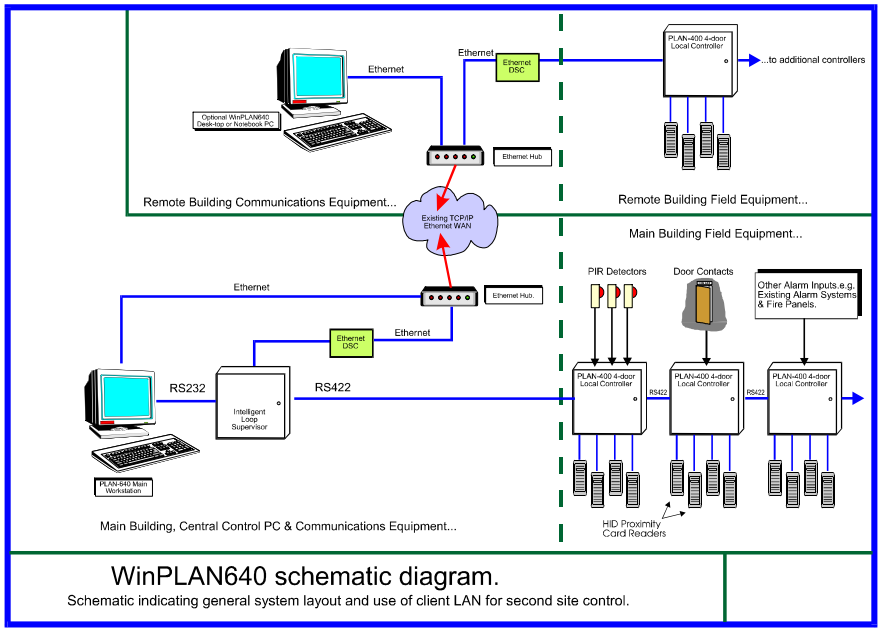
Existing Client Multiplexor

PLAN400s can use spare capacity on communications equipment already in place (such as Kilo stream Mux hardware). A single chain up to 16 PLAN-400's can be connected to a spare Async port on such equipment. The communications requirement is: 1 x Async V24 port, Full Duplex 1200 baud at each site. Equipment supply, setup and support should be provided by (or in association with) the clients IT dept.

Existing Client :LAN/WAN

A P400 DSC (Data Signal Converter) is employed at each site to convert the native P400/P640 communications protocol into TCP/IP Ethernet compatible packets. These are then transmitted over the existing LAN. The DSC simply provides the interface between the first P400 in each location and the network. A cluster of P400's in close proximity would be hard wired together in the normal manner. This connection is transparent to the P400's and they carry on operation as if they were directly connected. Bandwidth used by the PLAN-400 communications is minimal. As serial data, the rate equates to 1200 baud.

Hundreds of remote sites can be connected in this manner to create an enterprise wide solution for a 'harmonised' access control system for any organisation.



P400DSC's are available for 10/100baseT and 10base 2 (ports comply with IEEE 802.3 physical and MAC layer specifications).

Other options…

The above list of schemes for remote site communications is by no means definitive. In many cases, existing equipment such as Fibre-optic Multiplexor hardware, internal telephone systems (such as ISDT) and Radio/micro-wave links will provide a suitable path for the low bandwidth serial communications required by the P400's. This is often in addition to the primary function of the hardware.

Operator Training

Training is essential to ensure adequate operational knowledge of the Access Control System and it's various components. The Schedule described below is a list of the issues which will be covered in a typical training session....

Typical Training Schedule

Introduction

Outlines the various areas of system operation to be covered in the training session and introduces conventions used. Also includes a brief description of the function and purpose of the component parts of the PLAN-640 control system.

Using the PLAN system

Editing - General editing using the PLAN system user interface. Specific topics covered:

Logging on.

Entering data.

Backing up.

Listing functions.

Detailed explanation of system facilities

Covers the use and configuration of:

Time Profiles, Access Levels, Door Records, Passwords, Adding Editing and Deleting Card Records. Analysis options. System Configuration. Alarm Acknowledgment. Remote Door overrides. Alarm Acknowledgment. Roll Call listing. Personnel Quick-searches. Extended Alarm Monitoring. Audit Trail Listing Facility.

System Messages

An explanation of the meaning of the various messages displayed and printed by the system.

Questions

Prior to a period of supervised 'hands on' use of the system, the operators will be given the opportunity to ask questions on any issue concerning the system.

Examples and Exercises

In order to ensure that the training has been successful, the operators will be given the opportunity to 'use' the system. They will be presented with 'typical' scenarios which will require them to carry out a procedure or prompt for a specific response. At this time the individuals undergoing the training will be informally assessed in order that any areas which need reinforcement can be covered again.

WinPLAN-640 Access Control System Data

The access control system data is split into the following individual database files:-

1) Time Profile Records
2) Door Groups
3) Access Levels
3) Door Records
4) Password Records
5) Card/Personnel Records
6) Alarm Point Records
7) Asset Records

The system software provides a separate editor for each of the above data files. Editor functions include the ability to add, change, delete or print a record. All functions are security level protected . A brief description of the main elements of each type of record is given below.

Time Profiles:- 128 user programmable time profiles are available. Each provides 4 Time Zones for setting different active periods for different days of the week. Time Profiles are used for the following purposes:-

1) To control card access.

2) To disable card readers during certain hours.

3) To enable/disable groups of alarms during specific time periods.

An individual status field within each record will allow an authorised system operator the option to manually disable any Time Profiles currently in effect.

Door Groups:- For ease of administration, Groups of readers/doors can be combined into individual door Groups, each of which contain a record number and text name plus a list of selected doors which constitute the group.

The system will allow up to 1000 individual Door Groups to be configured.

Access Levels:- An Access Level contains a list of door groups at which cardholders will be allowed access, additionally, each record contains a selected time profile (which will control when the groups will be enabled), a record number and text name.

The system will allow 800 Access Levels to be configured.

Door Records:-

Each Door Record is configurable in the following ways:-

Field Name	Description
Lock operate mode:	This field should be set to suit the type of locking device installed. e.g. Fail Safe or Fail Secure.
Door Identifier:	A 32 character door or location name should be keyed in, to enable easy identification of each door during listings etc. This name will be displayed on the event monitor screen, and in event listings.
Free Time Profile:	A Free Time Profile, which when active, leaves the door free by permanently releasing the lock for the duration of the active period. At all other times the door will be accessible to valid card holders only.
Bolt Time Profile:	When a Bolt Time Profile is set it will cause the door to become permanently locked or "Bolted" whenever the Time Profile becomes active. This will have the effect of locking out all cards.
Lock Operate Time:	The Lock Operate Time, or strike delay, is set in seconds and can be anything between 001 & 255.
Alarm Control Profile:	A Time Profile can be selected, which, when active will cause the door alarms to use the 'Active Delay' (see below). When the Time Profile is inactive, the 'Inactive Delay' will be observed. By this method, a user can configure door alarms to be more tolerant of doors held open at certain times of the day. Door alarms can even be switched off for pre-determined times using this option.
Active/Inactive Delay:	A door left open for longer than the Alarm Delay Time will cause a Door Left Ajar warning. Similarly, a door opened without a valid card entry (or exit request) will cause a Door Forced Alarm.
Auto-acknowledge:	Door Forced and Ajar alarms can be individually set to be either automatically acknowledge by the system or manually the operator.

Passback Code: A drop list allows the selection of a Passback mode. This can be set such that if a card holder passes through a door with Entry Area '1' then they will not be able to pass through another door with that passback level until they have entered their card at a door with Exit Area '1'.

Door Type: Normal/Entry or Exit can be selected in order to define the boundaries of the building, so that when using Quick Search or Roll Call, the operator can determine whether a card holder is "on-site" or "off-site"..

Password Records:- Each operator password record is made up of a table of all operator actions in which each action is marked as accessible or not accessible to the operator. In this manner, an operator can be given the authority to view or print card/personnel records but not to add, change or delete them.

The will allow 64 individual Password records to be created.

Card Records:- Each card record should contain the pre-programmed unique code encoded onto the card. A status field indicates whether the card is active, inactive or expired. If the current status is inactive then it is classified as barred. The card record contains the following additional information.

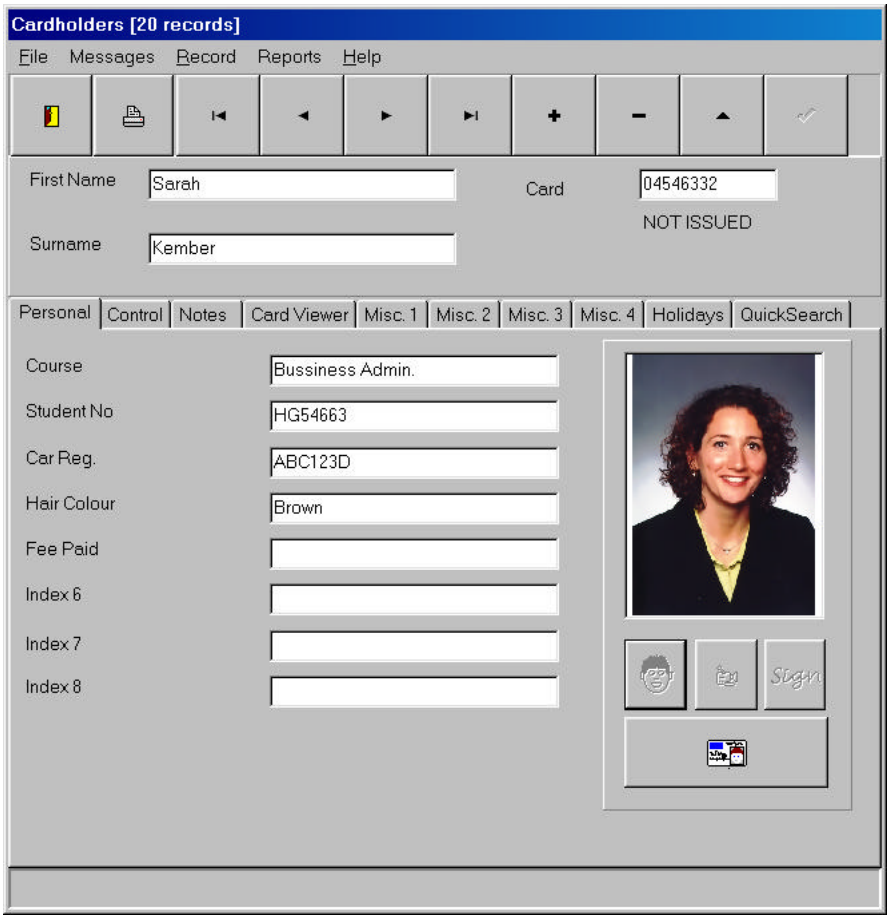
1) Date on which the card is to be issued (validated)
2) First name
3) Last name
4) Date on which the card expires
5) Access level
6) Card-holder Image
7) 8 additional user defined active fields. (See below).
8) ID Badge design and card print preview.
9) Free text notes.
10) 32 additional user defined text fields.

For maximum flexibility the card record database can be tailored to suit the requirements of the customer by configuring 8 user defined fields in the personnel record. It will then be possible for searches & listings to be performed using the data in these fields as the sort criteria. A further 32 user defined (non-searchable) text fields is provided on four separate Tab pages to allow for extended administrative data to be stored within the card record.

Editor functions include the ability to add, change, delete or print a card record. Using the integrated Photo-ID badging facility live video image data can be displayed and then stored in the card record for badge printing. All functions are security level protected.

The PLAN-640 card record database will be sized to support the required 200,000 card records – this is expandable and dependant only on the system hardware storage and resources. (Max. 22,000 valid at any one xPLAN400 local control unit - Upgradeable to 32,000).

A typical Card record is shown below, complete with cardholder picture.



The Tabbed pages (Control/Notes/Card viewer etc.) allow the operator access to other information such as Issue/Expiry dates, Watched card status, Access Level, Badge design (with preview), Holiday settings as well as 32 additional user defined text fields, held in the Misc pages.

Alarm Point Records:- An alarm point record must be set for every extended alarm input device connected to the system. Each Record can be configured in the following ways:-

Field Name	Description
Shunted:	The Shunt status will be either set to "Yes" or "No". "Yes" indicates that the Alarm Point has been switched off & alarms will not be reported from this device, regardless of the state of the door/device that it is connected to. "No" in this field means that this alarm point is active, subject to the status of either of the Armed or Disarmed Time Periods described below.
Point Identifier:	A 20 character Alarm ID or location name can be programmed to enable easy identification of each point during listings etc.

Armed Time Profile: A Time Profile can be selected, which when active will arm the Alarm point for the duration of it's active period. At all other times, the system will disregard data from this Alarm Point.

Disarmed Time Profile: A Disarmed Time Profile will cause the system to ignore Alarm information from the associated Input device whenever the Time Profile is active.

Sound: A field for selection of different wav file alarm sounds for each alarm input.

Control Action: Here the operator can select from a list of pre-defined system actions to be carried out automatically in the event of this alarm being set. Available options are to Lock, Unlock or set to normal all doors or any selected group of doors. Additionally, the alarm can be enabled to automatically print a roll call on activation of this input.

Messages: A total of four lines of additional text information can be keyed in to form a message which will be displayed/printed in the event of the alarm being set. Headings include:-

1st Line:	Alarm Message
2nd Line:	Contact Name
3rd Line:	Actions line 1
4th Line:	Actions line 2

Asset Records:- Effective Asset tagging requires a reading technology which is capable of detecting multiple cards on the move at long range. The PLAN system features and advanced level of Asset protection utilising a dedicated panel developed specifically for this purpose. This solution benefits significantly over competitive systems which do not have the advantage of a dedicated asset controller which allows the local verification of Assets with any of their allocated owners (up to 16 owners per asset) instantaneously with no PC or central control involvement.

An Asset record must be created for every 'Tagged' item in the system. Each card record should contain the pre-programmed unique code encoded onto the Asset Tag, an Asset Name and a list of authorised 'Owners' for this piece of equipment.

A 'details' tab page allows the operator to store specific additional information about this article as well as the optional facility to store a picture.

Integrated PLAN-640 Photo-ID Software

General Description

An integrated Photo-ID capability can be supplied which incorporates, image capture, card database and printing software. The system will utilise a Direct to Card Dye Sublimation colour printer and will be compatible with the card technologies offered.

Because the badging facility is an embedded feature of the PLAN system e.g. it is linked to the main PLAN-640 and shares card record data with it. Creating a Badge and issuing an access control card can be streamlined into one simple procedure – carried out from a single workstation.

WinPLAN Virtual Control Room Software

General Description

The **WinPLAN** Virtual Control Room System is a programmable, computer-based, electronic security management software package which has the capacity to combine, in a highly integrated manner, Access Control, C.C.T.V., Intercom, Paging, & Alarm Monitoring systems into a common user interface.

Control of the Virtual Control Room workstation will be achieved through the use of a Mouse, (or optionally Touch Screen) user interface.

The graphics workstation is capable of displaying detailed colour graphics images of the site, it is possible to import these graphics from commercial CAD packages, or create new designs with the software supplied.

Once created, site maps can be annotated with various equipment Icons for alarm enunciation. This is achieved through the use of the Windows 'Drag & Drop' facility. By the same method, Customisable 'Equipment Pads' can also be created and then selected on the screen to allow the operator direct control of field equipment. Activation of on screen icons will allow the operator to control external devices such as Door Overrides, CCTV Equipment, Intercoms. In this manner a 'Virtual' security console can be created on screen, allowing intuitive control over remotely located equipment, whilst at the same time, graphical indication of the current status of alarm sources.

Zoom in and out icons will allow the operator to link to more detailed maps of different areas of the site. The typical time taken to display a full colour map with icons etc. will be less than 1 second. Map display is automated e.g. specific alarms will cause specific maps to be displayed, however, it is possible to select from a drop down menu list or 'hot-link' from an on screen 'button' to any map stored on the system.

It is possible to create complex commands involving many separate elements of the different sub-systems and to attach these (using Drag and Drop) to inputs from the Card, Intruder or other systems. These commands will then be carried out automatically in the event of that alarm being set.

All sub-systems have the capability for redundant control in the event of loss of communications with the system.

VisiPLAN Visitor ID badging and registration software

General Description

The VisiPLAN software can be deployed by PLAN system users as an add on to their existing system or as a stand alone visitor management solution. The objective is to simplify the registration of visitors to the site by providing a simple, automated self registration system.

Visitors will be directed to a plinth, wall or kiosk mounted touch screen (pictured below) workstation where they will carry out a simple self registration procedure. A badge can be printed and dispensed by the workstation, or, visitors can report to a reception desk to collect their ID card.

The VisiPLAN Touch-screen visitor management software integrates the process of automated visitor badging with the function of an access control system. As such, visitors who are logged 'in' using a touch screen terminal will appear on roll call listing if an evacuation occurs during the period of their visit.

ID cards can be printed onto self adhesive labels, PVC cards or special perforated cards all of which can incorporate safety and fire evacuation instructions.

As part of the 'WinPLAN' suite of software applications, at all times, the software integrates seamlessly with the PLAN system cardholder database.

Access Control System - Equipment overview

Central Control Equipment

The PLAN-640 CCU will be based on an Intel Pentium™ PIII P.C. (or better). The minimum system requirements will include the following:-

1) 128 megabytes of main system memory
2) 1 x 6.0GB/<12mS Fixed Disk
3) 1 x 3.5" .1.44Mb Floppy Drive
4) 1 x Zip Backup device
5) ETHERNET interface and software drivers
6) 2 x serial communications ports
7) Intel Pentium™ PIII CPU (clock speed of >300 MHz)
8) XGA graphics adapter (4mb video memory).
9) 17 inch colour monitor
10) QWERTY keyboard

In addition, the CCU shall make use of the following software elements:-

1) MS Windows'95,98, NT 4.0 or 2000.
2) Compatible Network software
3) WinPLAN-640 Central Control Software

Optional PLAN-640 Administration Workstation (ID Badging Station)

The ID badging workstation shall be based on an Intel Pentium™ PIII P.C. (or better). The minimum system requirements will include the following:-

1) 128 megabytes of main system memory
2) 1 x 4.3GB/<12mS Fixed Disk
3) 1 x 3.5" .1.44Mb Floppy Drive
4) ETHERNET interface and software drivers
5) 2 x serial communications ports
6) Intel Pentium™ PIII CPU (clock speed of >300 MHz)
7) XGA graphics adapter (2mb video memory).
8) 15 inch (minimum) colour monitor
9) QWERTY keyboard
10) Image Capture Card
11) Desk Mounted Camera
12) Dye Sublimation PVC Card Printer

In addition, the CCU shall make use of the following software elements:-

1) MS Windows'95,98, NT 4.0 or 2000.
2) TCP/IP Compatible Network software drivers.
3) WinPLAN-640 Remote Administration Software (includes badging software)

ILS-400 Intelligent Loop Supervisor

The PLAN ILS-400 is available as either an 8-loop or 2-loop controller. The 2-loop unit is supplied in a desk top housing, designed to sit adjacent to the Main PLAN-640 PC, whilst the 8-loop unit is available in either a Wall, Desk

or Rack Mount enclosure. For the purposes of this scheme the 2-loop version has been utilised.

The ILS provides a highly resilient, communications bridge between the Main PLAN-640 PC and the PLAN-400 field control units.

Field Control Equipment

Microprocessor Controlled Field Panels - PLAN-400's

To maintain the highest level of system fault tolerance, each PLAN-400ex is a complete, full functioning, integrated access control unit. This means that the system will continue functioning at 100% capability even when disconnected from the PLAN-640 CCU, e.g. when "off line", the system shall continue to allow only valid cardholders through their selected doors & at their authorised times, it will also store the last 2,000 events in the cyclical memory until communications are restored at which time, the PLAN-400 will inform the CCU of all access control decisions made while off-line.

Emergency programming can be achieved using the 24-button keypad & LCD display.

Each PLAN-400 will have the following interfaces:-

a) Card Reader x 4

b) Electromagnetic Lock x 4

c) Egress Button x 4

d) Door Monitoring x 4

e) Network Connection x 1

f) RS232 Printer Interface

g) Supervised extended alarm input x 16

h) Fire Alarm Door override interface x 1

An RS232 printer port is available as standard at each local Controller. Transactions which occur at the P400 shall normally be printed at the Host, with the local printer port being for emergency and maintenance purposes.

For ease of maintenance, all network, reader and lock connections to the field panel will make use of de-mountable terminal block. **The time taken to replace a PLAN-400 shall be less than three minutes**, and shall require no special tools or training. Reliability of the control unit should be greater than 40,000 hours MTBF.

The PLAN-400ex control units are **warranted for 5 Years from date of commissioning**.

Enclosures

The PLAN-400's are housed in a lockable steel cabinet with rear and side cable entry and an integral PSU/charger. A Tamper switch is fitted which can be set to indicate an alarm when the control cabinet inner lid is opened.

PSU's

PLAN-400's, Card Readers and Magnetic Door Locks which require approximately 12vDC can powered via the PLAN-400 3.0 Amp PSU/Charger

built into the enclosure. Reliability of the PSU is greater than 40,000 hours MTBF at full load.

Each lock output is independently fused. The power supply is backed up with a lead acid rechargeable battery. Space is available within the enclosure which allows for up to 14 amp/Hrs of battery to be accommodated.

The PSU is also available in a separate housing (to be sited adjacent to the PLAN400). This Aux. PSU is utilised where additional Lock Power over and above that provided by the standard PLAN400 PSU is required.

Card Reading Equipment.

The system is compatible with most other types of card reading technology. Supported card readers are;-

Proximity

Mifare Contactless Smart Cards

Mag-stripe

'Watermark' Magnetic Stripe

Wiegand Swipe

Proximity & Long Range Hands Free

Scramble PIN entry keypad

Various Biometrics

Infra-Red Bar Code

It is possible to mix different reader technologies from the above list throughout an installation.

Locking Equipment

The xPLAN-400 is compatible with most types of electromagnetic locking devices switched through the 1.0 amp voltage free relay contacts on the PLAN-400's or using the 500mA 12vDC fused lock outputs.

In accordance with the requirements of the specification, fail safe monitored Mag-locks have been allowed for at each controlled point identified on the door schedule.

Break Glass Units

A break glass unit will be located adjacent to each controlled Fire Exit door according to the door schedule. Activation of a break glass unit shall immediately open the door to allow free exit, this function shall not depend on the operation of any other the part of the system.

Fire Alarm Door Override Input

In addition to the local Break Glass Points at each door, the PLAN system can accept door override signals from a Fire Alarm system in two ways.

a) Each Panel features a configurable Fire Alarm door override input. This must detect a closed contact '*safe*' signal at all times from the Fire detection Panel. If the fire alarm link is removed, the selected doors connected to this panel will open. The doors which open in this event are selected by means of a series of jumpers on the PLAN400 PCB. Since this facility does not

depend on the microprocessor to operate it can be considered truly fail safe in operation.

b) Any supervised alarm input (16 per panel) can be set-up in software to open all doors, a single door or a specified group of doors. Using this scheme only one signal is required from the Fire Panel for the whole system.

EMC

All products are marked with the CE symbol and as such conform to the protection requirements of Council Directive 89/336/EEC, relating to Electromagnetic Compatibility by the application of the various appropriate standards.

BS EN 50133- part 1

Depending on the final configuration of the installed system, the equipment will meet the General requirements of the British Standard for Access Control Systems for use in security applications (published March 1997) ranging from Security Classification 2B to 3B.

Software Upgrades: The PLAN software is subject to a continuous development program. The resulting enhancements and software upgrades are available on disk to clients Free of Charge, for the life of the system. Free upgrades are usually offered to clients during routine maintenance visits.