

Product Specifications

Checkpoint Systems 512 Reader Threshold Enterprise Access Control System

Features

Users:	50,000
Doors:	512
Operator Levels: (user defined)	64
Outputs:	8192
Inputs:	4096
Access Levels:	256
Time Zones/Intervals:	64/8
Holidays:	32
Auxiliary Stations:	Consult factory
Printer Station:	Consult factory

PART 1 General

1. GENERAL OVERVIEW

Threshold Enterprise is an application designed to operate under Microsoft Windows NT operating system. The system shall be a true Multi-User, Multi-Tasking. The computer requirements are application dependent but at a minimum shall be a Pentium class machine (specified by Checkpoint Systems) suitable for operating Windows NT Workstation OS or Windows NT Advanced Server OS supporting a minimum of five networked NT Client and/or Workstations and the Threshold Enterprise access control application. It shall be possible to "remotely" access the Threshold Enterprise application for off-site support and/or management. The Threshold Enterprise application shall make use of Microsoft Windows NT printers available on the network. In addition, a dedicated incremental print, Event Printer shall be provided.

Featuring standard Microsoft GUI interface conventions the application shall allowing the day to day operations to be performed using a standard Microsoft two button mouse. All devices shall be client definable using plain English text labels and all operator instructions and messages shall be in plain English. The complete operator instruction manual shall be imbedded in the On-line help and shall be assessable using standard "Help Topic's," "Index," "Key Word," and "Search" requests. The client shall have the ability to define Events for viewing in any one of four event viewer screens or any combination of those screens. Events shall also be designated for printing to selectable printers. The Threshold Enterprise application shall provide at a minimum, utilities for Backup and Restoration, Operator actions and overrides, Alarm handling and response, site Floor Plans, and Report Generation of Card Holder activity, records and history, system activity and operator activity.

The access control application shall control up to 512 doors, 20,000 cardholders expandable to 50,000 cardholders, and monitor up to 4,096 individual alarm and/or device monitored input points linkable to any of the up to 8,192 controllable output relays. The application shall also offer operator-configurable reporting of event history and cardholder activity. The application shall have a minimum of two hundred fifty six (256) access levels and sixty-four (64) time zones containing eight (8) unique intervals per zone.

2. COMMAND CENTER COMPONENTS

2.1 Command Center Computer

The Checkpoint Threshold Enterprise Command Center Computer as supplied by Checkpoint for operation of a dedicated access control and security ID station shall be at a minimum ...

THRESHOLD NT SERVER CONFIGURATION

ATX MID-TOWER CASE WITH 235WATT POWER SUPPLY
INTEL PENTIUM III 550MHz PROCESSOR WITH 100MHz BUS
TYAN DUAL PROCESSOR PENTIUM III MOTHERBOARD
256MB SYNCHRONOUS DRAM MEMORY 100MHz
TEAC 1.44 MB FLOPPY DRIVE
TEAC 40X ATAPI IDE CD-ROM DRIVE
ATI EXPERT 8MB AGP VIDEO CARD
PRINCETON GRAPHICS EO-705 17" SVGA MONITOR
DPT PM2044UW SCSI CONTROLLER (ULTRA WIDE)
(2) SEAGATE ST39140W 9.1 GB SCSI WIDE HARD DRIVES
SONY SDT-7000 DDS-2 4mm 8GB DAT TAPE BACKUP UNIT
SONY DG 120 120M 4mm DAT TAPE
MICROSOFT INTELLIMOUSE PS/2 MOUSE
KEYTRONICS 104 KEY ENHANCED KEYBOARD
ETHERNET TWISTED PAIR PATCH CABLE
3COM 3C905B 10/100 ETHER NET ADAPTER (TP ONLY)
DB9 to DB25 SERIAL CABLE (1 ft)
PCANYWHERE 32 9.0 (HOST AND REMOTE)
SUPRAMAX 56K V.90 INTERNAL MODEM
MICROSOFT WINDOWS NT SERVER 4.0 5 CLIENT

3. NETWORK COMPONENTS

3.1 General

The system components shall be of modular design to allow ease of installation, service, future expansion, upgrades and additions to the system.

The system shall consist of the interface of two levels of intelligent controllers with distributed architecture. These controllers shall have operating environments to allow complete functionality at a temperature range of 0° to 50° C and a relative humidity of 90% (non-condensing).

3.2 Main Controllers

The main controller shall be microprocessor based with on-board time and date generation with battery to allow a minimum of 48 hours data integrity. This device shall be responsible for maintaining the data communications between the attached

terminal controllers and the Command Center CPU. This device shall also maintain a buffer for a minimum of 4000 event transactions for off-line operations or in the event of lost communications with the CPU. The system shall be capable of accepting a minimum of 128 main controllers. There shall be a minimum of 16 terminal controllers attached to any one main controller for a system maximum of 256 terminal controllers. These main controllers shall be modem compatible for communications over standard 3002 dial up and/or leased telephone lines.

The main controller shall provide for the management and supervision of anti-pass-back across terminal controllers and additionally for the management of Input to Output linking across terminal controllers.

3.3 Terminal Controllers

The terminal controller shall be microprocessor based with on-board time and date generation with battery to allow a minimum of 48 hours of data integrity. This device shall be responsible for all access control decision and alarm monitoring detection in the system at the terminal controller level.

It shall also be responsible for all its output responses to alarm detection and create the appropriate response through its processor logic. This controller shall be capable of maintaining a buffer of a minimum of 200 event transactions in the event of communications lost with its main controller.

Each terminal controller shall be capable of maintaining all 50,000 card holders in the system along with their access levels and time zones at the controller level. Systems that rely on a command from the computer to grant or deny access are not acceptable.

Each terminal controller shall be capable of interfacing the following card reader technologies, without the necessity of special interfacing panels or modules. Additional logic panels or personality modules are not acceptable. All reader technologies must be plug for plug compatible. The acceptable technologies

are Mirage Proximity, Wiegand Swipe, Dorado Magnetic Stripe and Threshold Keypads. Each terminal controller shall be capable of accepting two readers. In addition, each terminal controller shall also be capable of supporting two Checkpoint Threshold Keypads thus providing Card and PIN logic.

The terminal controller shall have all necessary provisions to implement access control for two doors. The capacity shall be present for two door position contacts, two request to exit input devices and two door strike outputs. These strike outputs shall control power to the door locking device and are to be rated at a minimum of 1 Amp at 24 VDC or .5 Amps at 24 VAC. For ease of service, these devices shall be connected to the terminal controllers through snap-in Buchanan type plugs. These controllers shall be labeled to insure the correct wire coding is followed and the appropriate devices are wired in the correct locations.

As standard, the terminal controller shall provide for two additional auxiliary inputs for monitored devices and two additional outputs for controlled devices. Each terminal controller shall provide for expansion capacity of 14 additional auxiliary input contacts and 30 form C outputs contacts through use of a plug on I/O Expansion Module.

3.3.1 Input/Output Expansion Modules

The system shall provide the interface of an I/O module to be directly interfaced to any and all terminal controllers in the system. This interface is accomplished through a manufacturer supplied cable allowing the I/O board to share the terminal controller logic, terminal controller address and power supply.

The I/O board shall be logic driven by the connected terminal controller and allow for the input contact and output control to operate as further specified. These abilities shall exist whether the terminal controller is on-line or off-line to the main controller.

Each input point shall have four (4) state supervision capabilities, i.e., secure, active, short, cut and shall allow a minimum 500

foot, overall shield, 22 gauge twisted wire run to each input device.

Each control output shall be single pole, double throw (SPDT) Form C relay. These contacts shall be rated for 1 Amp at 24 VDC or .5 Amp at 24 VAC. All outputs shall be made to allow for any of the following states to be programmed. Outputs shall be configured to latch, close momentarily (programmable from 1 to 120 seconds or 1 to 120 minutes) or set to reflect the state of the corresponding input or inputs. These states shall work in conjunction with outputs being managed under time zones and/or selected Events as well.

3.4 Input/Output Alarm Controller

The system shall provide support for I/O Alarm Controllers thus providing for 16 four state supervised monitored inputs and four (4) single pole, double throw (SPDT) Form C output relays. This will allow for modular and economical expansion of a system that requires extensive monitored points yet a limited number of card reader points.

4. NETWORK WIRING

The Controller communications network shall be made up of a primary main controller bus and secondary terminal controller bus. The communications protocol used shall be RS485. The primary bus and secondary bus shall use a shielded, dual twisted pair, Belden #8723 (22 AWG) or equal. Both bus networks shall be capable of a distance of 4000 ft., total wire. In addition, any point(s) between either the primary and/or secondary bus, shall have the capability of being connected using Checkpoint's OPTICOM Fiber Optics Repeaters. Fiber Optics Repeaters shall provide network wiring capability of a minimum of 4,000 feet between controllers using 62.5 micron Fiber Optic Cable.

The system communications shall be supervised for integrity. If communications is detected as failed, the system shall report the loss and automatically enable the affected controller(s) buffer. Systems that require Site Codes, Facility Codes, degrade to these

codes and/or do not buffer event information in the event of lost communications are not acceptable.

All reader cabling shall use a overall shield, 5 conductor West Penn #3280 (18 AWG) or equal. A reader shall be wired a minimum of 500 ft. without wire size change. Readers requiring a wire size change or special adapters to drive signal this distance are not acceptable.

Input and Output wire and cable requirements shall be application specific and shall use the proper shielded cable as required by the specific application and/or code.

5. THRESHOLD ENTERPRISE APPLICATION SOFTWARE

5.1 General

This section details the minimum requirements necessary for the application software. The software will be a Microsoft Windows NT application engineered as an Access Control and Alarm Point Monitoring program. It shall provide an integral solution for incorporating optional Checkpoint Video ID verification and Photo ID Badging, Closed Circuit TV Control, Time and Attendance, Paging and other third party linked applications.

The applications shall be Microsoft ODBC compliant and shall provide a relational database for export of Archive History and Card Holder data to third party software and applications. Of primary importance, the system shall be a graphical user interface using standard Microsoft Windows list boxes, option buttons, check boxes and mouse support.

The application shall provide an easy to use Graphical User Interface (GUI) with Icons for Event Monitor, Card Holder Database, Reports, System Administration, Installer and Administrator Setup, Operator Action, Alarm Response, Reminders, Time Zones, Groups, Events and Operators.

At a minimum, the Event Viewer shall allow for four separate Viewing Screens with client selectable events vectored to each

screen. Each event line shall contain at a minimum, an event number, a date and time, an event type and event description. It shall be possible for the client to select with components of the event lines shall appear in any event viewer screen. It shall be possible for an operator to select viewing on only one viewer screen, two viewer screens, three viewer screens or four viewer screens at any one time. It shall also be possible to use standard Windows sizing of the columns for event number, a date and time, an event type and event description.

The application shall provide a capability of defining a minimum of 512 card readers and 20,000 card holders, expandable to 50,000; 4,096 monitored input points and 8,192 controllable output points. The application shall provide on-help to insure an operators ability to receive on-line informational context sensitive help when required. The system points will be identified in English text with Client assignable definitions of Door, Reader, Keypad, Input and Output points. The application shall allow easy understanding of any event transaction in the system.

5.2 Time Zones

The application shall provide a minimum of 64 time zones. Time Zones One and Two shall be fixed as Time Zone Never and Time Zone Always respectively. The additional Sixty two (62) of these time zones shall be client definable and have a minimum of 8 definable intervals and shall allow a client assigned Time Zone description. These intervals shall be programmable for starting and stopping times assignable to individual days of the week. The intervals shall also define holiday usage. Time zones shall be assignable to doors, readers, card holders, outputs, inputs and selected system events.

5.3 Holidays

The application shall provide for enrolling a minimum of 32 holidays annually. Holidays, in conjunction with time zones, shall be assignable to doors, readers, card holders, outputs, inputs and selected system events. Client assigned Holiday description shall be possible.

5.4 Door Access Group Privilege Levels

The application shall have the capabilities to relate cardholders to readers for door access by time. It shall be possible to restrict any single card holder or group of card holders through the use of these access levels. The application shall have a minimum of 256 access group levels and shall allow a client assigned description of each. The application shall have the ability to create a privileged card holder group. This group shall be assignable to any or all reader(s) in the system and those cards assigned shall have 24 hour a day access every day of the year. There shall be a minimum of 8 card holders assignable to this privileged group per reader in the system. These privileged groups shall not diminish the 256 access level minimum in the application. The application shall provide the ability to generate a report on all 256 access levels and their client assigned definitions.

5.4.1 Assigning Access Group Levels

Each Card Holder in the system shall be assigned at least one of the 256 Access Level detailing the times, days of the week and holidays that Card Holder shall be granted or denied access to each Reader/Keypad within the system. Additionally, any Card Holder or group of Card Holders may be assigned a second and/or third access level from the list of 256, for access to other groups of readers/keypads. The assigning of a second and/or third level access shall not negate the access granted in the primary access level.

5.5 Door and Reader Configuration

The application shall allow all 512 doors and 512 readers to be configured for their own unique requirements. Each door shall be identified in client defined text form. Each reader shall be identified in client defined text form. The door strike unlock time and door propped open time are to be assignable independently for a minimum of 1 second to up a maximum of 120 minutes. All door unlocks shall be time zone configurable and once unlocked shall be configured to report state change at client's discretion. It is understood that the Request-To-Exit device will be capable of unlocking its related door; additionally, all doors shall be unlockable by a minimum of 2 auxiliary input configured

overrides. These inputs shall be described in client defined text form and overrides reportable based on an assigned time zone.

Each access controlled door in the system shall have the ability to generate a local alarm output in the event of that door being forced or left open beyond an allowable time. This local alarm output shall be configured to any of the following states: latched or timed. In the event of the output being latched it shall only be reset through operator intervention or the passing of a valid card at that door's reader. The reporting of these two events shall be time zone definable.

The door status shall be configurable to report the physical state of the door based on time and condition. The system shall provide at a minimum the following Door/Reader/Card Holder status events: Door Left Open, Door Forced, Door Opened and Door Closed, and Admitted, Admit In, Admit Out, Entered, Exited, Expired, Inactive, Is In, Is Out, No Access, Not Time, and Unknown Code. The system shall be capable of reporting by client assigned time zone, valid and/or invalid code presentations on a "per" reader basis. The system shall also provide for a "False Count" setting of zero to seven invalid code presentations prior to reporting the invalid code event. This feature is necessary when using numeric keypads as reader devices.

The application shall allow the client to program a message unique to each door and each reader in the system. This message shall appear automatically under alarm conditions for that door or that reader when any status event is set as an Alarm Level Event.

5.5.1 Anti-Pass Back

The system shall provide for enforcing "Anti-Passback" on doors controlled by an In Reader and an Out Reader. The system shall have a minimum of three methods for anti-passback forgiveness. The first method allows the system to forgive anti-passback at the controller(s) by time. The second method allows the system to forgive anti-passback by door groups or individual door(s). The third method allows a privileged operator to forgive anti-passback by card holder. Any method may be invoked by an operator so privileged.

5.6 Request-To-Exit

Each Request-To-Exit (REX) device shall be assignable to unlock its door on a time zone/holiday basis. If the device is not programmed to unlock the door the door contact shall still be shunted upon activation of the request to exit device. Additionally, reporting and archiving of the Request To Exit device Event shall be time zone/holiday assignable.

5.7 Input and Output Configuration

The application shall allow for a minimum of 4,096 monitored Input points and a minimum of 8,192 controlled Output points to be configured for their own unique requirements. Each input and/or output shall be client defined in text form.

Each of the input points shall have four (4) state supervision capabilities, i.e. secure, active, short, cut. Any input in the system shall have the ability to report a state change of Secure/Active and Cut/Short. The reporting by these four events shall be client definable by time zone.

It shall be possible to Shunt any input or group of inputs by an operator so privileged. A system status Flag shall display on the CRT Screens indicating that a Shunt action has been instituted and is in effect. The system Flag shall only reset upon all inputs being in an Un-Shunted state.

Each output shall allow for any of the following states to be programmed. Outputs shall be configured to latch, close momentarily (selectable for a minimum of 1 second to a maximum of 120 minutes) or set to follow the state of the corresponding input or inputs. These states shall work in conjunction with outputs being managed under time zones and/or selected Events as well. It shall be possible for an operator so privileged to control outputs from any workstation in the network. Privileged operators may activate outputs individually or in groups, on a momentary basis or latch outputs on or off using the mouse or menu driven commands.

It shall be possible for any input in the system to activate any output or group of outputs in the system. The relationship shall

be Local (any input activates any output under its same terminal controller), Regional (any input activates any output under its main controller on any other terminal controller) and Global (any input activates any output under any main controller on any other terminal controller). It shall also be possible for any Event, i.e., Log In, Log Off, Failed, Modified, Traced, etc., to activate any output in the system.

It shall be possible for any Access Level to activate any output(s) under a terminal controller thus providing (but not limited to) client required Elevator Floor Button control, HVAC control and Alarm shunting.

The application shall allow a client programmed message unique to each input and each output in the system. This message shall appear automatically under alarm condition for that input or that output when any status event is set as an Alarm Level Event

5.8 Device Configuration and Copy Feature

The application shall provide the ability to display a controller, door, reader, input and/or output configuration of any device in the system. While displayed, the configuration may be modified by a privileged operator if necessary. All or any portion of the configuration of a device may be copied onto any other like device using the time saving Copy Feature of the application.

5.9 Operator Interface, Alarm Handling and Overrides

5.9.2 Operator Actions

The application shall provide for an operator so privileged, the ability to take action on Doors, Inputs and/or Outputs. Selected "Operators" shall be granted ability to or restricted from, Locking, Unlocking, Momentarily Unlocking or Query Status of any door or group of doors in the systems. Selected "Operators" shall be granted ability to or restricted from, Turning On, Turning Off, Momentarily Turning On/Off or Query Status of any Output or Group of Outputs in the system. Selected "Operators" shall be granted ability to or restricted from, Shunt or Query any Input or Group of Inputs in the System. Selected "Operators" shall be granted ability to or restricted from, Refreshing or Query any Controller or Group of Controllers in the System.

5.9.2 Alarm & Status Events - - Priorities

The application shall provide client, the means to prioritize alarm status events. These events shall be generated from any of the nine event origins. These origins shall be as follows: System Events, Main Controller Events, Terminal Controller Events, Card Holder Events, Door Events, Reader Events, Input Events, Output Events and Diagnostic Events.

These events shall be configurable to any one of sixteen (16) priority levels which will display in unique corresponding colors. The color assignment shall permit selections from a basic color chart having samples and shall also provide for the user to configure custom colors down to the Hue, Saturation, and Luminosity level.

It shall be possible to route events for display in any one or more of the four event display quadrant screens, and/or printing, on any or all display and event printer devices on the system, based on event type. Each individual device event shall have the ability to be assigned different alarm priority levels in accordance to the needs of the client, i.e., Not Time event on Reader one may be assigned Alarm Level two, but the identical event, Not Time on reader two may only require an Alarm Level six response.

5.9.3 Alarm & Status Events - - Operator Response

The system shall also be capable of notifying the operator of designated alarms, set over a specific priority level, while the operator is in other access control screens or in other applications.

Events set as "Alarm Events" shall also have the ability to be designated as "Breakthrough," "Flash ICON Notification," or "Audible." Alarms for the security operator of the system shall be displayed and made interactive via an Alarm Annunciation screen.

"Breakthrough" alarms shall interrupt the operator's program being run and present the alarm notification box, in priority color, at the center of the screen. "Flash ICON Notification," and/or "Audible" alarms shall not breakthrough but will blink or flash the

alarm alert ICON to draw the attention of the security operator for response and disposition or sound the internal computer audible device.

Alarms shall be displayed based on priority. For each alarm priority queue there shall be a minimum of 256 unacknowledged alarms. All alarms displayed shall have the ability to be acknowledged singularly or as a group based on priority, by an operator so privileged. The application shall provide the ability to enter an operator response documenting action taken. The application shall provide annunciation of alarm events at any or all work stations as allowed by the Windows NT network; based on priority.

A simple click of the mouse on any selected "Event," shall bring up a "Detail" window with complete information regarding that particular event.

An alternate method of operator response using Icon's shall be through the use of Facility Maps and Graphics.

5.10 Facilities Maps & Graphics

The application shall be capable of allowing the creation of dynamic and linkable client created graphic maps. Applications using a separate video display screen to generate or display maps shall not be acceptable. The application shall be capable of using imported, client provided ACAD files for the creation of floor plans.

The applications graphics shall be able to represent system devices by use of "Icons". The icons shall be dynamic and reflect the real time status of the device it represents. The application shall provide a library of icons per device type in the system as well as allow for unique client defined icons. Any icon can be oriented and moved to reflect the actual installation of the device it represents. By selecting an icon in alarm, the application shall display text and alarm message in the same screen as the original map. Applications not able to display alarm text and message in the graphics screen are not acceptable. The application shall be able to allow operators to acknowledge the alarm represented by the chosen icon. Applications that can not

acknowledge the alarm from graphic map shall not be acceptable.

The application shall be capable of linking together graphic maps to provide multiple and expanded views of any system device and/or client area. The application shall provide links, each being numbered to represent the map connected to that link. The application shall also allow the client to provide a text description for the linked map.

These links, like the maps they are associated with are dynamic, and shall display the highest priority color of any device associated with the graphic map the link represents.

System graphic map screen format shall allow the display of an alarm queue for all 16 alarm priority levels. This alarm queue shall be real time and each level will increment any changes to alarms in the application at each level. As alarms are acknowledged the corresponding alarm priority will decrement its queue accordingly. Applications that do not give system alarm overview as part of graphic map screen are not acceptable.

5.11 Card Holder Database Configuration

The application shall provide a Microsoft compliant SQL relational database. The application shall have the ability to support 20,000 card holder records (expandable to 50,000 card holder records). These records shall have at a minimum the following fixed fields: card holder last name, card holder first name, card holder identification number, card holder PIN, card holder access group levels, card holder activation or deactivation status, card/PIN activation and expiration dates and individual card holder TRACE or LOCATION status, and card holder classification, i.e., Employee, Visitor. For ease of use, the application shall provide alphabetical TABS for selecting Card Holders by name.

The application shall also support 32 client-configurable data fields on eight restricted pages. These fields are necessary for maintaining but not limited to, vehicle license plate numbers, phone numbers, departments, addresses, etc.

The application shall provide client-configurable report capabilities that allow selection, search and sort combinations of any and all fields to be used to create desired reports. These reports once generated shall be displayed and/or printed at the client's discretion. Additionally, it shall be possible for an operator so privileged to perform a "Quick Search" of card holder extended data information, example, "Quick Search" an automobile license plate number.

The application shall provide the ability to set a validity period on the cardholder. This feature allows a cardholder to be activated and/or deactivated based on specified dates. The application shall provide the ability for cardholders to be placed in a minimum of two classes. These classes shall include Visitors and Standard. It shall be possible to generate a report based on Visitor cardholders only. It shall be possible to place any cardholder in a Trace status mode. A Traced Card Holder shall generate a separate event that may be displayed and/or printed when any Traced Cardholder presents their card at any reader in the system. The Traced Event shall allow tracking of selected individuals throughout a facility.

5.11.1 Social Security Number and ANSI Standard Format Cards

It shall be possible to set the application software to identify 12 digits of the 48 digit ANSI standard numbering format. This will allow for using Dorado magnetic stripe cards and ICI bar code cards that have been programmed with a card holder's social security number plus personal ID number.

5.11.2 Personal Identification Number

It shall be possible to set the application software to require selected entry points to grant access only when a valid Card Holder presents a valid Card in conjunction with a valid Personal Identification Number (PIN). The PIN shall be selectable from one to six digits. It shall be possible to enforce a Card/PIN combination by time zones on a "per" reader basis, thus allowing Card only entry during selected hours.

5.11.3 Duress Code

It shall be possible to set a system wide Duress Code that when entered at any Threshold Keypad will grant access to that entry point and in addition alert the Command Center of the Duress situation and entry point.

5.12 Operator Privilege Levels

The application shall have a client defined number of operators. Any enrolled card holder may be assigned operator privileges. The application shall allow the Client to distinguish between operator privileges by defining a minimum of 64 levels. Once defined, these levels shall allow an operator to have restrictions placed on them down to the point level. Each of these operator privilege levels shall be named for their group of operators. These operator privilege levels shall be English text definable.

An operator may be assigned an Operator Level of *view only* and thereby totally restricting those operators from modifying entries. The system shall alert any operator trying to access a restricted menu selection with an on screen message. The message shall state "Access Denied - See your System Administrator".

The application shall provide the capability of generating a report outlining operator privilege capabilities per level and a list of operators assigned to each Operator Level.

5.13 Reports

The application shall provide at a minimum, the ability to generate reports on the following criteria and allow (or restrict) so privileged operators, access to selective reports or all reports. The application shall allow for the creation of report "Templates" that may be set to filter a report for specific information. Once created, these templates shall be saved as modified for future and continual use. Report templates by only be modified by operators so privileged.

Event History Archive (minimum of 64 report templates)

Card Holder Configuration (minimum of 64 report templates)

Device Status

Card Holder Location Status

System Version

Time Zone and Holiday
Access Level Readers
Access Level Outputs
Input Output Control
Operator Level
Event Configuration
Class Configuration
Network Configuration
Graphic Configuration
Event Generated Output Configuration

5.14 Event Archives

The system shall allow event history to be written to the hard drive disk and accumulated as archives. The hard disk drive shall determine the amount of history archived but must support a minimum of 750,000 recorded transactions. Warning messages shall be standard Microsoft Windows in nature. The system shall have the capacity to off-load the archive files onto any standard medium including 3.5 inch floppy diskettes, tape drives, IO Mega Flopitical or SyQuest.

5.14.1 Event Archived History Reports

The application shall allow reports to be generated from the history accumulated on the system's hard disk drive and/or backup diskettes. The application shall allow any report template to be cleared or modified. Archived templates shall be created through a selection process of event classifications available. This selection allows individual event types to be selected by an all, some or none choice. An operator choosing a "Some" category shall be able to include or exclude any sub-category of any event type. The selection of none excludes the entire event type and all corresponding sub-categories. There shall be a minimum of 64 archive report templates in the application.

5.15 Who's In / Who's Out Report

The application shall have the capacity to generate a "Quick Status Report" giving a status as to who is in and/or who is out of a specified area. The report generated shall provide the following information: card holder by name, card holder access level, in/out status. This report shall be able to be created at any

time for any group of readers configured as read in and read out. This report shall be printed and/or screen displayed as desired.

5.16 Operator On-Line Help

The application shall provide help that is specific to the area of the application being used. The on-line help shall be context sensitive for general help, specific help and glossary of terms. These help screens shall be selectable by a single mouse click of the Help Icon.

5.17 Query Status of System Components

It shall be possible to query the status of any or all of the system controllers, access control doors, input and/or output devices. This status shall display dynamically the current state of the device in question. The application shall have the ability to group doors, readers, inputs and outputs into groups. Doors, readers, inputs and outputs shall have a minimum of 256 groups each, for a total of 1,024 groups. Each group shall have the ability to be described in plain English text. Each door, reader, input or output group may contain any number of its system devices and any device may be assigned to more than one group. Group Configuration provides a filtering mechanism during Report Generation and simplifies Operator Actions.

5.18 Filters and Use Of

The application shall provide for setting of Filters. Filters allow for placing Doors, Readers, Inputs, Outputs, Main Controllers, Terminal Controllers, and System Events in to a filter or multiple filters. These filters may then be used to easily request information or take action on any device within the selected filter.

5.19 Installation Configuration

The application shall provide for configuring a "Tree" or "Riser" of system devices consisting of Main Controllers, Terminal Controllers, Doors, Readers, Inputs and Outputs. These system devices shall then be placed in an Active Tree or Riser or kept in a Maintenance Tree or Riser. Placing a Maintenance device into an Active Tree shall be a simple matter of standard Windows "Drag & Drop" into the Active Tree Riser.

5.18 Backup and Restoration

The application shall provide the ability to archive a minimum of 750,000 events, and generate reports, print selectable to how and when. The software shall have the capability to back-up archival data to a standard 350Mb tape media automatically based on the system internal clock and be capable of formatting either a standard 3 1/2 inch, 1.44 MB diskette or 250 MB tape media in the background. It shall provide the ability to backup and restore archival history, reports, system configuration database, card and cardholder database.

5.19 On-Line Maintenance

The application shall provide on-line diagnostics and communications maintenance for adjustment to the operating environment. These diagnostics shall allow for the modification of baud rate, system packet information, and network polling. It shall be possible for the application to adjust the data handshake ability through channel commands and channel response. On-line maintenance providing real-time communications conditions of all system controllers is required.

The application shall be required to have the ability to generate a version report which notifies the operator of the current software version that exists in all NT Stations and polls all main and terminal controllers for the current firmware versions of all controllers on the network.

Copyright © 2000, Checkpoint Systems ACPG, [GMR Communications](#) & [Media Fusion Technologies, Inc.](#)

All Rights Reserved.

Copy and/or distribution in any form is strictly prohibited.