

# Softcon BMS Requirement

Version 01.17

# CONTENTS

<b>1</b>	<b>OVERVIEW .....</b>	<b>3</b>
<b>2</b>	<b>REFERENCES .....</b>	<b>3</b>
<b>3</b>	<b>OWNERSHIP / GUARANTEES .....</b>	<b>3</b>
<b>4</b>	<b>STANDARD SPECIFICATIONS .....</b>	<b>3</b>
<b>5</b>	<b>SYSTEM ARCHITECTURE .....</b>	<b>3</b>
<b>6</b>	<b>ACCESS CONTROL CARDS .....</b>	<b>5</b>
<b>7</b>	<b>READERS .....</b>	<b>5</b>
<b>8</b>	<b>CONTROLLERS .....</b>	<b>5</b>
8.1	General.....	5
8.2	Access, Input/Output controllers .....	6
8.3	Mimic driver controllers.....	7
<b>9</b>	<b>COMPUTER SPECIFICATIONS.....</b>	<b>7</b>
<b>10</b>	<b>SOFTWARE .....</b>	<b>8</b>
10.1	General.....	8
10.2	Security levels .....	8
10.3	Language support.....	9
10.4	Schedules (Time zones and groups), Holidays.....	9
10.5	Data display and editing .....	9
10.6	Activity displays .....	10
10.7	Graphical displays .....	10
10.8	Events.....	11
10.9	Counters .....	11
10.10	Timers.....	11
10.11	Access control .....	12
10.12	Card holders .....	14
10.13	Card ACCESS ZONE DISPLAY.....	15
10.14	Card maker .....	15
10.15	Visitor control.....	16
10.16	Input/Output.....	17
10.17	Vending, Fuel management, POS.....	18
10.18	Parking.....	18
10.19	Time accumulation, T&A .....	19
10.20	Asset management.....	20
10.21	Message displays .....	21
10.22	Operator occurrence log.....	21
10.23	Audio wave files.....	21
10.24	SMS .....	21
10.25	Email.....	21
10.26	Tele-Call Control.....	22
10.27	Logging .....	22
10.28	Reports .....	22
10.29	Interfacing to host programs.....	22
10.30	Back-up storage data .....	23
10.31	On-line help Windows.....	23
10.32	Software version and upgrades.....	23
10.33	Video Linking, *Video /camera control .....	23
10.34	*Control via WWW.....	23
10.35	*Guard tour .....	23
<b>11</b>	<b>TESTING – SIMULATION AND MONITORING .....</b>	<b>23</b>
11.1	HW Off-line .....	23
11.2	SW On-line, off-line .....	23
<b>12</b>	<b>FUNCTIONS / OPTIONS SUMMARY.....</b>	<b>25</b>
12.1	System.....	25
12.2	HW.....	25
12.3	SW .....	26

# 1 OVERVIEW

The system shall be capable of providing the following building management functions:

- Access control.
- Vehicle control.
- Visitor Control registration.
- Visitor pre-registration via email.
- Vending control, including Point Of Sale.
- ID Card generation.
- Alarm monitoring and intrusion detection.
- Control of doors, gates, sirens, lighting, etc.
- Mimic panel control.
- Time accumulation.
- Link to Time attendance systems.
- Asset management.
- Integrated video (camera selection and control, snap-shots).
- Random search.
- Integrated video (camera selection and control, live display).
- Guard Tour.
- Available in future versions

All these options shall not be required initially but shall be available for future expansions. The appendix lists functions that shall be included initially as a minimum. Options not required shall be priced as separate items and prices shall be valid for one year. Throughout this document, the term 'could' implies that if the option is required, the option 'shall' function as required. Requirements stated as "x or y", implies that either of options x or y shall be available if required, but not together. "X and y" implies that both shall be available at the same time. "X, as an alternative y" implies that only one option shall be available, the other not.

## 2 REFERENCES

The system must have a wide installation base and be proven to be stable and reliable in the 24 hours a day, in both small and large applications. Contactable references must be provided.

## 3 OWNERSHIP / GUARANTEES

Guarantees as provided by the manufacturer shall be transferred to the client and be a minimum of a one year guarantee against fault components and bad workmanship. All design / manufactured errors must be corrected as soon as possible and the manufacturer must support the equipment for a minimum of five years.

All equipment shall be installed to the manufacturer specifications/instructions by approved, certified installers.

HW maintenance procedures shall be made provided to aid in the repair of HW. If so required, the circuit diagrams and source code must be lodged in trust to be made available to nominated parties on defined circumstances.

Once all parties have been paid, all products become the property of the client.

## 4 STANDARD SPECIFICATIONS

All HW shall be UL and CE compliant. All warning notifications, dielectric tests (alternating current potential of 1200V is passed through the transformer for 1 second) and radiation requirements shall be adhered to.

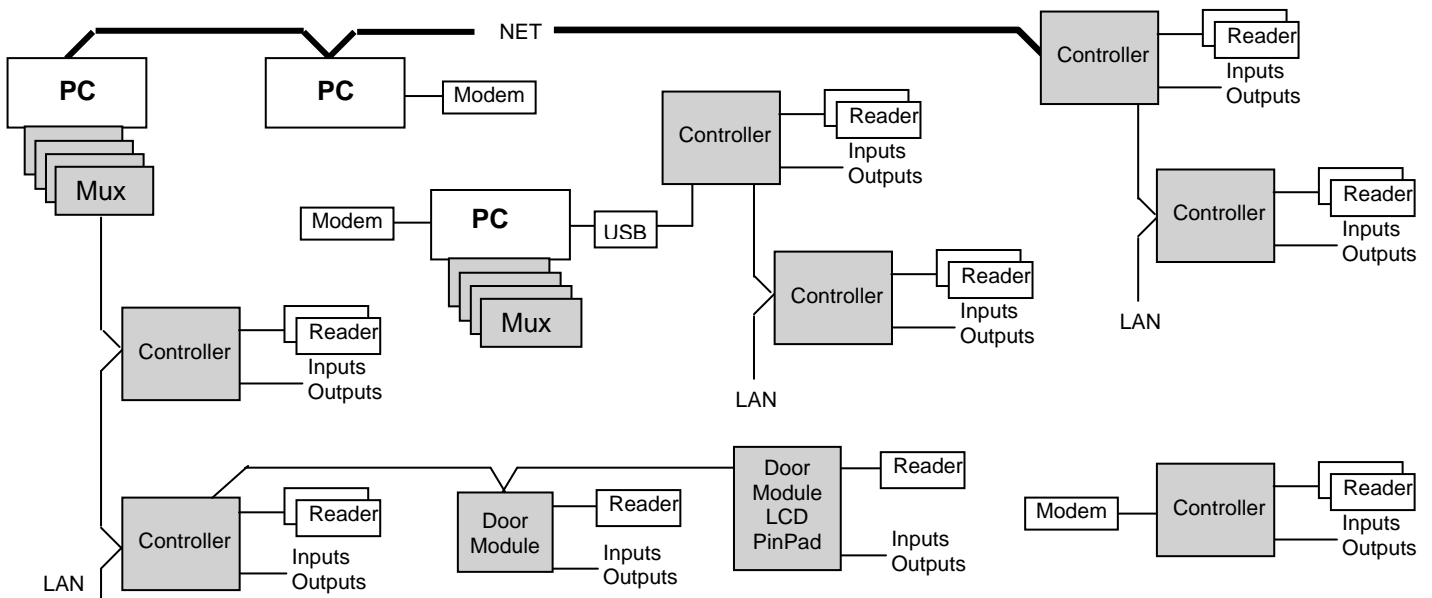
## 5 SYSTEM ARCHITECTURE

Intelligent field control panels (controllers) shall perform all functions in a stand-alone mode and shall monitor and control all inputs and outputs on set time-groups (schedules), with changes being reported. The only non stand-alone functions shall be for linking, counting, time-out, inter-controller anti-pass back (APB) and zone enforcing. Controllers shall contain all relevant set-up and card databases in local battery backed-up memory. Access controllers shall interface to 2 card readers directly, or via door control modules on a RS485 link.

Data between the controllers and PC(s) shall be transferred via Local Area Network(s) (LAN) and PCs shall be linked via PC networks (NET). The LAN shall use a multi-drop RS485 interface via shielded twisted pair cables (maximum of 2000m cable) or fibre optical links (maximum of 4500m per segment) where distance or higher level of isolation is required. The NET shall use TCP protocol via UTP or fibre cables, linked via hubs.

Communication on a LAN shall be via intelligent interfaces installed in to the PCs PCI bus (at least 4 per PC). The data packets must contain checksums and error detection and repeats are to be done by the interfaces. Power loss at a controller must not affect RS485 communication to other controllers. Fibre interfaces that regenerate communication must have UPS units. It shall be possible to connect at least 254 controllers per LAN and sub-LAN controllers must be available, providing the capability of having 4 x 254 x 254 (258,064) controllers per PC. LAN communication shall be at 9600 or 19200 baud and data transfer must be maximized with off-line controllers only being re-polled every 5 minutes. Empty data packets shall typically be transferred within 5 or 10 msec (19200 or 9600 baud) and packets with data within 10 or 20 msec. A transaction rate of 15,000 per hour shall be achievable, with LAN speed and protocol not the limiting factor. When LAN communication is stopped or not available, controllers shall buffer 1000 transactions in battery backed-up memory. Controllers shall time and day of month stamp all transactions.

Where LAN cables are not available, communication shall be via on-line or dial-up modems (up to 4 modems per PC). Dialling schedules shall be set for each controller with modem and when a connection is required, an unused modem shall be selected and the number dialled. Alarms at controllers shall result in auto dialling. When connection is made, the databases shall be synchronised and events transferred to the server. A password shall be set per dial-up controller. Similarly to dial-up, it shall be possible to connect controllers directly to PCs via COM ports, RS232 (only one controller to a port).



Controllers should optionally be directly connected to PCs the system via TCP/IP or USB connections. Such controllers could also serve as LAN controllers, transferring data between the PCs and the controllers on the sub-LAN.

Events and alarms shall be reported to the PCs in the system on active time group, which log, display, print and possibly generate new events or set-up changes as a result. All functioning of controllers, alarms, events, displays, etc. shall be set at the PC and kept in database files. Changes to set-ups shall automatically be sent to the appropriate PCs and controllers.

PC SW shall be implemented in a server (communicates with databases) and clients architecture. Data transfer between Clients and Server shall be by TCP/IP & Port Number and client applications could be installed on remote PCs or on the same PC as the server. Client applications shall interface to controllers via the LAN and all the editing and displaying of data done via the clients. Client programs shall be optimized for speed via RAM tables and should the server or the link go down (i.e. off-line), changes shall be stored at the client and the server updated when the link is re-established.

In multiple servers systems where PCs function independently (with own servers programs), systems shall be synchronized on time schedules with repeats, synchronizing edited data and transferring log and audit files as required. Synchronizing events shall be logged and scheduled events optionally logged (errors always logged). The links between the systems shall be TCP networks (not requiring sharing of drives / directories) or dial-up modems. It shall be possible to use multiple modems with an automatic selection of a free modem. Alarms could be set to be automatically sent to certain servers.

PCs and controller shall synchronize date and time when connection is made and within every 90 minutes there after. PCs to which date/time is synchronized shall be selectable. Changing the date/time on any PC shall result in all on-line PCs and controllers being synchronised. Setting of the time and date shall be performed via password protected menus, not requiring access to the operating system.

## **6 ACCESS CONTROL CARDS**

Cards shall be of robust PVC material and construction, credit card sized and be proximity, passive (read range of 10cm.) and permanently factory encoded with numbers & facility codes. Cards shall be suitable for direct printing or be detailed by sticking on specialised printed sticky labels. All cards shall have printed numbers. Various clips and holders shall be available.

## **7 READERS**

The controllers shall be able to interface directly to card / tag readers with the following interfaces:

- 2-wire Wiegand
- Data/clock
- 1-wire Dallas
- Serial – RS485 or RS232 (9600 baud)

Card code structures that could be read are:

- Wiegand 26, 30, 32, 34, 35 (Corporate 1000), 36, 37, 38, 40, 44 and 52 bit. Cards could have a facility code and coding could be binary or in binary coded decimal (BCD). Checksums shall be verified. Data could be received starting with the least or most significant bits (card swiped in either direction). New card structures shall be facilitated by additions to look-up tables.
- Magnetic cards, track 1, 2 or 3. Coding shall be in binary or according to the ISO7811/2 standard. Character checks bits and longitudinal redundancy checksums shall be verified. For ISO cards, the location of the facility code and card number shall be configurable. Alternate card number locations could be set for when facility codes do not match (enabling the use of staff cards and guest cards at the same readers.
- Dallas random touch tags.
- Any popular barcodes that can be decoded via the appropriate readers.
- Hitag, Mifare or ISO 14443 smartprox, read/write.
- Tag receivers.

Readers shall be capable of reading random card numbers of up to 10 hex digits.

It shall be possible to interface Biometric Readers (such as finger print and palm readers) between readers and controllers, verifying the cardholder. Fingerprints shall be linked to cards – cards can be used or not. For access control, all fingerprints shall be stored in the readers (up to 48 000, reader dependant). The addition of these readers shall require no addition settings to the normal access system.

It shall be possible to interface Biometric Readers (such as finger print and palm readers) that connect via TCP networks or serially to PCs to read and register fingerprints and grant or deny access according to normal access control functions.

It shall be possible to use digital Keypads (Pin Pads) in a 3 \* 4 matrix instead of readers or in conjunction with readers and to set time groups for when each reader and Pin Pad must be used. Pin numbers from 1 to 6 digits could be used. Cardholders given a zero pins shall require only a card for access. A duress alarm shall be given when a zero digit is entered before the pin number, with all access functions applicable to a duress event.

Three LEDs shall be controlled per reader (via 2 or 3 line control) – Flashing (or optionally steady) amber when reader is enabled and ready, green when access is granted or door is open and red when access is denied or the reader is disabled. Both red and yellow shall indicate incorrect card type or facility code or parity error. In 2 line control, amber is created by both red and green on.

## **8 CONTROLLERS**

### **8.1 GENERAL**

All controllers shall be intelligent, microprocessor based control panels that function within the system architecture as described above.

Controllers shall be supplied with 110 or 220VAC (10W, excluding latch and reader power) and shall optionally have integrated 6 AH UPS, or could be supplied with 9 to 12VDC (700mA, excluding latch and reader power). It shall be possible to monitor UPS mains power failure. All set-up, card database and buffered data and real time clock shall be battery backed up (10 years with the power off). The RTC shall be synchronized to the PC RTC when the controller goes on-line and within every hour thereafter.

Controllers shall be contained in white powder coated steel metal housings; with key locked hinged lids (lid opening shall be monitored). Additional cover plates with appropriate high voltage warnings must protect power supplies. Mains supplies shall be filtered and transorb protected on the entry to the housing. Sufficient knockouts and cable space must be provided for cable entry and routing, with cables routed appropriately away from the PCBs. The housing and lid shall be appropriately earthed to the mains earth and terminals provided to earth cable screens. Reader cables screens shall be earthed and LAN screens earthed per segment and the segment screens isolated from one another.

All connections shall be via unpluggable, high quality terminals. Terminal connections, link and switch options shall be listed within the housing and an installation booklet provided with each controller. IC shall be mounted on high quality tulip IC holders.

Diagnostic LEDs shall be visible on the outside of the housing and mounting should be such that they are visible. LEDs shall indicate that the controller is on and running, the status of the LAN and the reader and I/O activity.

Controllers shall endure environmental conditions of -20 to 65 degrees C storage (-46 to 150 degrees F); 0 to 45 degrees C operational (32 to 113 degrees F); 80 % humidity non-condensing. Where controllers are mounted within enclosures, sufficient external ventilation shall be provided.

Communications with controllers shall be RS485 (data, /data and RTS, /RTS) or RS232 (with modem option) and be transorb protected and have serial protection resistors. Fiber optical interfaces and additional resistor/ capacitor/ inductor/ transorb/ surge arrestor interface shall be installed where greater distance and protection is required. The fiber interface shall be mounted in the enclosure and powered by the controller. The additional protection interfaces shall be mounted externally. Modems shall be installed within the housing where required. Total cable lengths shall be 2000m for RS485, 30m for RS232 and 4500m per fiber segment. RS485 cables must be terminated at the two ends with the characteristic impedance (typically 120 ohm). USB or TCP/IP connection between PC and controller shall be an option.

The controllers shall have a unique electronic ID and have SW version information that are reported to the PC.

Controllers shall have a minimum of 15 input, 15 output, 15 access, 15 reader enable, 15 Pin Pad and 15 latch control time groups (schedules) and 30 holidays that are selected for when I/O and readers are monitored and controlled and when access is granted or denied. An alternative selection of 60 time groups, with 8 time zones per 15 time groups shall be possible, with any of the time groups selected for any of the time functions.

It shall be possible to expand I/O locally (in the same housing) to 80 inputs and 60 outputs and remotely via multi-drop 1-wire or IIC interfaces. Relay, supervised inputs and temperature sensor interface modules shall be available. All relay contacts shall be protected against fly-back (RC-network for AC loads and diode for DC loads) at the load (externally to the controller).

Controllers shall contain SW and HW (power monitored) watchdog reset circuits.

Controller status changes shall be reported to the PC, these include on-line and off-line (by the PC communication interface) and power-up (by the controller).

High level languages shall be used in Firmware development where possible, with machine code only used when speed is critical.

## **8.2 ACCESS, INPUT/OUTPUT CONTROLLERS**

Data/clock and Wiegand reader interfaces shall be opto-isolated or transorb protected and the maximum cable lengths of 100m for 12V readers and 20m for 5V readers.

Controllers shall have at least 16 supervised input ports (short and open circuit, contact open or closed) – expandable to 80, and 12 output ports - expandable to 60 - that are relays (rating 28VDC/250VAC, 3A) or

open collector (rating 500mA/50VDC). Input ports shall be SW configured for functionality as Action complete, APB enable, APB reset, Auxiliary input, Booth occupied / continue, Card capture detect, Egress, Reader enable, Reader tamper or Latch monitor, Random Search; and outputs as Auxiliary output, Booth busy, Buzzer, Capture, Latch or Reader Isolate, interlock busy and Random Search. I/Os shall be set for active time group for each detection level and auxiliary inputs as counting inputs, with count changes reported to the PC after set time-out after count incremented. Card capture units shall be set at either or both readers. Random search and output control on card output group shall function in an offline mode.

The controllers shall function in a stand-alone mode with a local card database of up to 196,000 sequentially numbered or 65,000 (10 digit) randomly numbered cards (32,000 with PIN). It shall be possible to select 16 digit cards. All access functions shall be controlled locally, and access granted, denied, card captured, card not captured, door not opened, etc. are reported to the PC. APB and anti-time back (ATB) shall function locally between the two readers. APB setting shall be to disable reader used / enable other or disable both. APB reset shall enable all cards for both readers if enabled for either or regardless of current enable.

Access configured I/O shall be set as normally open/closed (or changeover for outputs), with time-outs and time delay options. Booth/mantrap control shall be done locally with doors, latches and presence being monitored and a booth busy output could be configured. Setting the interlock option shall prevent both doors opening. Readers and egress shall be disabled on command from the PC, on linked inputs or on time groups. Local alarms of illegal door openings, open too long and illegal access requests shall set local alarm outputs. Multiple illegal requests could disable the reader.

A multi-output control (typically lift control, alarm activation) option shall be available - via relays controlled locally by outputs of the controller – each card allocated an output group 1 to 64. Each output group shall be allocated function(s), with a maximum of 128 functions in a controller. A function shall be linked to an output group number and is set a reader number of the controller, the output action (activity) and a time group (output is only activated when the time group is active). Activities will be: nothing, off, pulse, till out group input changes, follow latch, follow door open, toggle or on.

It shall be possible to view and edit data in the controller with a hand programmer that is connected via a peripheral serial port, with an option of an on-board LCD / PIN pad.

Peripheral serial ports shall be available that can communicate to readers (with 3x4 Pin Pads, and 2x16 LCD back-lit displays), door control modules (that have a reader and supervised door I/O interface), tag receivers or peripherals such as note readers, printers, vending machines, etc. (may require specialized SW). It shall be possible to display the real time and the access status (e.g. “denied” or “proceed”) and PC messages such as the cardholders name, available subsidy, accumulation time, messages, etc. on the LCD.

### **8.3 MIMIC DRIVER CONTROLLERS**

It shall be possible to install controllers that display the status of inputs via 128 x LEDs to on, off or flashed (in alarm, not accepted) Local accepts alarm and lamp test shall be reported to the LAN.

## **9 COMPUTER SPECIFICATIONS**

The minimum requirement is a PC running and compatible with Windows 2000 or XP operating system:

Processor:	Pentium III 1GHz.
RAM:	128M (256M if more than 5000 cards, or high number of events).
Hard disk:	1G.
Video:	1024 x 768 SVGA with true colour.
PCI slots:	1 to 4 slots for MUX cards.
CD or CDW:	Required for Windows and SoftWin3 installation and updates.

Optional:

Stiffy or CDW:	1.44M stiffy or CD-writer for backups.
Network:	100MHz TCP-IP (if required).
Modem:	Required for remote sites and access to Internet (56k or better).

# 10 SOFTWARE

## 10.1 GENERAL

The PC SW shall have been developed by a certified Microsoft Solutions Provider using Visual C++ (32bit) and incorporates COM object modules. The platform is Microsoft Windows 2000, XP or Vista operating system. The SW shall comply with the requirements are described in the system architecture section above.

The SW shall effectively allow for modular implementation, with numerous options, features, maximums, etc. being switched off, hidden, not enabled or set as required (purchased options and/or user setting). Options and upgrades are listed below.

The SW architecture shall be client / server programs, with the server program executing database read and write functions using the Structured Query Language (SQL). Connection to the database shall be open via ODBC's, facilitating connection to practically any database (MS Access, Oracle, SQL Server - 2000, 2005, 2005-express, with authentication or not). MS Access 2000 shall be the standard used with the server program installed where the databases are located, with no SQL command being executed over a network. When the server starts running, databases shall automatically be compacted and selectively checked for correct fields and types and the set number of records. If incorrect the data shall automatically be repaired or repaired on query and defaults shall be set for records to be added. It shall be possible to set/change databases location, file name, table and field names and field types, size and indexing and fields could be set as unique, preventing duplication (e.g. unique ID, card and employee numbers). Via command line options, it shall be possible for clients to connect to predefined servers (e.g. to server running on local PC, PC xyz or on PC abc).

Databases shall selectively be password protected and encrypted and passwords and menu access setting shall be encrypted and can only be changed via the appropriate menus and password levels.

The software shall be highly configurable and be event-driven, with a variety of objects available in the system, namely Readers, Inputs, Outputs, Controllers, Cameras, Counters, Timers, Event buttons, EXE buttons, System, Base products, Vend items, Asset receivers and Venders. These could be virtual objects (memory based) or allocated to hardware and the status of these are set/ reset/ incremented/ decremented via events.

All access control functions shall generate events and include a variety of anti-pass back, time-back, strictly from, time-out in area, zone counting, visitor control, asset tracking, Video integration, trade union lockout, etc. functions. Except for specialized functions (e.g. visitor cards that are linked to host), access shall be granted or denied by the controllers that contains a local databases of the latest cards to have been graded access at the controller.

It shall be possible for events to generate audio and graphical indications, photos (bmp/tiff/jpg), database items, messages, activity logging and video recording. The controllers shall report I/O changes on active time groups.

As on option, Point of sale (POS) shall be incorporated in to the system as a separate exe client program and it shall be possible to incorporate Vending applications such as canteen and vehicle park entry control, cashless vending, Photostat-, Laundromat-, Car wash control, fuel pump control, cash loaders, etc. An add Cash module shall be available as a separate exe client program.

The set Windows date and time formats shall be used and for clarity and simplicity the format YYYY-MM-DD HH:mm:ss shall be set.

## 10.2 SECURITY LEVELS

It shall be possible to set any number of users as members of multiple user groups, with user groups set to have access to menus, displays, records, fields and every item shall be set as not visible or as not editable / selectable. List boxes and combo boxes shall be set to select and/or display options per group. Editing in combo boxes shall be password protected.

Users shall be set with start and expire date/times and passwords could be set to expire, forcing the user to change password. Logging off shall revert to a default group whose access rights are configured. As on option, users shall log-on with reader connected to the PC (password required), or with a fingerprint reader connected to the PC (password not required). Application settings (window position and size) shall be stored

per user. Auto log-off could be set, logging off after a set time-out of no operator activity. The name of the logged-on operator shall be displayed in the Windows header.

### **10.3 LANGUAGE SUPPORT**

All display and print strings shall be set in data files, facilitating the change thereof to different languages and **language choice shall be set per user.**

### **10.4 SCHEDULES (TIME ZONES AND GROUPS), HOLIDAYS**

Time related functions (e.g. when access is granted) shall be set via time groups. There shall be a minimum of 15 groups per function, with 8 time zones per function. The functions shall be:

- Access control (when access is granted).
- Reader enforced (when reader must be used when requesting access).
- PinPad enforced (when PinPads must be used when requesting access).
- Unlock of access control latches.
- Input monitoring.
- Output control.
  
- PC buzzer control (when the PC buzzer must sound on alarm).
- System group 1 (additional groups used in PC time functions).
- System group 2 (additional groups used in PC time functions).
- System group 3 (additional groups used in PC time functions).
- System group 4 (additional groups used in PC time functions).

PC time functions shall use any of the time groups, time groups used by controllers shall use only the relevant groups (top 6 above). An optional setting for controllers shall allow selection of any of the first 60 groups for any of the relevant function.

A group shall be set active for time zones per day of the week (Monday to Sunday) and for holidays. Holidays settings shall have precedence over day of the week, i.e. if not enabled for a holiday, the weekday setting are ignored on holidays. 30 holidays could be set.

Access cards shall be allocated a time-group limiting when access is granted or time group for each area zone for the cards area group shall be used.

It shall be possible to use time groups in event algorithms, with the time group being true when active at the instant the time group is tested.

### **10.5 DATA DISPLAY AND EDITING**

It shall be possible to log all edit functions in audit files (file per day). Changes affecting controllers shall automatically be sent to the appropriate controller(s).

All set-up and card data shall be accessed via list and/or property sheet displays and all displays and items on a display are set to be invisible, displayed and editable according to the logged on user. Displays shall selectively be set to be updated in real-time. Where appropriate, data shall be referenced to other databases with the descriptions being displayed and selections made via list or combo boxes, with combo boxes set for editing and/or selection. List and combo box data selection shall be set linked to password groups (e.g. certain operators can only make certain selections from the list). Changing list / combo boxes to text boxes shall be possible by changing configuration set-up (does not require SW changes).

A list shall comprise of rows and columns of data similar to a spreadsheet, with a row displaying a record of data and the records displayed via selected filters. These filters shall be administrator defined SQL command. Columns are fields and it shall be possible to order and change the width by simple click and drag actions. Column names shall be editable and columns be hidden, or set as visible (faded) or editable. It shall be possible to display columns in bold font. Sorting of records (ascending or descending) shall simply be by clicking on column names and multiple sorting of records shall be possible (e.g. sort by department, then by name). The displayed color of the data shall be set to change depending on the value of data in the record (set via administrator defined SQL commands), typically alarm conditions are displayed in bold red and normal conditions in green. Administrators shall be able to create new lists and lists ordered in menus for status (displaying the current status or readers, inputs, outputs, etc.) set-up, card data and vending. A variety of lists shall be provided, showing inputs in alarm, not accepted, etc. It shall be possible to print the visible columns for selected rows (with column names and widths as displayed).

Property sheets shall display the data of a record and be logically grouped in tab pages (e.g. card data is divided in to personal information, access information and vending data, etc.). It shall be possible to set items in property sheets as mandatory – must enter data before moving to another display.

Editing aids shall be available by right clicking on an item (or multiple selected items or record, inversed) and selecting find, delete record or field(s), default record or field(s), copy record or field(s) (copied to clipboard or to selected card/cards) or paste record or field(s) from clipboard or selected card.

Batch load functions shall be available by setting a search criterion (a property sheet identical to a card, with non null setting used for the search) and load data (a property sheet, with the non blank/null settings over writing the found card settings).

Wizards to simplify set-up shall be included. These use minimum keystrokes and follow logical patterns and provide access to all required functions, with appropriate defaults set automatically. Non-required settings shall be hidden (e.g. only two level setting are displayed and set if an input is not supervised).

Date selections shall be aided with calendar displays and date/time formatting.

It shall be possible to connect serial or USB card and barcode readers to PC COM or USB ports at settable baud rates and bit structures (including parity) and to incorporate a reader with the keyboard. Where appropriate, cards and barcodes are read to find card holders and items and used to edit card numbers and item codes. Data masks shall be set for serial, USB and key readers, filtering data read to match data in the databases. It shall be possible to use USB smart card readers.

Changing of window sizes, positioning, minimizing / maximizing / iconizing shall be password controlled.

## **10.6 ACTIVITY DISPLAYS**

Activity displays shall be provided that are scrolling list displays (500 line buffer per display), displaying selected events as they occur, each display with a selected filter (e.g. one display alarms, another card movement) and own size (newest displayed at the bottom). Columns shall be sized, hidden, ordered and activity scrolling be paused (scrolled, ordered by column, data copied, printed) and restarted.

Each input, output, counter and reader event shall be set for display or not, for each status (e.g. display a door opening, not closing) and displays could be time selected (e.g. certain door openings are only displayed after hours). Settings shall be available to select which PC(s) activities are to be displayed.

## **10.7 GRAPHICAL DISPLAYS**

Pixel based animated graphical drawings with symbols linked to each status of inputs, outputs, readers, etc., shall indicate the status of all monitored and controlled objects in the system. When objects change status and are in alarm, the symbol shall flash in inverse video until accepted (by clicking on the flashing symbol) or the generation of an accept alarm event (by clicking on an event button or generated by other means). When an alarm is accepted, the current status symbol shall be displayed. Drawings with alarms shall automatically be displayed on the top of the desktop. It shall be possible to link drawing to other drawing (via item icons) and to have sub-drawing (right click on an item icon).

It shall be possible to display and edit database items and counters on a drawing and to link data and photos to cards presented to readers. Clicking on certain display items shall generate events (e.g. disable a reader, open a door), open other drawings or run programs, batch files or scripts.

Drawings and every item on a drawing shall be set to be visible or editable for user groups.

A library of bitmaps, jpeg or tiff files symbols shall be provided and can be added to, with a background to a drawing also a symbol. An item shall be a symbol or text.

The creation of drawings shall be via an integrated drawing module. It shall be possible to add, delete or modify items and free text and to copy (as a single item or as a group – with distances between them fixed), align, equally space, bring to top or send to back of display. WYSIWYG editing features shall be incorporated with pixel position settings and display. Font, size, rotation, color and attributes (bold, italics and underline) of text and database items shall be settable, with an undo provided. Hot keys shall be available to simplify editing.

## 10.8 EVENTS

Events shall be generated by occurrences that happen in the system:

- Hardware. I/O changes, reader activity, status changes, etc.
- System. As a result of events, generate new events, e.g. when a CARD OUT-OF-AREA event is received from a controller and the card is checked as not out of area, a CARD ENABLED event is generated.
- Operators. Changing set-up, clicking on buttons, log-on, etc.
- Set time. Fixed time of day with settable repeats, after time-outs.
- Set events. Events generated on set algorithm of event triggers.
- Set counters. Counters that change as a result of event triggers.
- Set timers. Timers that time-out (started by event triggers).

Events shall be set as normal or as alarm by the system (e.g. power-up is always an alarm), on set time group (e.g. a monitored input closes after hours) or as set by event generators (e.g. by an operator button or on a timed event).

Event occurrences shall be set to be logged (to a daily log file on disk), printed as they occur, used as triggers to generate new events and be displayed (on activity lists or graphical displays), or only on active time group (when the event occurs, the set time group must be active). Certain events actions shall be fixed (e.g. power-up is always logged, printed, event-trigger, display), others shall be settable (e.g. every input level is set).

Events shall be used as triggers to increment and decrement or calculate the sum of counters, trigger new events or start programs (on set PCs), batch files or run scripts (with set parameters) and set/reset the status of objects. New events and start of programs shall be on an algorithm of events, statuses (e.g. disable a reader when a counter becomes maximum and an input is in a certain level) or on a sequence of events. Set card triggers referencing virtual cards, use the referenced card as a mask to match card events tested as valid trigger (allowing specific cards as triggers or a group of cards). Sequences shall be set to occur within set time-outs (HH:mm:ss) between events and shall typically be set to require a sequence of cards (specific and/or group) before an open door event is generated. It shall be possible to use time groups in algorithms, with the time group being true when the time group is active.

It shall be possible to set events that change card properties – status (en- / disable / capture), area group and time group. Changes shall automatically be sent to controllers and the changes audited.

## 10.9 COUNTERS

Counters shall be kept on entries per reader and every input and output shall have a counter, incrementing when the input or output changes to a count level set per input or output (e.g. when the door opens). It shall be possible to reset these counters with events, recording when the counter is reset.

It shall be possible to create virtual counters that increment or decrement by set values on specified events (triggers). The new count value shall be reported as an event count minimum (the new count is equal or below a set minimum), as count maximum (the new count is equal or above a set maximum) or as count available. These new events shall be set to be logged, printed, and displayed or to be used as a new trigger for new events or counters, or only on certain times (via a time group). It shall be possible to set counters to any value via events.

It shall be possible to set inputs to be counters, with the count being done in the controller. A timeout of 0 to 99 seconds shall be set after which the change in count is reported by the controller (the latest count is reported). Counting shall only be done when the set time group is active for the input.

Counters shall be settable to be the sum of other counters, with the calculation of such a counter triggered on any event.

## 10.10 TIMERS

Timers that generate set events on time-out shall be configurable. On algorithm of event triggers, timers shall be set to start (reloads pre-set to current value and continues), stop, set current value or continue with current value. It shall be possible to pre-set timers to cycle, reloading the pre-set value and continuing on time-out.

## 10.11 ACCESS CONTROL

**Area zones** shall be defined that are physical locations and are named appropriately, e.g. "OUTSIDE", "RECEPTION". Each reader shall be set with an area zone in (access from) and an area zone to which access is requested (access to).

**Zone linking:** It shall be possible to link area zones to other area(s) for anti-pass back (APB) purposes, for example: reader A gives access to zone "OUTSIDE VISITORS/STAFF" and reader B gives access to "OUTSIDE STAFF". Visitor cards are set to only exit via reader A (which has a card capture unit) and not via reader B (no capture unit). Staff can exit via reader A or B. Both readers give access to the same physical area zone, but B is configured to ensure capturing of visitor cards. If APB is used on staff cards, the two "OUTSIDE" areas need to be linked to prevent APB problems.

**Area groups** are a selection of area zone(s) to which cardholder(s) have access. Each card shall be allocated an area group, which can be unique to the card, or cards can share groups (e.g. cleaner group, admin group), or be allocated multiple groups, e.g. parking group and 1<sup>st</sup> floor group. Area groups could be batch loaded with area zones. An area group could be disabled.

**Anti-passback:** APB shall be settable per reader, with the last area zone entered by each card, via an APB reader – the last APB location being stored. Access shall be denied when a non-pass back card requests access at an APB reader, and the last APB location of the card is the same as the zone the reader grants access to.

**Enforced zone control:** Each reader can be set as a strictly from reader, when access is requested at a strictly from reader and the cards current location is not in the same area the reader gives access from, access shall be denied. Denied accesses as a result of APB and strictly from considerations, are reported as such. A card could be set to have a free APB/strictly from movement. A global free APB/strictly from movement could be set (by editing or via an event) and if a card access is denied with APB or strictly from, access shall be granted if the last APB movement was before the free set time.

**Zone time-out:** It shall be possible to set area zones in access groups with time-out of 1 to 99 minutes, with cards disabled if they stay in the time-out area zone longer than set time-out.

**Card status:** Each cards status shall set as enabled, disabled or as a capture card.

**Start/expiry:** Start time-date and expire time-date could be set per card. When not within the start and end time-dates, a different card status setting shall be used (e.g. the card could be a capture card). Area zones could be added and deleted from the cards access zones when the card is not within the start and end time-dates.

**Inactive:** An inactive time-date period could be set per card. When last movement exceeds the time-date period, a different card status setting shall be used (e.g. the card could be a capture card). Area zones could be added and deleted from the cards access zones when the card is not within the inactive time-dates.

**Zone counters:** Each card could be set with an overall and with a period zone counters, with area zones selected to which access results in decrementing (or incrementing) of the two counters. When either counter does not have a count available, an alternative card status shall be used and area zones could be added or deleted from the cards area groups. A count period could be set per card and the period counter shall automatically re-loaded when the card is used in a new period. The start of count periods shall be synchronized to a certain time of day, to a specific day of the week or day of the month.

**On-line/Off-line:** Each reader shall be set to contain a reader database or not. When set with a database (generally set), the controller shall effectively execute access control functions in an off-line mode, granting access only if the door is not permanently locked, the reader is enabled, card facility codes is correct, the card is found and is enabled for the reader and the time group is active (correct time of day holiday setting pass). On entry, if APB is set, the card shall become disabled for the reader. When reader does not contain database, only the facility code shall be checked by the controller, all other functions done by the PC. APB, enforced zone control, zone counting, cards linked to hosts, random search and expiry functions shall always be controlled by the PC which updates the controllers as required. A reader could be set to allow access to cards with correct facility code when the controller is off-line (card database settings not checked).

**Reader databases** shall be set to use running number databases with up to 65,000 cards in controller memory (facility and card number) or 10 character (HEX) random number cards with up to 15,000 cards in controller memory. Cards not in the controller memory shall reported as out of area and if access is granted, the oldest card to have been granted by either reader shall be replaced in the controller by the new card. It

shall be possible to set controllers to require a PIN code (on time schedule), with or without card (on time schedule). 10,000 cards with PIN shall be stored in the controller.

**Card numbers:** Card holders could be allocated two cards (e.g. a prox and a MAG card), with card set 1 or 2 allocated to readers (only one set per controller). A card holder could be set a virtual card that is not sent to controllers and shall typically be used to identify group cards.

**Card masks** shall be set each card set and for serial or USB readers connected to the PC. A mask could contain fixed characters, ignored digits, certain number of card number and issue number characters (zeros stuffed in front or back).

**Control group (control card):** Cards could be linked to a card control group. Card setting of zero use the corresponding setting of the card control group. For example cards holders belonging to a trade specific trade union are linked to a specific card control group, with the card holders setting for status (en- disable) and area group set to zero, thus using the card control group settings and should the trade union be "locked out", only the area group and status of the card control group is changed. Any card in the database could be used as a card control group.

**Master card link:** Multiple cards could be linked to a card holder by setting a card link to a master card. All zero parameters of a card using the parameters of the linked master card. Typically a card linked to a master card only has the card number set.

**Temporary card link:** It shall be possible to link a card to a temporary card and while the temporary card has a master card link back and the temporary card status is enabled, the master card shall be disabled. The temporary card shall function as a card with a master card link. When the card with a temporary link is used (disabled should be reported) and the temporary card is not linked back (master card link) or not enabled, the temporary link shall automatically be cleared. When a card with master card link and the master card has a temporary link back is disabled, the temporary link of the master card and the master link of the temporary card shall automatically be cleared. Typically the temporary card shall be set as a capture disable card (automatically disabled on capture) or set with an expiry and a disabled status when expired.

**Access events** shall be generated for specific access activities, in the order: Wrong format, wrong facility, not found, disabled, wrong PIN, expired, out-of-count, APB error, strictly from error, out-of-area, out-of-time, no host and enabled, entered, duress, captured, not opened, opened too long. It shall be possible to allocate a trigger group to each card that is included in the cards events – to be used to match count or event triggers (e.g. count cards that belong to a specific trigger group).

A **dual badging** function shall settable per reader – linking a reader to another (or to itself), requiring the badging of two cards that have access within a settable time period to gain access.

The **dual badging** function is settable per reader – linking a reader to another (or to itself), requiring the badging of two cards that have access within a settable time period to gain access.

By selecting a reader to used Vehicle registration as data, **number plate recognition** reader shall find the first card with matching registration for granting access (the access parameter of the card is checked). By using the dual badge option, all the vehicle registrations for the card used will be checked for matching vehicle registration.

The **random search** function shall be triggered automatically when cards enter via readers set for random search. A search % shall be set for each search reader and could be overwritten by a % set for the card, i.e. the cards set % shall be used or if zero, the reader setting used. Events could be generated (e.g. by inputs or via the operator clicking on drawings) to disable or enable random search or to force search (100%). Outputs linked to the search readers shall be controlled closed or open when search is required or not. Random search shall optionally be via PC control or function within the controller.

**Multi-output control** (typically lift control, alarm activation)– shall be possible via relays controlled by outputs of the controller – locally by the controller or by events in the PC. When controlled locally, a card is allocated an output group 1 to 64. Each output group is allocated function(s), with a maximum of 128 functions in a controller. A function is linked to an output group number and is set a reader number of the controller, the output action (activity) and a time group (output is only activated when the time group is active). Activities shall be: nothing, off, pulse, till out group input changes, follow latch, follow door open, toggle or on.

For lift control, the relays are generally connected in series with the floor selection buttons, allowing only the selection of certain floors. Alternatively the lift control reads the access controller relays or receives command via a serial link with the controller. The reader and controller is generally mounted in the lift – the user enters lift, badges card and selects one of the floors available to the card holder.

## 10.12 CARD HOLDERS

The number of cards in the system shall be configurable.

Each card within the system shall be allocated to a unique reference number, which is typically the database record number. This number shall be displayed and logged when card activities take place.

A cardholder's data shall be displayed in lists and property sheets. The data that could be viewed and edited (password dependant) is listed below. Editing aids and batch loading shall be as described in the editing section.

- Location, Time.** The current location of the card (area zone) and when it moved there (YYYY-MM-DD, HH:mm:ss), and the previous location.
- Personal Data.** This general data regarding the cardholder and shall have no effect on the functioning of the system. These editable administrator-defined data fields shall not be checked for format or contents, and shall not change when the card moves. The default data shall be (spare fields available):  
Surname, initials, first and nick names, employee number, company and description.  
Title, gender, department and union affiliation (selected from an editable lists).  
Work, home and cell telephone numbers (can be used in tele-call identification).  
Address, suburb, city, code and email.  
ID number and citizenship.  
Three vehicle registrations and descriptions.  
Comments – free edit of 255 characters.
- Photo.** A photo of any popular type (bmp, jpeg, tiff), with the default directory and field used for file name settings (e.g. use ID or employee number for file name).
- Access Data.** The cards **area groups, zones** added and deleted when card has expired and when either of the cards counts are not available (full or empty), shall set where the card has access to.  
The cards **status** (disabled, enabled or capture) shall be set for normal operation, when expired and when the cards counts are not available.  
Card **start/expire** time-dates sets when the card is active and could be set automatically to either at a fixed time (e.g. at 20:00 on the same day) or after a fixed period (e.g. issued time plus 4 hours). When not within the start/expire, the alternative status shall be used and the add/delete area groups checked.  
**Absent** (on leave) start and end date-time with area zones added / deleted and an absent status when within absent period.  
A **capture group** sets where the card is to be captured.  
A **control group** links the card to a card that serves as group control – card settings of zero use the corresponding settings of the linked group control card.  
A **master card** links the card to a master card (used to give a holder multiple cards) - card settings of zero using the corresponding settings of the linked group control card.
- Time Group.** Defines when a card may be granted access. One of 15 access time groups shall be selectable (with 8 time zones), e.g. "Time group 1 - managers" with 24 hr access. Selection of time group 0 sets that the card uses the time groups set per area zone in the cards area group.
- Trigger Group.** Selects a group that is added to the cards events and is used to trigger events and/or counters.
- Accumulation.** Day, week and month totals since the last day-, week- and month-end, shall automatically update when the card enters via clock in and out readers. These totals shall not be editable. The required total minutes could be set and used in reports that calculate accumulated times exceeded and shortfalls. The period leave time could be entered. Card could be enabled or disabled from clocking.
- Counters.** Two counters are to be available for each card, an overall counter and a period counter (which limits entries within the period set for the card). For example limit to 3 entries per day (period counter limit of 3, period of 0000-00-01) with a total limit of

	25. Both counters increment (and both decrement) whenever there is an entry to the counting area zone. When either counter reaches the cards set limit, area zones (via an area group) could be added and deleted from the cards access zones and an alternative card status shall be used. The cards available period count shall automatically reloaded when the card is used in a new period. Periods shall be synchronized to time of day, day of week or day of month.
<b>Number.</b>	Two card numbers could be set for a card. These numbers are the true number encoded in to, or on to the card or tag. Readers are set to which card number must be used (e.g. a holder could have a PROX and a MAG card).
<b>Previous.</b>	This number shall indicate the previous card number the cardholder used and shall only be used for documentation purposes and shall not affect the functioning of the system.
<b>Linked to.</b>	The card could be linked to a host card; only being allowed access via readers which gives access to the area (or linked area) in which the host is located (follow me). Access control of cards linked to hosts shall be by the PC (data not in controller). If the host card number is a virtual card, it shall be used as a mask to find cards present that match non-zero settings of the host card.
<b>Visitor ref.</b>	If the card is a visitor card, as entered by the visitor system, the last visitor reference (i.e. the visitor that last was allocated to use the card) shall be displayed. If a normal card, the reference is zero.
<b>Pin code.</b>	A 1 to 6-digit pin number could be allocated to cards when Pin Pads are installed. Depending on the set-up of the Pin Pad and reader time groups, access shall be via either card or pin code or both. Cards set with a pin code of zero gain access only by card and no pin shall be required. A duress alarm shall be generated (access is granted if the card normally has access) when the code entered is proceeded with a zero digit.
<b>Pass back.</b>	A card can be set as a pass back card, overriding APB, i.e. the card is be used for multi-access to the same area zone without the requirements to exit the zone (as required for APB).
<b>Random.</b>	A random search % of non-zero overrides the search % set for search readers and shall be used to determine if the cardholder must be searched.
<b>Licence.</b>	Six licence types with expiry shall be selectable and enabled for expiry checking, with the earliest expiry used as the expiry of the card (typically when a medical licence expires, access is denied to certain areas).
<b>Vend data.</b>	Card token, subsidy and values shall be used in POS and vending applications. Amounts available, remaining and periods could be set per card. Cards could belong to a cost group – using the token, value and subsidy of a group. A discount group could be set, with item discounts being allocated to the group.
<b>Park start.</b>	When entering via a reader set as a park entry reader, the time and date shall be set to park start. This data shall be used when the card is presented to park display, park pay and park exit readers.

## 10.13 CARD ACCESS ZONE DISPLAY

A terminal shall be available that cardholders can badge cards and view areas that the card has access to. The general card info - Employee and ID numbers, First and Surname, Cell and Email and Car registration and the access info – Status, Time group, Issue and Expiry dates are displayed and all area zones the card has access to. The display is password controlled, en/disabling the edit of data and zones.

## 10.14 CARD MAKER

A Card maker option shall be integrated in the client system or run as a separate program. Data captured with the card maker shall be the same data used by the access control system. Photos / signatures / documents shall be saved as .bmp, .jpeg or .tiff files, with settings for default directory and field used for file name set (e.g. use ID or employee number as file name). Photos / signatures / documents could be read from files and be resized (zoomed in/out) and could be cropped. Capture sizes (aspect ratio) shall be set as required, per PC. Fingerprints shall be captured for use in access control, with settings of 1 or 2 fingers per person.

Any numbers of card designs shall be made via the integrated WYSIWYG drawing design module described in the graphical display section. A card design shall be selected for each card. Card encoding information could be set on the card design, linked to database data. Issue number could be set to automatically incremented on card encoding. All printing and encoding events, the print reason and material batch shall be logged, and reports shall be available.

Any Windows compatible video capture interface shall be supported, including NTSC, PAL or composite video inputs, USB cameras, etc. Photos could be selected as color or black & white. Pixel resolution shall be as defined by the installed interface.

It shall be possible to use any Windows compatible printer. Print preview shall be available.

## 10.15 VISITOR CONTROL

Controlling of Visitors shall be limited to three aspects, Card access control, Visitor register system and Visitor pre-register system.

### 10.15.1 Card Access Control.

Visitors shall either issued cards simply as staff via normal cardholder by editing of the card database, or by a visitor registering system, which transfers visitor data to the card database. Once in the card database, the card shall functions as a normal access control card, adhering to all normal functions of access control, i.e. card enable, access to selected zones, start and expiry, area zone counting, time groups, Anti-Pass back, Strictly from, etc. Additional specific visitor related options could be set:

**Card Capture.** Cards could be set as capture cards, to be captured at readers that have capture units. Cards could be set to be captured at selected capture units (not captured at not selected bins). Access granted at a capture reader to a card that set to capture at that reader, a control signal shall open the capture bin and once the card is "dropped" in the bin, the door/barrier shall be opened. For cards that are not to be captured, the reader functions as if no capture bin is present. Cards captured shall be logged as being captured and the cards could automatically be disabled (set per reader).

**Link To Hosts.** A visitor card could be linked to hosts (many visitors to a host), and if access is allowed at a reader, access shall only be granted to the visitor card if the host is present in the area to which access is requested. Should the host card be a virtual card, the host card shall be used as a mask to find present cards that match non zero settings (e.g. setting a dummy host card with department x and all other parameters to zero, access shall be granted to the visitor the card if any card with department x is present). The PC shall grants access to cards that are linked to hosts, i.e. visitor card data will not reside in the controller and the PC must be running the access program for access to be granted.

**Fingerpirnt.** Options for using only fingerprint for access control (card not required) shall capture fingerprint on entry and grant exit only if matching fingerprint currently entered. Taking of video snapshots on entry and exit shall be possible.

### 10.15.2 Visitor registering system.

This shall be an optional system used to register visitors and shall be a client program running on one or more PCs that access and edits a visitor database on a server PC (could be the same PC). The visitor database is to hold data on visitors that have been registered. Functionality of the system shall be as follows:

Visitors that have been registered previously are search for by an appropriate data field (e.g. by name, ID number, etc.) or by fingerprint. Visitors not in the database are added. All relevant data is entered or edited as required, including where the card has access to. Any of the fields could be password protected, allowing only certain operators to change data (e.g. where the card has access to). Editing aids described in the data display and editing section shall be available.

Data in the pre-registered data base (see below) could be accessed and copied to the visitor on display, by presenting the card issued by the pre-registering system, at a reader connected to the PC or by selection via appropriate lists.

Optionally, photos, signature and a document (e.g. ID book) could be taken / scanned by the system and be displayed and stored on the PC disk and automatically allocated file names linked to a set data field (e.g. ID number, database reference). Photo / signature / document capture specifications and options shall be the same as the card maker.

Voice samples could be captured in .wav files that are linked to the visitors and fingerprint could be recoded to be used for search when the visitor revisits.

The field used as default to name the photo / audio files and the folders shall be selectable.

The visitor data shall be copied to the active access card database by allocating an access card to the visitor. Data that was not editable shall not transferred, facilitating the pre-setting of visitor cards with certain parameters (e.g. to where that card has access). Card start and expiry could be set automatically to either at a fixed time (e.g. at 20:00 on the same day) or after a fixed period (e.g. issued time plus 4 hours). The data shall be transferred by entering the card number (if the function is enabled) or by presenting the card to a reader attached to the PC. Data field(s) could be set to be copied back to the visitor database for further editing (e.g. copy back the allocated cards area group, enabling the editing of the groups area zones).

An ID card or label could be printed on any Windows printer installed. Multiple print formats could be designed by the system as described for the card maker. A card design shall be allocated to the card.

Card activity shall be logged with the visitor database reference, enabling reports to use data from the visitor database (and not from the card database). The last location, date-time and status of the visitor card shall be recorded in the visitor database. Manual and automatic facilities shall be available to delete cards from the visitor database that have not been active for a set period of time.

Operators can click on icons that generate event to open doors, barriers, etc.

All menus and functions within menus shall be password protected. Operators shall log on/off.

### **10.15.3 Visitor pre-registering system**

This shall be an optional client program used to pre-register visitors, running on one or more PCs. A visitor shall be pre-registered by entering data such as visitor and host names, expected arrival and departure, parking required with vehicle registration, colour and make. The data could be set via a web page and emailed to the system that automatically adds the data in the database. Email shall require a specified format and password – email users must be registered with a password.

The visitors pre-registered for the day shall be displayed in a list. Visitors that have arrived and not left could be displayed in a selected colour. Visitors that have already left shall be deleted automatically. Selected data could be edited, password permitting. Data could be sorted by clicking on any column.

The visitor shall be given a card that is linked to the visitor via a reader connected to the PC or via a reader in the system, e.g. a barrier reader. The card shall be issued by clicking on the visitor data and presenting the card to the reader or if a card “spitter” is installed, the card shall be issued automatically and read. The barrier shall automatically be opened. The cards shall be enabled for selected readers and adhere to all access control selections. Cards start and expiry could be set automatically.

The visitor could be allocated an available parking bay from a list, reserving the bay to the visitor (providing a link from vehicle to visitor). This is to be done by clicking on the required parking bay.

On exit at a reader connected to the PC or via a reader in the system (e.g. a barrier reader with a card capture bin), the card visitor shall be removed from the pre-register database. The parking bay shall be set as available and the barrier automatically opened. Data in the pre-registered database of visitors not currently on site shall automatically be deleted if the expected departure date exceeds the current date.

The visitor registering system could access the data in the pre-register database, copying data to the visitor database.

All menus and functions within menus shall be password protected. Operators shall log on/off.

## **10.16 INPUT/OUTPUT**

Inputs shall be set as special function inputs (Action complete, APB enable, APB reset, Booth occupied, Card capture detect, Egress, Reader enable, Reader tamper or Latch monitor) or as auxiliary inputs. Auxiliary inputs could be set as counting inputs, with count changes reported to the PC after set time-out after count incremented. Each input shall be set for number of levels:

- 2 closed/open.
- 4 short circuit/closed/open/open circuit.
- 5 closed/open/illegally opened/open too long/not opened.
- 7 short circuit/closed/open/illegally opened/open too long/not opened/open circuit.

Each level shall be set with a description, active time group for the controller (controller does not report change when time group is not active), alarm time group (when the level change is an alarm) and activity on level change (log, display, trigger other events, print).

Outputs shall be set as Auxiliary output, Booth busy, Buzzer, Capture, Latch or Reader Isolate. Multiple output control on card read shall be as listed in **Multi-output control** above.

I/Os shall be set for active time group for each detection level.

## **10.17 VENDING, FUEL MANAGEMENT, POS**

The vending option controls vending machines, Photostat machines and fuel pumps via controller and Point Of Sale (POS) PCs. All functions shall be controlled via access cards that request dispensing/purchases. The system shall function on-line, with the PC client program granting or denying the requests.

Every item dispensed shall be set with a price and optionally with a token, discount and a subsidy value. Cardholders have token, value and subsidy amounts that shall be used for dispensing/purchases. Value amounts could be added to via cash add PC menus or via note acceptor controllers (cash loaders). Token, subsidies and value shall be set to automatically reload by amounts set per card, on periods set per card. Reload time could be synchronized to time, date, day of week or month. Cardholders could optionally be allocated to cost groups that share token, value and subsidy.

Machines shall be interfaced to via controllers with electro-mechanical interfaces or with serial interfaces (BDV, Executive, MDB and Tockheim pump protocols accommodated as standard).

Product stock management could be enabled by setting the recipe for each item and setting of the full quantities of each base product in each machine. Low-level alarms of base products shall be generated.

Maintenance, filling and cleaning service alarms shall be generated if these activities are not performed within set periods.

POS shall run on a PC and be cashless or optionally have a cash draw – purchases by using the values and subsidies available on a card and/or use and manage cash via a cash draw. A POS shall function as a vending machine (all vending functions apply). A card shall be read via a reader connected to the PC (or the card or employee number is entered – if configured), and the holder's photo, name, employee number and available subsidy and values are displayed. Items shall be purchased via keyboard, barcode scanner or mouse selections (quantities could be entered and items could be returned or altered). Receipts (configurable) could be printed automatically (the number of prints and slip printer(s) shall be set – e.g. two at the POS and one in the kitchen). Available amounts shall automatically be updated and included on the print. Items could be identified with a barcode scanner connected to the POS.

When dispensing fuel, the vehicles kilometer reading shall optionally be entered via a keypad, being logged and available for reports. Kilometer entering can be enforced per card holder and values entered shall be checked for validity (more than last and less than last + maximum for a full tank). A "virtual pump" program shall be available to enter fuel added to vehicles.

All cash loaders, vending units, POS terminals and slip printers shall display/print card holders name and remaining tokens/subsidy/value.

When using cash tills, operator functions of take-on and cash-up shall be logged and can only be performed when the keyboard is enabled by a supervisor.

## **10.18 PARKING**

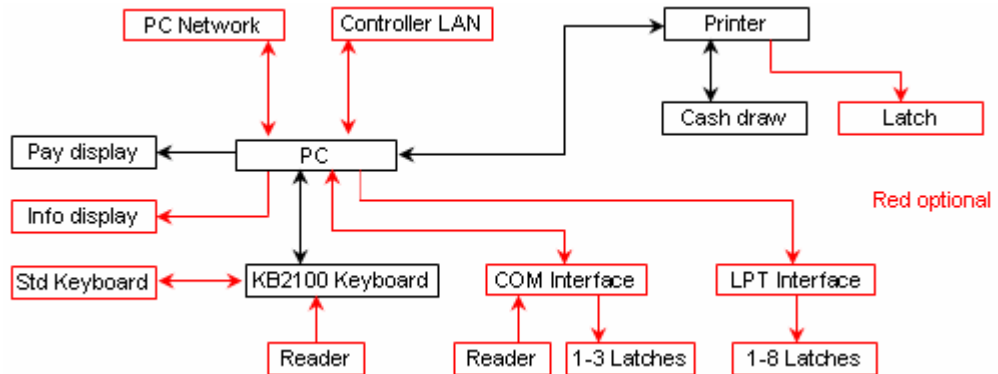
### **10.18.1 Pay on exit – Access system**

A pay on exit option to access control shall allow the setting of readers tied to LAN access controllers as Park Entry, Park Display, Park Pay or Park Exit readers. On entry, the date and time shall be logged to the card database. The exit reader shall only grant exit when the time present (after entry or after pay) is free. A parking fare data table shall set the amounts payable for the present intervals. Park display readers shall indicate the present time and the amount payable and pay readers displays the time present, the amounts due and reset the entry time to the current time (the amount due shall be logged).

### 10.18.2 Counting system

It shall be possible to set the access control system to control parking area(s) for multiple tenants (companies), limiting access based on a maximum count per tenant. Available parking for the appropriate tenant shall automatically decrement when cards enter and increment on exit. Visitors shall be granted access when count is available to the tenant visited – via tenant entry and exit push buttons or by clicking on appropriate graphical displays (these shall not be functional when no count is available to the tenant), decrementing / incrementing the tenant count. It shall be possible to set overall counters per area, denying access to selected tenants (even if tenant count is available).

### 10.18.3 Pay on entry/exit – POS system



Referred to as parking POS (PPOS), pay on entry and a pay on exit management options shall allow for the entering of vehicle details via a POS terminal with programmed keys (dedicated keyboard or touch screen) and a cash draw. Data entered shall be vehicle color, registration and number of occupants and shall be set as required, optional or not required per vehicle type. Overriding of this setting shall be via administrators.

Parking tariffs shall be selected from preset values (e.g. car, taxi, bus, lost card, pedestrian) per entry lane and can vary on time of day/week. A configurable slip containing the selected data shall be printed.

Guest cards could be presented to a reader connected to the PC, with the holder's name being obtained from an external system and displayed and printed on the slip. Guest cards could be granted free access in accordance to data received from the external system.

Operators shall log on with a "take-on" amount and a cash-up prints and logs the number of vehicles entered free, paid and amount taken. Take-on and cash-up options shall only be available when the keyboard is in supervisor mode via a key setting or set via a management PC.

The amount payable shall be displayed on a pole display. A multi-line message display could be connected to a PPOS terminal, displaying data as set via a management PC.

Pay on exit PPOS will use access cards that are issued on entry and retrieved on exit. These cards shall be tagged at readers in the access control system or at readers connected directly to the PC (serially or integrated with the keyboard). Readers shall be set as entry, exit or both (toggled as entry or exit reader by the operator).

Barriers / gates / turnstiles (linked to vehicle type) and the cash draw shall be controlled via relays connected to serial or parallel controllers (COM or LPT ports) or via the slip printer.

## 10.19 TIME ACCUMULATION, T&A

Time accumulation and time and attendance (T&A) shall be optional functions that require readers to be set as clock in, clock out or clock in/out readers. The area zone entered shall be set for clocking (facilitating different clock readers per card). Cards could be individually be enabled or disabled from clocking. By setting zone enforcing, clocking or movement to a specific area after clocking could be enforced. LCDs could be set to display card holders name and accumulated time.

### 10.19.1 Accumulation

The system could be set to perform an overall time accumulation of how long each cardholder was "on site". Full time and attendance options shall available by linking to T&A systems.

The provided accumulation functions shall be as follows:

When a card enters via any reader in the system that is set as a clock-in reader, accumulation for that card starts and ends when the card enters (exits) via any reader set as a clock-out reader.

Three totals shall be kept: a daily, weekly and a monthly total. The daily total shall be cleared at the end of the day, the weekly at the end of day at the end of the week, and the monthly total on the day end, at the end of the month. On week or month end, all cards with totals for the week or month respectively, shall be logged and cleared of daily and weekly or monthly totals. On other day ends, only cards with daily totals shall be logged and cleared of daily totals.

Before any total is cleared (at day end), a daily accumulation log file shall be created, and loaded with all cards that have accumulation totals. These accumulation files shall contain the card number, and the current day, week and month totals and shall be used in generating accumulation reports.

Cards that equal 24 hr accumulation for the day (which indicates that the card did not clock out), shall be given a total of 0.

### 10.19.2 T&A Systems

It shall be possible to interface numerous Time and Attendance and payroll systems to the Access system. The Access system shall provide the clock in and out times to such systems which then calculate the effective hours worked and what salaries and wages are to be paid out.

The clock times could read from the events stored in the daily log files, with additional data available in card databases. As an alternative, a special SW driver shall be available which logs the clock in/out events in dedicated file(s) and can specifically be tailored to the T&A system requirements. These log files shall typically be "flat ASCII" files, with a line per clock in/out. A typical format of the line shall be:

```
010 employ_ment_nr 0 yyyy-mm-dd hh:mm x 00 crlf
```

where the employment number is 13 characters and x=I for clock in and x=O for clock out. The characters 010, 0 and 00 are used as check/synchronisation characters. The card number could replace the employment number. Separating character could also be changed. Typically:

```
010 0000000102000:06:13 15h37 I 00
010 0000000202000:06:13 15h37 I 00
010 0000000202000:06:13 17h37 O 00
```

The file name and path into which the clock data is written shall be set-up as required. If the file does not exist, a new file shall be created when a card clocks in/out. The T&A system shall rename the file before reading the data.

## 10.20 ASSET MANAGEMENT

Asset management options shall be integrated in the client system or run as a separate program.

An asset database shall contains the following data (\* data is used for asset tracking tags):

Reference:	Running index number.
Name:	Descriptive name.
Code:	Barcode or Asset tag number (mounted on to asset).
Issue To:	Reference to current user to who the item is issued/taken (zero when not issued).
Start:	Date/time asset was issued to last user.
Returned date:	Date/time by when the asset is to be returned.
Period, cost:	Cost groups set hour period and cost of the periods (e.g. above 2 hours R40/h, above 4 hours=R20/h, above 8 hours=R40/h).
Returned by:	Previous user who returned the item.
End:	Date/time the item was previously returned.
*Location:	Last detected tag location (reader area zone to).
*Detected:	Date/time tag last detected.
*Battery:	Last reported tag battery measurement.
*Alarm status:	Last reported tag alarm status.
*Alarm date:	Date/time last tag alarm reported.

\*Detection period: Date/time period of no detection after which alarm is generated.

Additional information fields shall be available that could be displayed and edited: Purchase price and date, supplier, maintenance period, next maintenance date and responsible person.

Asset management options shall be:

#### **10.20.1 Asset issue/return**

An asset issue/return menu shall be integrated in the client system or run as a separate program, with all functions password protected and generally users shall only have access to the system via asset and card readers.

Assets shall be issued by selecting or reading the item code (barcode reader or asset tag reader tied to the PC) and selecting the user issued to (card reader tied to the PC can be used). Assets not previously returned shall not be issued. Start date/time shall automatically be entered when issued.

Assets shall be returned by selecting or reading the item and the user returning the item (could differ from the user issued to). Alarm events shall be generated when assets are not returned before the set return by date.

On issue and return, slips containing all relevant information (configurable) could be printed automatically, or on request. All events shall be logged with date/time, logged on-operator, user issued to, user returned and charged data. Reports shall be available on current asset status and on the logged events (selections for date/time period, user, department and item).

#### **10.20.2 Asset pre-book**

Asset can be pre-booked, with start and end dates.

#### **10.20.3 Asset tracking**

Automatic tracking of fixed asset and assets linked to user(s) shall be via external systems or via asset tag readers connected directly to the controllers. The last reported tag location, date/time, battery measurement, alarm status and alarm date/time shall be recoded automatically.

These options are being integrated.

### **10.21 MESSAGE DISPLAYS**

Events could be set to open a message window, displaying a set default file for the specific event (not editable by the operator) – typically giving more information about an alarm and giving instructions on what is to be done. The file shall be in .RTF format and could be created with editors such as Microsoft Word or Write (included with Windows) and allows font and color selection, pictures, etc. The time of the event, the item name and level (e.g. front door, open) could automatically be inserted in the display.

### **10.22 OPERATOR OCCURRENCE LOG**

Events could be set to open an occurrence window similar to the message display. Editing shall be allowed and operators enter data in to the log book and the data shall be stored to a daily .RTF log file.

### **10.23 AUDIO WAVE FILES**

Specific events could be set to play pre-recorded wave files, containing specific sounds or audio messages, e.g. sound "Door open too long". The wave files shall be generated on PCs that have audio multi-media installed.

### **10.24 SMS**

It shall be possible to set message that are sent as SMS messages to cell number(s) via GSM modems connected to serial ports tied to a PC in the system. The messages shall be sent on algorithm of event triggers (time groups could be used in an algorithm, with messages only being sent when the time group is active). A message could automatically include event and event-referenced data (e.g. controller number and controller name). SMS activities shall be logged as events.

### **10.25 EMAIL**

Similar to SMS, messages could be set that are sent as Email on algorithm of event triggers.

Email sent from Web pages to change, set or request data, should be available in future updates.

## 10.26 TELE-CALL CONTROL

By linking a cell-modem, it shall be possible to generate events on identifying the caller ID (referencing to the card database) without answering the call – typically to open a gate if the callers access parameters have access to the area zone.

## 10.27 LOGGING

Events shall be set to be logged per input level, output level and per reader and could be set only to be logged on defined time groups (e.g. only after hours). All system events such as power-up, on- and off-line, log on and off shall be logged and logging shall be done in database files, with a new file being created per day. Optional log fields and the length of such fields could be set (e.g. card holder's name and employee number). The oldest day files shall automatically be deleted when the server's disk becomes 80% full.

Editing of data, including the adding and deleting of records shall be logged in database audit files, recording the operator, the old and the new data. A new file shall be created per day.

## 10.28 REPORTS

A comprehensive separate reporting system shall generate reports from data files. A report can be generated to the display, a printer or to a file or can be emailed automatically. A report could be a simple extraction of data from a single database (e.g. list all cards that belong to a specific department), or a complex report extracting data from event files, referenced to numerous other data files (e.g. who of a specific department was in a defined area, for longer than a certain time, during a defined period of a day).

Reports available shall include all set-up, audit, accumulation and events. Parameter requested of the operator could be configured.

The report forms shall be generated utilizing Seagate Crystal Report (Crystal Reports shall not provided, the forms shall be). Report forms shall contain the site name and totals of the number of records found. Reports supplied shall be ordered to certain fields (e.g. by department), with details, summaries, totals of groups, daily and report totals, etc.

Password permitting, reports (password per report) could be generated via any PC linked to the system. Reports could be automatically generated on certain times of the day, on certain dates, when specified events/alarms occur or on operator request. Who generated what report shall be logged.

## 10.29 INTERFACING TO HOST PROGRAMS

### 10.29.1 Event linking.

Optional on-line interfacing to other programs shall be via a TCP or serial link. The IP address of the PC running the host program and port number used by the program shall be settable. Commands shall be available to transfer events to the host system and to receive events from the host system. Clock in and out event could be set to add lines to a flat ASCII file containing date-time, in/out and employee number. File names shall be configured and could contain date characters. Directory sharing will not be required.

### 10.29.2 Data sharing.

In order to eliminate the duplicate entry of data in the BMS system and host systems, the data must be shared in one of two methods:

**Shared database.** The common fields of data shall be located in a central database, accessed by both systems. The BMS system shall be able to access this data in real time, i.e. the database must always be available when transactions take place. The database type could be of any type for which an ODBC driver exists. Where networks and servers are not always available, the database should be located where the server program is run.

**Updated database.** Host systems could update the card database directly and mark the record as changed, resulting in the update of remote PC databases and controllers. The period of checking for changed record shall be settable or could be done on event.

**Converters.** A variety or convert programs shall be available that load data from flat ASCII files to the card database and to the area zone-group database (setting where cards have access

to). When run, all databases shall be updated accordingly. An configurable LDAP converter shall available that imports data to the card database.

### **10.30 BACK-UP STORAGE DATA**

Back-up shall be performed by running a batch file and triggered on events (manually by the operator or shall be done automatically on a scheduled time or external events).

### **10.31 ON-LINE HELP WINDOWS**

The system shall have built in comprehensive help and contain all Software and Hardware set-up and installation related issues. Pop-up help (in the selected language) shall be displayed when the cursor is held on column names, list column properties and on property sheet data descriptions.

### **10.32 SOFTWARE VERSION AND UPGRADES**

Different versions shall be available that limit certain functions and quantities and be protected via encrypted installation files and by HW keys that could be protected by expiry keys. Access to more options shall be via appropriate keys.

Updates shall be available from the manufacturer or on the Internet. Most updates shall be free, additional functions could be charged for. When updating a system, the installation set-up shall not be lost, the new functions simply added. Changes to field types shall be reported and could be updated or accepted.

### **10.33 VIDEO LINKING, \*VIDEO /CAMERA CONTROL**

It shall be possible to link to external video systems via TCP or serial links. Video snap-shots shall be taken on events, saving to files with names referencing the date-time, camera reference and the event.

A configurable snap-shot viewer shall be available, with settable window sized, display filters selecting start/end date-times and event parameters (e.g. out-of-area Readers A and C). When scrolling through snap-shots, it shall be possible to freeze Windows, save-as and delete.

I/O events can be exchanged with the external video systems. Database information (typically cardholders name, reader name) can be sent to the external systems on events.

The control of cameras (pan, tilt, zoom) shall be available in future versions.

### **10.34 \*CONTROL VIA WWW**

Options shall be available in future versions.

### **10.35 \*GUARD TOUR**

Options shall be available in future versions.

## **11 TESTING – SIMULATION AND MONITORING**

### **11.1 HW OFF-LINE**

All controllers and modules shall have SW versions for testing and be used to test all functions of the controller or module. Test jigs interlinking inputs and outputs and linking to a PC running a test program shall be available. Test results shall indicate passed or where errors are encountered.

### **11.2 SW ON-LINE, OFF-LINE**

The following monitors and simulators shall be provided with the system:

- Event monitor – shows events within the system.

- Event simulator – generates event within the system.

- MUX messages monitor – shows data to and from the MUX interfaces, i.e. data sent and received from the LAN.

- MUX out simulator – sends data to the MUX interfaces (no events are generated).

- MUX in simulator – send data to the system as if it was received from the MUX interfaces.

Editable simulation text files shall be provided for all controller types. Simulation commands for simulation speed and to create execution loops could be set. Parameters such as PC time and literals such as interface

and node numbers could be set in commands, simplifying the use of stored simulation files. Single line could be executed or files could be run continuously.

Monitors could contain filters, showing selected data. Data could be paused, saved or cleared.

## 12 FUNCTIONS / OPTIONS SUMMARY

The following tables are summary lists of the possible requirements detailed above. The minimum requirements are indicated as 'yes' in the requirements column. For each possible requirement, a 'yes' must be set for either the included or additional column, indicating whether the function is included as standard or an available as an added option. No in both these columns indicates that system cannot comply with the requirement (Softcon systems comply with all the requirements).

### 12.1 SYSTEM

Para	Description	Require	Included	Additional
5,8.2	Controllers function in stand-alone mode	Yes		
5, 8.1	Battery backup memory (set-up and card database), real time clock	Yes		
5	Directly to 2 readers	Yes		
5	Door modules	No		
5	Fiber controller LAN	No		
5	PC network – TCP via UTP or fiber, linked via hubs	No		
5	LAN comms via intelligent interfaces with error detection and repeats	Yes		
5	Comms to controllers TCP and USB	No		
5	Sub-LAN between controllers and LAN controller	Yes		
5	1,000 transaction buffer in backup memory, time and day of month stamped by controller	Yes		
5	Dial-up between PC and controllers on schedules or alarm	No		
5	PC SW in server/ client architecture	Yes		
5	Server/ clients on multiple PCs	No		
5	Clients continue functioning off-line if server not available	Yes		
5	Database synchronization between PC systems on set schedules, on alarm	No		
5	Dial-up between PCs	No		

### 12.2 HW

Para	Description	Require	Included	Additional
6	Cards directly printable	No		
7,8.2	Opto-isolated Wiegand reader interface	Yes		
7	Serial, data/clock, touch reader interface	No		
7	Wiegand 30 bit cards with facility code and checksum verification	Yes		
7	Wiegand 26, 32, 34, corporate 1000	No		
7	Smartprox (read and write)	No		
7	ISO MAG cards with settable data location and checksum verification	No		
7	Asset tag receivers directly to controller	No		
7,8.2,10.12	Latest 15,000 10 digit random or 65,000 facility running numbered cards in controller	Yes		
7	Fingerprint or palm readers integrated with system	No		
7	Pin pads with/without card readers on time group, duress alarm	No		
7	3-LED readers (Flash amber=ready, Red=reader disabled/denied, Green=access)	Yes		
8.1	Monitored 6AH UPS integrated in controller	Yes		
8.1	Controller RTC synchronized with PC on on-line and every hour thereafter	Yes		
8.1	Earthed steel enclosures with lockable, hinged, monitored lids with covered high voltage	Yes		
8.1	Filtered, tranzorbed mains supplies	Yes		
8.1	LAN protected via tranzorbs and resistors, screens earthed per segment	Yes		
8.1	Terminal, link, switch diagrams and installation booklet per controller. Unpluggable connectors	Yes		
8.1	Controller diagnostic LEDs	Yes		
8.1	HW version and electronic ID available at PC	Yes		
8.1	Time groups (schedules) for I/O, access, reader/PIN enable in controllers, with 30 holidays	Yes		
8.1	I/O expansion via modules	No		
8.1	Controller SW and HW (power monitored) watchdog reset circuits	Yes		
8.1	On-line, off-line, power-up reported to PC	Yes		
8.2	Supervised inputs with short and open circuit alarms	Yes		
8.2	Relay outputs, or capable to drive relays	Yes		
8.2	Configurable inputs (action complete, egress, capture, presence, reader enable, latch, auxiliary)	Yes		
8.2	Configurable output (capture, latch, auxiliary, booth busy, buzzer)	Yes		
8.2	Counting inputs in controller	No		
8.2	Local control of APB, ATB, illegal attempts (reader disabled)	Yes		
8.2	Mantrap controlled directly by controller with presence, door, latch monitors and busy output	Yes		
8.2	Readers and egress enabled via local inputs, time groups and from PC	Yes		
8.2	Local alarms to buzzer	No		
8.2	Controller hand programmer	Yes		
8.2	Reader/door modules with PIN pad and LCD (displaying date-time, accumulation, messages)	No		
8.3	Mimic drivers with accept alarm and lamp test	No		

## 12.3 SW

Para	Description	Require	Included	Additional
10.1	Windows 2000, XP	Yes		
10.1	Modular SW with server/client architecture	Yes		
10.1	MS Access databases accessed via SQL	Yes		
10.1	Automatic database compression and correction on start-up	Yes		
10.1	Setting of table names and locations, field names, type, size, indexed, unique	Yes		
10.1	Database encryption	No		
10.1	Event driven PC SW	Yes		
10.1	Virtual objects	Yes		
10.1	Windows date/time format	Yes		
10.2	Multiple users in multiple user groups. Passwords and users expire. Auto log-off	Yes		
10.2	User groups set to view, select, edit data and select items / do control	Yes		
10.2	Log on via card reader	No		
10.2	Log on via finger print reader	No		
10.2	Application settings per user	No		
10.3	Language settings per user	No		
10.4	15 time groups, 8 time zones per function type (access, reader- PIN used, input, output, buzzer)	Yes		
10.4	Week day, 30 holiday selection per time group for each time zone	Yes		
10.5	Audit operator changes	Yes		
10.5	Changes sent automatically appropriate controllers	Yes		
10.5	List displays configurable to be updated in real time	Yes		
10.5	Lists referenced to databases	Yes		
10.5	List columns set to change color according to status, sizable, ordered, column names editable	Yes		
10.5	List records filtered, sorted by selected column(s)	Yes		
10.5	Print selected rows in displayed list	Yes		
10.5	Generation of new lists, grouped in status, card, set-up, vending menus	Yes		
10.5	Property sheets with data ordered in tabs	Yes		
10.5	Editing aids – batch load/search, find, copy/paste, delete, add, default	No		
10.5	Setup wizards	No		
10.6	Scrolling activity lists with filters. Columns selectable, sizable. Pause, copy, print, restart selections	Yes		
10.6	Input, output, counter, reader events set for display on time group	No		
10.7	Events display graphical symbols (bmp/tiff/jpg) flashing when in alarm on drawings	Yes		
10.7	Drawings with alarms displayed on top of the desktop	Yes		
10.7	Drawings contain editable database items linked to objects	No		
10.7	Drawing display photos (bmp/tiff/jpg) linked to readers	No		
10.7	Drawings contain selectable objects that generate events, execute programs (exe, batch, scripts), select other drawings	Yes		
10.7	Editable symbol library	Yes		
10.7	Integrated drawing WYSIWYG editor, with font, align, space, copy, rotate, order and undo functions	Yes		
10.8	Events set to be alarms on active time groups	No		
10.8	Events set to be logged, displayed, printed, used as triggers. Optionally only on active time groups	Yes		
10.8	Event generated on time schedules	Yes		
10.8	Event start applications, generate new events (real or virtual) on algorithm of triggers	No		
10.8	Algorithms are settings of logical (and, or) events, statuses, time groups and sequenced events	No		
10.8	Algorithms can use virtual objects, virtual cards used as a card mask (filter)	No		
10.9	Input, output, reader events running total counts are kept. Reset on events	No		
10.9	Events increment/decrement / sum / set virtual counters, generating max, min, available count events	No		
10.10	Timers generate events on time-out. Algorithm of triggers start, stop, reset, load and cycle timers	No		
10.11	Readers set with in and to area zones, with zone linking for APB	Yes		
10.11	Card allocated shared, own or multiple area groups. Groups could be disabled, batch loaded	Yes		
10.11	APB and enforced zone control set per reader, overwritten per card	No		
10.11	Area groups set to time-out cards in area zones	No		
10.11	Card statuses settable as disabled, enabled, capture for normal, expired, zone count full, inactive	Yes		
10.11	Zones added and deleted for expired, zone count full, inactive	No		
10.11	Overall and period zone counter set per card, with reload and period settings	No		
10.11	Databases optionally set in reader or only in PC	No		
10.11	2 card numbers set per holder. Cards linked to master cards, to temporary cards (master disables)	No		
10.11	Cards linked to control cards (virtual cards)	No		
10.11	Card masks set for access and serial readers	No		
10.11	Access events (in order): Wrong format, wrong facility, not found, disabled, wrong PIN, expired, out-of-count, APB error, from error, out-of-area, out-of-time, no host, enabled, entered, duress, captured, not opened, open too long	Yes		
10.11	Cards allocated a trigger group for event/counter trigger filtering	No		
10.11	Random search set per reader, superseded by card setting. Search disabled, enabled or forced with events	No		
10.12	Cards personal data includes surname, first name, title, gender, employee, department, company, description, union, telephone numbers, vehicle registrations and descriptions, address, email, ID,	Yes		

10.12	citizenship Card access data included location and time, card and issue numbers, PIN, random %, pass back, counters and linked to master-, temporary-, visitor- cards	Yes		
10.12	Card are linked to the groups: time-, area-, capture-, control-, trigger-, host-, group	Yes		
10.12	Capture groups set where cards set with the group are captured	Yes		
10.13	Card maker with photo (bmp,tiff,jpg) capture, integrated WYSIWYG designer	No		
10.13	Card photos cropped and resized	No		
10.13	Card printing and programming (auto issue increment) logged.	No		
10.14.1	Visitor(s) linked to host(s)	No		
10.14.1	Visitor registering system	No		
10.14.1	Identifying visitor using finger print reader	No		
10.14.1	Linking visitor card to card database via card reader	No		
10.14.1	Cards allocated to visitor logged with visitor reference	No		
10.14.1	Visitor photo capture, integrated WYSIWYG label designer, print	No		
10.14.2	Visitor pre-register system via www, with parking bay allocation			
10.15	Inputs set with function type and number of levels (for supervised and door monitoring), with levels set with monitor and alarm time groups and event activity	Yes		
10.15	Outputs set with function type and activation time group	Yes		
10.16	Vending, POS, cash-loaders, add cash applications, with token, subsidy, value, discount set per item	No		
10.16	Vending product and service management with low level and time to service alarms	No		
10.16	Fuel management	No		
10.17	PPOS, pay on exit	No		
10.18.1	Time accumulation	No		
10.18.2	Link to T&A systems	No		
10.19.1	Asset management – issue, return	No		
10.19.2	Asset tracking	No		
10.20	Events display messages	No		
10.21	Events open an occurrence log-book	No		
10.22	Events sound audio wave files	No		
10.23	Events generate SMS messages	No		
10.24	Events generate Email	No		
10.25	Events on tele-call	No		
10.26	Daily log files for events and audit	Yes		
10.27	Crystal reports generated to display, printer, file. Operator selections or fixed	Yes		
10.27	Status, events, set-up reports with site name, number of records, sorting sums and totals	Yes		
10.27	Creation / design of new reports	No		
10.27	Reports generated automatically	No		
10.28.1	Interfacing with host programs via files and TCP, serial links	No		
10.28.2	Data changes by external systems	No		
10.28.2	Data converters	No		
10.29	Backup via batch files, triggered on events (operator, timed, external)	Yes		
10.30	Integrated help files and pop-up help	Yes		
10.31	Access to additional SW functions via encrypted keys	No		
10.32	Control via www options available in future versions	No		
10.33	Guard tour options available in future versions	No		
10.34	Video / camera control options available in future versions	No		
11.1	Off-line testing of HW	Yes		
11.2	On-/Off-line SW monitors with filters and simulators with pause, save, clear, go to, speed, literals, parameter settings	Yes		