

Softcon BMS Specification

Version 01.17

CONTENTS

1	OVERVIEW	3
2	REFERENCES	3
3	OWNERSHIP / GUARANTEES	3
4	STANDARD SPECIFICATIONS	3
5	SYSTEM ARCHITECTURE	3
6	ACCESS CONTROL CARDS	5
7	READERS	5
8	CONTROLLERS	5
8.1	General.....	5
8.2	CR355 (Reader and I/O controller)	6
8.3	CR390 Reader, I/O and lan controller	7
8.4	CR372 (Door module)	8
8.5	CR374 (Door module with Pin Pad and LCD)	8
8.6	DF355/6 (I/O controller).....	9
8.7	MD350 (Mimic driver)	9
8.8	MD351 (I/O controller)	9
9	COMPUTER SPECIFICATIONS.....	10
10	SOFTWARE	10
10.1	General.....	10
10.2	Security levels	11
10.3	Language support.....	11
10.4	Schedules (Time zones and groups).....	11
10.5	Data display and editing	11
10.6	Activity displays	12
10.7	Graphical displays	12
10.8	Events.....	13
10.9	Counters	13
10.10	Timers.....	14
10.11	Access control	14
10.12	Card holders	16
10.13	Card ACCESS ZONE DISPLAY.....	18
10.14	Card maker	18
10.15	Visitor control.....	18
10.16	Input/Output.....	20
10.17	Vending, Fuel management, POS.....	20
10.18	Parking.....	21
10.19	Time accumulation, T&A	22
10.20	Asset management.....	23
10.21	Message displays	24
10.22	Operator occurrence log.....	24
10.23	Audio wave files.....	24
10.24	SMS	24
10.25	Email.....	24
10.26	Tele-Call Control.....	24
10.27	Logging.....	24
10.28	Reports	25
10.29	Interfacing to host programs.....	25
10.30	Back-up storage data	25
10.31	On-line help Windows.....	25
10.32	Software version and upgrades.....	25
10.33	Video Linking, *Video /camera control	27
10.34	*Control via WWW.....	27
10.35	*Guard tour	27
11	TESTING – SIMULATION AND MONITORING	27
11.1	HW Off-line	27
11.2	SW On/off-line	27
12	FUNCTIONS / OPTIONS SUMMARY	28
12.1	System.....	28
12.2	HW.....	28
12.3	SW.....	29

1 OVERVIEW

The system provides 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 – snap shots on events, I/O control with external video system.
- Random search.
- Integrated video (camera selection and control, live display).
- Guard Tour.
- Available in future versions

2 REFERENCES

Since 1989, Softcon systems have been installed at more than 2,000 sites in 29 countries, using more than 20,000 control panels and have been proven to be stable and reliable. Contactable references are available.

3 OWNERSHIP / GUARANTEES

All Hardware (HW) designs and circuit diagrams, Firmware (FW) and Software (SW) code is the property of Softcon and is not provided and can only be altered by Softcon. HW maintenance procedures and partial diagrams are available to aid in the repair of HW. Upon special agreements, the circuit diagrams and source code could be lodged in trust to be made available to nominated parties on defined circumstances.

All products remain the property of Softcon until Softcon has been fully paid.

All Softcon products carry an ex-factory year guarantee against fault components and bad workmanship. Softcon cannot be held responsible for any loss as a result of product errors or failures. Softcon does endeavour to correct errors as soon as possible. Non Softcon products guarantees are as provided by the manufactures. No guarantees or support is given to products not installed to Softcon specifications/instructions or by non approved, certified installers.

4 STANDARD SPECIFICATIONS

The card reader controller is UL listed, UL Classified and UL Recognized. All HW is 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 are adhered to.

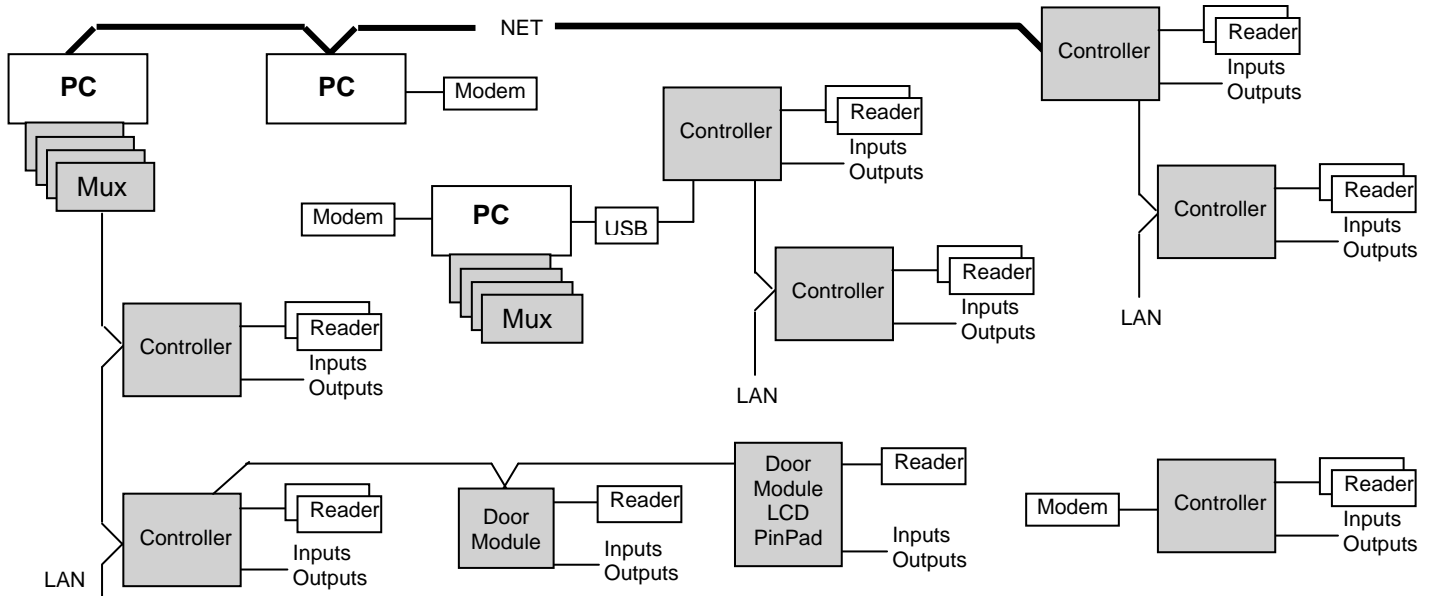
5 SYSTEM ARCHITECTURE

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

Data between the controllers and PC(s) is transferred via Local Area Network(s) (LAN) and PCs are linked via PC networks (NET). The LAN uses 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 uses TCP protocol via UTP or fibre cables, linked via hubs.

Communication on a LAN is via intelligent interfaces installed in to the PCs PCI bus (at least 4 per PC). The data packets contain checksums and error detection and repeats are to be done by the interfaces. Power loss at a controller does not affect RS485 communication to other controllers. Fibre interfaces that regenerate

communication should have UPS units. It is possible to connect at least 254 controllers per LAN and sub-LAN controllers are available, providing the capability of having 4 x 254 x 254 (258,064) controllers per PC. LAN communication is at 9600 or 19200 baud and data transfer is maximized with off-line controllers only being re-rolled every 5 minutes. Empty data packets are typically 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 is achievable, with LAN speed and protocol not the limiting factor. When LAN communication is stopped or not available, controllers buffer 1000 transactions in battery backed-up memory. Controller's time and day of month stamp all transactions.



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

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

Events and alarms are 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. are set at the PC and kept in database files. Changes to set-ups are automatically sent to the appropriate PCs and controllers.

PC SW is implemented in a server (communicates with databases) and clients architecture. Data transfer between Clients and Server is by TCP/IP & Port Number and client applications could be installed on remote PCs or on the same PC as the server. Client applications interface to controllers via the LAN and all the editing and displaying of data done via the clients. Client programs are optimized for speed via RAM tables and should the server or the link go down (i.e. off-line), changes are 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 are synchronized on time schedules with repeats, synchronizing edited data and transferring log and audit files as required. Synchronizing events are logged and scheduled events optionally logged (errors always logged). The links between the systems are TCP networks (not requiring sharing of drives / directories) or dial-up modems. It is possible to use multiple modems with an automatic selection of a free modem. Alarms can be set to be automatically sent to certain servers.

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

6 ACCESS CONTROL CARDS

The cards are passive and, with the exception of MAG cards, permanently factory encoded with numbers & facility codes. Cards are of robust PVC material and construction and are credit card sized. Most card types are suitable for direct printing, those that are thicker, can be detailed by sticking on specialised printed sticky labels. All cards have printed numbers. Various clips and holders are available. Read ranges will vary from type of card. Passive Proximity (prox) cards read range depends on the reader used (typically 10 to 750mm).

7 READERS

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

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

Card code structures that can be read are:

- Wiegand 26, 30, 32, 34, 35 (Corporate 1000), 36, 37, 38, 40, 44 and 52 bit. Cards can have a facility code and coding can be binary or in binary coded decimal (BCD). Checksums are verified. Data can be received starting with the least or most significant bits (card swiped in either direction). New card structures can be facilitated by additions to look-up tables.
- Magnetic cards, track 1, 2 or 3. Coding is in binary or according to the ISO7811/2 standard. Character checks bits and longitudinal redundancy checksums are verified. For ISO cards, the location of the facility code and card number is configurable. Alternate card number locations can 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.

Random card numbers can be up to 10 hex digits.

Biometric Readers (such as finger print and palm readers) that interface between readers and controllers, verifying the cardholder. Fingerprints are linked to cards – cards can be used or not. All fingerprints are stored in the readers (up to 48 000, reader dependant). The addition of these readers requires no addition setting to the normal access system.

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

Digital Keypads (Pin Pads) in a 3 * 4 matrix can be used instead of readers or in conjunction with readers. Time groups are set for when each reader and Pin Pad must be used. A Pin number is from 1 to 6 digits. Cardholders can be given a zero pin, requiring only a card for access. A duress alarm is given when a zero digit is entered before the pin number. All access functions are applicable to a duress event.

Three LEDs are 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 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 are intelligent, microprocessor based control panels that function within the system architecture as described above.

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

Controllers are contained in white powder coated steel metal housings; with key locked hinged lids (lid opening can be monitored). Additional cover plates with appropriate high voltage warnings protect power supplies. Mains supplies are filtered and tranzorb protected on the entry to the housing. Sufficient knockouts and cable space are provided for cable entry and routing, with cables routed appropriately away from the PCBs. The housing and lid are appropriately earthed to the mains earth and terminals are provided to earth cable screens. Reader cables screens must be earthed. LAN screens must be earthed per segment and the segment screens must be isolated from one another. Terminal connections, link and switch options are listed within the housing and an installation booklet is provided with each controller.

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

Diagnostic LEDs are visible on the outside of the housing and mounting should be such that they are visible. A green LED ticking once a second indicates that the controller is on and running. A red LED indicates the status of the LAN, with on indicating communications is correct. Yellow LEDs indicate the reader and I/O activity and flash appropriately indicating correct and error actions.

Environmental conditions are -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 must be provided.

Communications with controllers are RS485 (data, /data and RTS, /RTS) or RS232. These lines are tranzorb protected and have serial protection resistors. Fiber optical interfaces and additional resistor/ capacitor/ inductor/ tranzorb/ surge arrestor interface are available where greater distance and protection is required. The fiber interface is mounted in the enclosure and powered by the controller. The additional protection interfaces are mounted externally. Modems can be installed within the housing where required. Total cable lengths are limited to 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).

Data/clock and Wiegand reader interfaces are opto-isolated and the maximum cable length is 100m for 12V readers and 20m for 5V readers. Reader cables screens, metal housing and mountings must be earthed.

The new generation controllers (not MD350/1 or DF350/5) have a unique electronic ID and all have SW version information. These are reported to the PC.

15 input, 15 output, 15 access, 15 reader enable, 15 Pin Pad and 15 latch control time groups and 30 holidays are stored in the controller and are selected for when I/O and readers are monitored and controlled and when access is granted or denied.

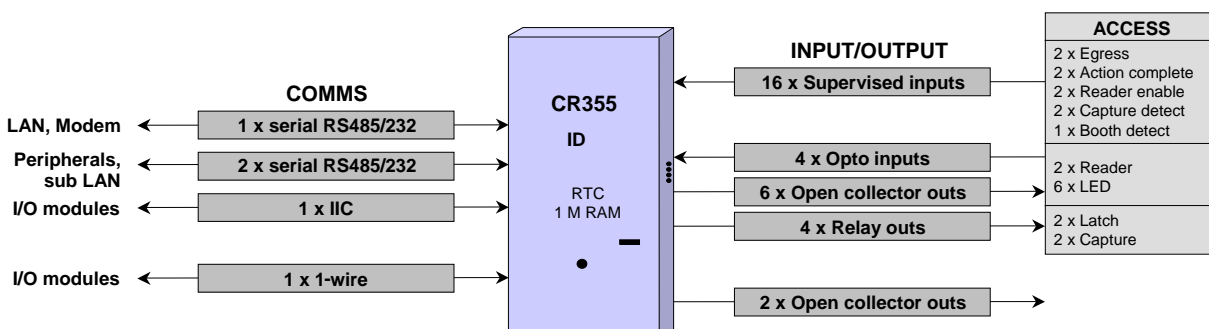
I/O can be expanded on the new generation of controllers and modules via multi-drop 1-wire and IIC interfaces. Relay, supervised inputs and temperature sensor interface modules are available. All relay contact by be protected against fly-back (RC-network for AC loads and diode for DC loads) at the load (externally to the controller).

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

Controller status changes are 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 are used in Firmware development where possible, with machine code only used when speed is critical.

8.2 CR355 (READER AND I/O CONTROLLER)



The CR355 controller has 16 supervised input ports (short and open circuit, contact open or closed), 4 opto-isolated input ports and 12 output ports (4 relays, two normally open, two normally closed, with 28VDC/250VAC, 3A rating; 8 open collector Darlington with 500mA/50VDC rating). I/O can be expanded to via multi-drop 1-wire or IIC bus interfaces. Two RS485/RS232 peripheral ports are available.

Ports are SW configured for functionality. Up to two reader port can be set (opto-isolated ports or via the peripheral serial ports). Inputs can be set as Action complete, APB enable, APB reset, Auxiliary input, Booth occupied, Card capture detect, Egress, Reader enable, Reader tamper or Latch monitor. Outputs are set as Auxiliary output, Booth busy, Buzzer, Capture, Latch or Reader Isolate. I/Os are set for active time group for each detection level. Auxiliary inputs can be set as counting inputs, with count changes reported to the PC after set time-out after count incremented. Capture units can be set at either or both readers.

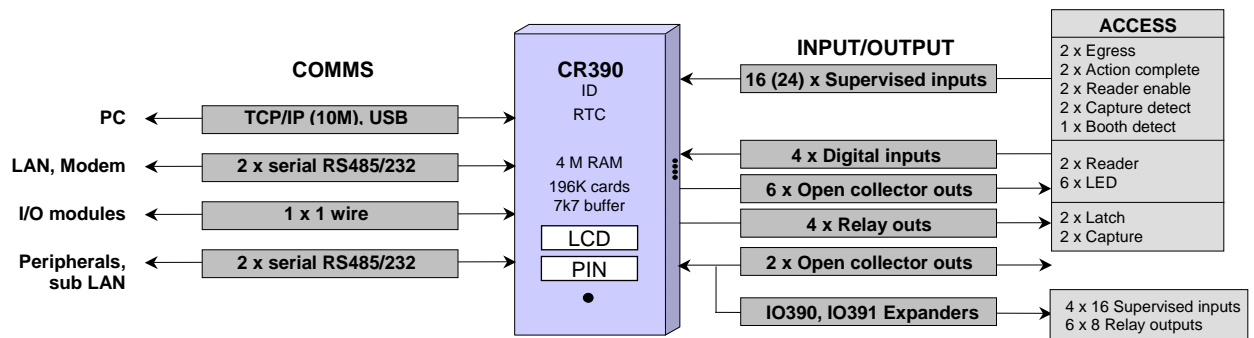
The controller functions in a stand-alone mode with a local card database of up to 65,000 sequentially numbered or 15,000 randomly numbered cards (10,000 with PIN). All access functions are controlled locally, and access granted, denied, card captured, card not opened, door not opened, etc. are reported to the PC. APB and anti-time back (ATB) function are controlled locally between the two readers – with time settings for each reader and selection of clearing other reader ATB for the current card. APB setting is for locally disable reader used / enable other or disable both. APB reset enables all cards for both readers if enabled for either or regardless of current enable.

Access configured I/O are set as normally open/closed (or changeover for outputs), with time-outs and time delay options. Booth/mantrap control is done locally with doors, latches and presence being monitored and a booth busy output can be configured. Setting the interlock option prevents both doors opening. Readers and egress can 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 can set local alarm outputs. Multiple illegal requests can be set disable the reader.

Data in the controller can be viewed and edited with a hand programmer that is connected via a peripheral serial port.

The peripheral serial ports can communicate to readers (with Pin Pads, and LCD displays), tag receivers or peripherals such as note readers, printers, vending machines, etc. (may require specialized SW).

8.3 CR390 READER, I/O AND LAN CONTROLLER



The CR390 controller has 16 supervised input ports with tranzorb protection (short and open circuit, contact open or closed), 4 tranzorb protected digital input ports and 12 output ports (4 relays, two normally open, two normally closed, with 28VDC/250VAC, 3A rating; 8 open collector Darlington with 500mA/50VDC rating). I/O expansion is via up to 4 IO390 (16 supervised inputs each – no tranzorb and 8 open collector outputs) and up to 6 IO391 (8 relay with change over – as above) expander modules – mounted in the CR390 housing. Additional remote I/O can be expanded to via multi-drop 1-wire interfaces and via a piggy-back interface. Two RS485/RS232 peripheral ports are available.

Ports and functions are identical to the CR355.

A random search function (set per reader or overwritten by card setting with inputs for 0% and 100% search) controls an output indicating search.

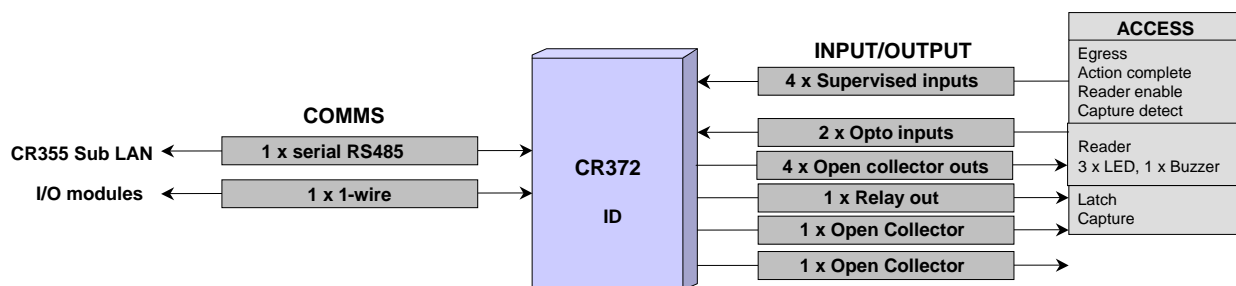
A multi-output control (typically lift control, alarm activation) option via relays controlled locally by outputs of the controller – each card is allocated an output group 1 to 64. Each output group is allocated function(s), with a maximum of 128 functions in a controller. A function is linked to an 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 are be: nothing, off, pulse, till out group input changes, follow latch, follow door open, toggle or on.

An on-board LCD and PIN pad are optional. The local database is up to 196,000 sequentially numbered or 65,000 randomly numbered cards (32,000 with 6 digit PIN). 32,000 16 digits cards can also be selected.

Data buffering is 1,700 to 7,000 transactions, depending on database selection. Communication with the PC is via RS485 (multi-drop), RS232 (modem), optical fiber interface (additional), TCP/IP or USB. The CR390 can also serve as a LAN controller, interfacing controllers via RS485 multi-drop to the PC.

Test modes are available to simulate multi-slave nodes and to generate multi-events. Communication monitor and test options can be set and configured.

8.4 CR372 (DOOR MODULE)

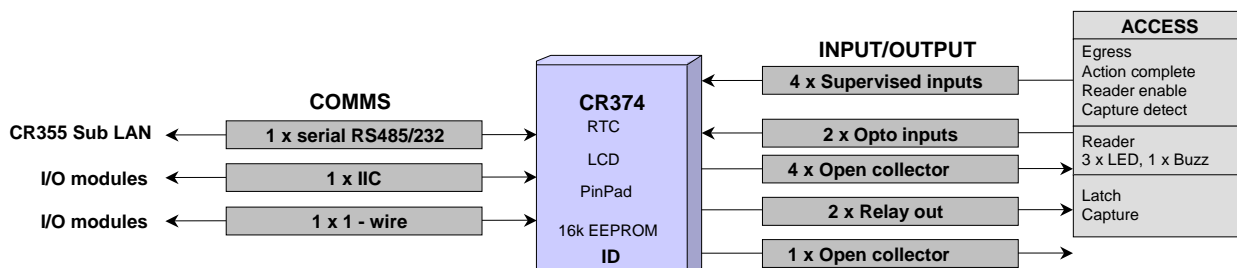


The CR372 module is a front-end door controller for the CR355 controller; monitoring 4 supervised input ports (short and open circuit, contact open or closed), a reader via 2 opto-isolated input ports and controls 7 output ports (1 normally closed relay with 30VDC 2A, 150VAC 1A rating; 6 open collector Darlington with 500mA/50VDC rating). I/O can be expanded to via multi-drop 1-wire bus interfaces. Input and reader data is read and changes passed to the CR355. The CR355 controls the outputs.

Communication between a CR372 and a CR355 is via a multi-drop RS485 cable with a maximum of two CR372/CR374s connected to the cable.

Supply is 12VDC, 50mA (excluding power to the reader and latch).

8.5 CR374 (DOOR MODULE WITH PIN PAD AND LCD)



The CR374 module is a front-end door controller for the CR355 controller with LCD and Pin Pad; monitoring 4 supervised input ports (short and open circuit, contact open or closed), a reader via 2 opto-isolated input ports and controls 7 output ports (2 relays, a normally open and a normally closed, with 30VDC 2A, 150VAC 1A rating; 5 open collector Darlington with 500mA/50VDC rating). I/O can be expanded to via multi-drop 1-wire or IIC bus interfaces. Input and reader data is read and changes passed to the CR355. The CR355 controls the outputs.

A 3x4 or 4x4 Pin Pad can be interfaced to, a 3x4 Pin Pad can be mounted directly on the PCB. The 3x4 matrix emulates a 4x4 Pin Pad by using a shift key to 4 of the keys. A standard LCD interface (8 data bit, R/W and enable) is used and a 2 line by 16 characters LCD (with back-lighting) can be mounted directly on the PCB. The CR355 controller displays the real time and the access status (e.g. "denied" or "proceed"). The

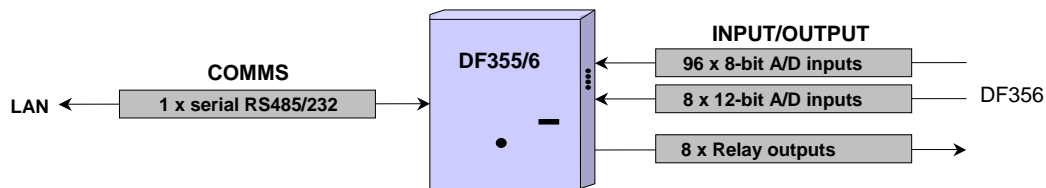
PC can display additional data such as the cardholders name, available subsidy, accumulation time, messages, etc.

Communication between a CR374 and a CR355 is via a multi-drop RS485 cable with a maximum of two CR372/CR374 connected to the cable.

A 16k EEPROM and a battery backed-up RTC can be incorporated on the PCB in specialized stand-alone applications.

Supply is 12VDC, 150mA (excluding power to the reader and latch).

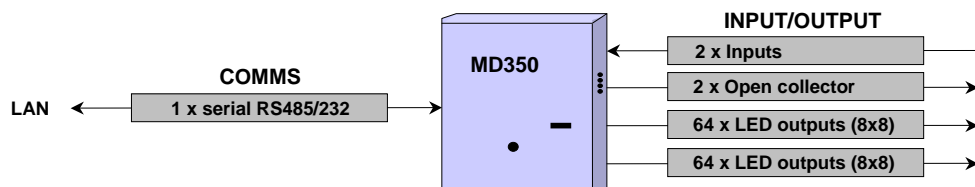
8.6 DF355/6 (I/O CONTROLLER)



The DF355 controller has 96 8-bit A/D input ports and 8 output ports (relays with 28VDC/250VAC, 3A rating). The DF356 has an additional 8 12-bit A/D input ports.

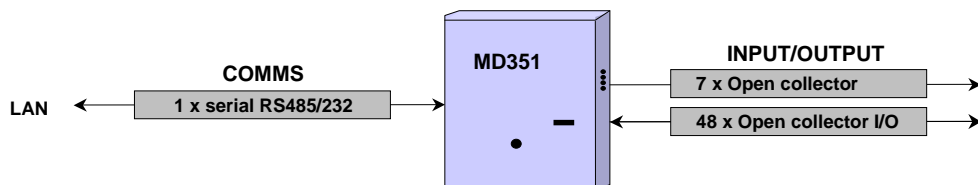
Input ports are SW configured for functionality and are A/D inputs or supervised inputs (short and open circuit, contact open or closed). Inputs are RC protected and resistor values can be changed to allow high input voltages (normally 0 to 24VDC, 20mA). Changes in input statuses and control of outputs on time groups are reported to the LAN.

8.7 MD350 (MIMIC DRIVER)



The MD350 controller strobes 128 x LEDs in two matrixes of 8 x 8. LEDs are pulsed with 8VDC. The inputs are monitored at TTL levels and are reserved as accepts alarm and lamp test (done locally) inputs (both are reported to the LAN). LEDs are switched on, off or flashed (rate received) by commands from the LAN.

8.8 MD351 (I/O CONTROLLER)



The MD351 controller has 7 open collector Darlington outputs with 500mA/50VDC rating and 48 ports that can be set as inputs (TTL levels) or outputs (open collector Darlington with 500mA/50VDC rating). Input / output selection is in sets of 8. Relays boards with 8 relays (28VDC/250VAC, 3A rating) are available. Changes in input statuses and control of outputs on time groups are reported to the LAN.

9 COMPUTER SPECIFICATIONS

The minimum requirement is a PC running and compatible with Microsoft Windows 98 (second edition), NT (with service pack 6 or later) or Windows 2000/XP operating system:

Processor: Pentium III 1GHz.
RAM: 128M (256M for installation of more than 5000 cards, or high number of events).
Hard disk: 500M.
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 has been developed by Softcon (certified Microsoft Solutions Provider) in South Africa using Visual C++ (32bit) and incorporates COM object modules. The platform is Microsoft Windows 98/2000/XP/Vista or NT operating system. The minimum requirements are:

Windows Millennium.
NT4 SP6.
2000.
XP
Vista.

The SW complies with the requirements are described in the system architecture section above.

The SW effectively allows 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 is client / server programs, with the server program executing database read and write functions using the sequential query language (SQL). Connection to the database uses open is via ODBCs, facilitating connection to practically any database (MS Access, Oracle, SQL Server - 2000, 2005, 2005-express, with authentication or not). MS Access 2000 is the standard used. The server program is installed where the databases are located, with no SQL command being executed over a network. When the server starts running, databases are automatically compacted and are selectively checked for correct fields and types and the set number of records. If incorrect the data can be automatically repaired or repaired on query. Defaults are set for records to be added. Databases location, file name, table and field names and field types, size and indexing can be changed (requires updating of report forms). Fields can be set as unique, preventing duplication (e.g. unique ID, card and employee numbers). Via command line options, client can be set to connect to predefined servers (e.g. to server running on local PC, PC xyz or on PC abc).

Databases can be password protected and encrypted. Passwords and menu access setting are encrypted and can only be changed via the appropriate menus and password levels.

The software is highly configurable and is event-driven. A variety of objects are 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 generate or are as a result of 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 is granted or denied by the controller that contains a local database.

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

Point of sale (POS) can be incorporated in the system as a separate exe client program.

Vending applications such as canteen and vehicle park entry control, cashless vending, Photostat-, Laundromat-, Car wash control, fuel pump control, cash loaders, etc. can be implemented. A Cash Add module is incorporated in the Client program or is available as a separate exe client program.

The set Windows date and time formats are used. For clarity and simplicity the format YYYY-MM-DD HH:mm:ss is referred to and preferred.

10.2 SECURITY LEVELS

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

Users can be set with start and expire date/times. Passwords can be set to expire, forcing the user to change password. Logging off reverts to a default group whose access rights are configured. Users can 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) are 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 is displayed in the Windows header.

10.3 LANGUAGE SUPPORT

All display and print strings are set in data files, facilitating the change thereof to different languages. Presently, English and French files are available. [Language choice is set per user.](#)

10.4 SCHEDULES (TIME ZONES AND GROUPS)

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

- 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 can use any of the time groups, time groups used by controllers use only the relevant groups (first 6 in the list above). An optional setting for controllers allows the use of any of the first 60 groups (8 time zones per 15 groups) for the relevant function.

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

Access cards are allocated a time-group limiting when access is granted. When time group 0 is set, the time group for each area zone for the cards area group is used, resulting in time groups per area zone.

Time groups can be used 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

All edit functions are logged in audit files (file per day) and changes affecting controllers are automatically sent to the appropriate controller(s).

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

A list comprises of rows and columns of data similar to a spreadsheet. A row displays a record of data and the records are displayed via selected filters. These filters are administrator defined SQL command. Columns are fields and the order and width can be changed by simple click and drag actions. Column names are editable and columns can be hidden, or set as visible (faded) or editable. Columns can be displayed in bold font. Sorting of records (ascending or descending) is by simply clicking on column names. Multiple sorting of records can be selected (e.g. sort by department, then by name). The displayed color of the data can 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 can create new lists. Lists are ordered in menus for status (displaying the current status or readers, inputs, outputs, etc.) set-up, card data and vending. A variety of lists are provided, showing inputs in alarm, not accepted, etc. Visible columns for selected rows can be printed (with column names and widths as displayed).

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

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

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

Serial or USB card and barcode readers can be connected to PC COM or USB ports at settable baud rates and bit structures (including parity). A reader can be incorporated 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 are set for serial, USB and key readers, filtering data read to match data in the databases. USB smart card reader can be used.

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

10.6 ACTIVITY DISPLAYS

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

Each input, output, counter and reader event is set for display or not, for each status (e.g. display a door opening, not closing). Displays can be time selected (e.g. certain door openings are only displayed after hours). Settings are 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., indicate the status of all monitored and controlled objects in the system. When objects change status and are in alarm, the symbol flashes 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 is displayed. Drawings with alarms are automatically displayed on the top of the desktop. Drawing can be linked to other drawing (via item icons) and to have sub-drawing (right click on an item icon).

Database items and counters can be displayed and edited on a drawing. Data and photos are display linked to cards presented to readers. Clicking on certain display items can 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 are set to be visible or editable for user groups.

A library of symbols is provided and can be added to. A background to a drawing is a symbol. Symbols are bitmaps, jpeg or tiff files. Free text can be included in a drawing and an item can be a symbol or text.

The creation of drawings is via an integrated drawing module. Items can be added, deleted, modified, copied (as a single item or as a group – with distances between them fixed). Items can be aligned or equally spaced, brought to top or send to back of display. WYSIWYG editing features with pixel position settings and display. Font, size, rotation, color and attributes (bold, italics and underline) of text and database items can be set. Align can be set on text. Undo is provided. Hot keys are available to simplify editing.

10.8 EVENTS

Events are messages that are generated by occurrences that happen in the system. Events are generation is by:

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 are 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 are set to 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 are fixed (e.g. power-up is always logged, printed, event-trigger, display), others are settable (e.g. every input level is set).

Events can 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 are 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 are set to occur within set time-outs (HH:mm:ss) between events. Sequencing can typically be set to require a sequence of cards (specific and/or group) before an open door event is generated. Time groups can be used in algorithms, with the time group being true when the time group is active.

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

10.9 COUNTERS

Counters are kept on entries per reader. Every Input and output has a counter, incrementing when the input or output changes to a count level set per input or output (e.g. when the door opens). These counters can be reset with events, recording when the counter is reset.

Virtual counters can be created that increment or decrement by set values on specified events (triggers). The new count value is 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

are 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). Events can set counters to any value.

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

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

10.10 TIMERS

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

10.11 ACCESS CONTROL

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

Zone linking: Area zones can be linked 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 is allocated an area group, which can be unique to the card, or cards can share groups (e.g. cleaner group, admin group). Area groups can be batch loaded with area zones. An area group can be disabled. Cards can be allocated multiple groups, e.g. parking group and 1st floor group.

Anti-passback: APB is settable per reader. The last area zone entered by each card, via an APB reader – the last APB location, is stored. Access is 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 is denied. Denied accesses as a result of APB and strictly from considerations, are reported as such. A card can be set to have a free APB/strictly from movement. A global free APB/strictly from movement can be set (by editing or via an event) and if a card access is denied with APB or strictly from, access is granted if the last APB movement was before the free set time.

Zone time-out: Area zones in access groups can be set with time-out of 1 to 99 minutes. Cards are disabled if they stay in the time-out area zone longer than set time-out.

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

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

Zone counters: Each card can be set with an overall and with a period zone counters. Area zones are 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 is used and area zones can be added or deleted from the cards area groups. A count period is set per card and the period counter is automatically re-loaded when the card is used in a new period. The start of count periods is synchronized to a certain time of day and to a specific day of the week or day of the month.

On-line/Off-line: Each reader is set to contain a reader database or not. When set with a database (generally set), the controller effectively does 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, the card becomes disabled for the reader if APB is set. When reader does not contain database, only the facility code is checked by the controller, all other functions are done by the PC. APB, enforced zone control, zone counting, cards linked to hosts, random search and expiry functions are always controlled by the PC which updates the controllers as required. Should a controller be off-line, these functions are not active for that controller. Where systems are configured to function independently, changes to card locations in one system are unknown to other systems (until databases are synchronized), possibly resulting in these PC related functions not functioning as expected – requiring implementation changes (not separate systems or reduce synchronize period). A reader could be set to allow access to cards with correct facility code when the controller is off-line (card database settings are not checked).

Reader databases are 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 are reported as out of area and if access is granted, the oldest card to have been granted by either reader is replaced in the controller by the new card. Controllers can be set to require a PIN code (on time schedule), with or without card (on time schedule). 10,000 cards with PIN are stored in the controller.

Card numbers: Card holders can 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). Using master card link (see below), a card holder could have multiple cards.

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

Virtual cards: Any card in the database can be set as a virtual card (by checking the cards virtual option) – such cards are not sent to controllers and are used as control group cards (see below) or as trigger matching cards. Selecting a virtual card in event triggers (e.g. events generated on trigger events), the set virtual card is compared with card in the triggering event – and should all the non-zero parameters of the virtual card match the card – the trigger is true. For example an alarm system must be disabled (by closing a contact) when any card is used that has trigger group 10 and belongs to department 15 (thus the virtual cards only settings are trigger group 10 and department 15).

Control group (control card): Cards can 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 can be used as a card control group by setting the virtual card option (card is not set to controllers).

Master card link: Multiple cards can be linked to a card holder by setting a card link to a master card. All zero parameters of a card use the parameters of the linked master card. Typically a card linked to a master card only has the card number set. Whereas control group cards are set as virtual, a master card is not a virtual card and can be used as an access card.

Temporary card link (typically used when a card holder has forgotten card at home): A card can be linked 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 is automatically regarded as disabled (the set status is not changed). The temporary card functions as a card with a master card link and typically only has a card number.

When a card that has a temporary link is used and the temporary card is not linked back (master card link) or the temporary is not enabled, the temporary link is automatically cleared. Thus the temporary card is automatic cancelled by either clearing the temporary cards master link or by disabling the temporary card. Typically the temporary card is set as a capture disable card (automatically disabled on capture) or set with an expiry and an expired status of disabled (or capture disable).

When a card becomes disabled (or when a disabled card is used) and has a master card link and the master card has a temporary link back (thus a card that was a temporary card), the temporary link of the master card and the master link of the temporary card are automatically cleared.

Access events are 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. Every card can be allocated a trigger group, which is included in the cards events – to be used to match count or event triggers (e.g. count cards that belong to a specific count group).

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 will 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 is checked for matching vehicle registration.

The **random search** function is triggered automatically when cards enter via readers set for random search. A search % is set for each search reader and could be overwritten by a % set for the card, i.e. the cards set % is used or if zero, the reader setting is 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 are linked to the search readers that are controlled closed or open when search is required or not. Random search can optionally be via PC control or function within the controller.

Generally, when access is granted an **output** (typically a latch or barrier) is controlled. This is generally done locally (on or off-line) by the controller – or via event in the PC.

Multi-output control (typically lift control, alarm activation)– can be done 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 are: 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 is configurable.

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

A cardholder's data is displayed in lists and property sheets. The data can be viewed and edited (password dependant) is listed below. Editing aids and batch loading is 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 is general data regarding the cardholder and has no effect on the functioning of the system. These are administrator-defined fields and the data is editable and is not checked for format or contents, and is not changed by the system when the card moves. The default data is (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.	<p>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), set where the card has access to.</p> <p>The cards status (disabled, enabled or capture) is set for normal operation, when expired and when the cards counts are not available.</p> <p>Card start/expire time-dates set when the card is active and can 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 is used and the add/delete area groups are checked.</p> <p>Absent (on leave) start and end date-time with area zones added / deleted and an absent status when within absent period.</p> <p>A capture group sets where the card is captured.</p> <p>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.</p> <p>A master card links the card to a master card (used to give a holder multiple cards) - card settings of zero use the corresponding settings of the linked group control card.</p>
Time Group.	<p>Defines when a card may be granted access. One of 15 access time groups are 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.</p>
Trigger Group.	<p>Selects a group that is added to the cards events and is used to trigger events and/or counters.</p>
Accumulation.	<p>Day, week and month totals since the last day-, week- and month-end, are automatically updated when the card enters via clock in and out readers. These totals are not editable. The required total minutes can be set and is used in reports that calculate accumulated times exceeded and shortfalls. The period leave time can be entered and a card can be enabled or disabled card from clocking.</p>
Counters.	<p>Two counters are available for a 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) can be added and deleted from the cards access zones and an alternative card status is used. The cards available period count is automatically reloaded when the card is used in a new period. Periods can be synchronized to time of day, day of week or day of month.</p>
Number.	<p>Two card numbers can 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).</p>
Previous.	<p>This number indicates the previous card number the cardholder used and is only used for documentation purposes and does not affect the functioning of the system.</p>
Linked to.	<p>The card can 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 is by the PC (data not in controller). If the host card is a virtual card, it is used as a mask to find cards present that match non-zero settings of the host card.</p>
Visitor ref.	<p>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) is displayed. If a normal card, the reference is zero.</p>
Pin code.	<p>A 1 to 6-digit pin number can be allocated to cards when Pin Pads are installed. Depending on the set-up of the Pin Pad and reader time groups, access is via either card or pin code or both. Cards set with a pin code of zero gain access only by card and no pin is required. A duress alarm is generated (access is granted if the card normally has access) when the code is entered proceeded with a zero digit.</p>
Pass back.	<p>A card set as a pass back card, overrides APB, i.e. the card can be used for multi-access to the same area zone without the requirements to exit the zone (as is required for APB).</p>
Random.	<p>A random search % of non-zero overrides the search % set for search readers and is used to determine if the cardholder must be searched.</p>
Licence.	<p>Six licence types with expiry can be selected 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).</p>

- Vend data.** Card token, subsidy and values are used in POS and vending applications. Amounts available, remaining and periods are set per card. Cards can belong to a cost group – using the token, value and subsidy of a group. A discount group can be set, with item discounts being allocated to the group.
- Park start.** When entering via a reader set as a park entry reader, the time and date is set to park start. This data is used when the card is presented to park display, park pay and park exit readers.

10.13 CARD ACCESS ZONE DISPLAY

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

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

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

Any Windows compatible printer can be used. Print preview can be selected.

10.15 VISITOR CONTROL

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

10.15.1 Card Access Control.

Visitors are 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 is 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 can be set as capture cards, to be captured at readers that have capture units. Cards can be set to be captured at selected capture units (not captured at not selected bins). If access is granted at a capture reader and the card is set to capture at that reader, a control signal opens the capture bin and once the card is “dropped” in the bin, the door/barrier is opened. For cards that are not to be captured, the reader functions as if no capture bin is present. Cards captured are logged as being captured and the cards can automatically be disabled (set per reader).

Link To Hosts. A visitor card can be linked to hosts (many visitors to a host), and if access is allowed at a reader, access will 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 is 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 is granted to the visitor the card if any card with department x is present). The PC grants access to cards that are linked to hosts,

i.e. visitor card data does not reside in the controller and the PC must be running the access program for access to be granted.

Fingerpirt. Options are available for using only fingerprint for access control (card not required), capturing fingerprint on entry and granting exit only if matching fingerprint currently entered. Taking of video snapshots on entry and exit can be set.

10.15.2 Visitor registering system.

This is an optional system that is used to register visitors. It is 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 holds data on visitors that have been registered. Functionality of the system is 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 can 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 are available.

Data in the pre-registered data base (see below) can 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) can be taken / scanned by the system and be displayed and are stored on the PC disk and are automatically allocated file names linked to a set data field (e.g. ID number, database reference). Photo / signature / document capture specifications and options are the same as the card maker.

Voice samples can be captured in a .wav file that is linked to the visitor and a fingerprint can 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 are selectable.

The visitor data is copied to the active access card database by allocating an access card to the visitor. Data that was not editable is not transferred, facilitating the pre-setting of visitor cards with certain parameters (e.g. to where that card has access). Card start and expiry can 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 is 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) can 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 can be printed on any Windows printer installed. Multiple print formats can be designed by the system as described for the card maker. A card design is allocated to the card.

Card activity is 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 are recorded in the visitor database. Manual and automatic facilities are 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 are password protected. Operators are logged on/off.

10.15.3 Visitor pre-registering system

This is an optional system that is used to pre-register visitors. It is a client program running on one or more PCs. A visitor is 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 can be set via a web page and emailed to the system that automatically adds the data in the database. Email requires a specified format and password – email users must be registered with a password.

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

The visitor is 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 is issued by clicking on the visitor data and the card is presented to the reader or if a card "spitter" is installed, the card is issued automatically and read. The barrier is automatically opened. The cards are enabled for selected readers and adhere to all access control selections. Cards start and expiry can be set automatically.

The visitor can be allocated an available parking bay from a list, reserving the bay to the visitor (providing a link from vehicle to visitor). This is 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 is removed from the pre-register database. The parking bay is set as available. The barrier is automatically opened. Data in the pre-registered database of visitors not currently on site is automatically deleted if the expected departure date exceeds the current date.

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

All menus and functions within menus are password protected. Operators are logged on/off.

10.16 INPUT/OUTPUT

Inputs are 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 can be set as counting inputs, with count changes reported to the PC after set time-out after count incremented. Each input is 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 is 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 are set as Auxiliary output, Booth busy, Buzzer, Capture, Latch or Reader Isolate. Multiple output control on card read is as listed in **Multi-output control** above.

I/Os are 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 are controlled via access cards that request dispensing/purchases. The system functions on-line, with the PC client program granting or denying the requests.

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

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

Product stock management can 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 are generated.

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

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

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

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

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

10.18 PARKING

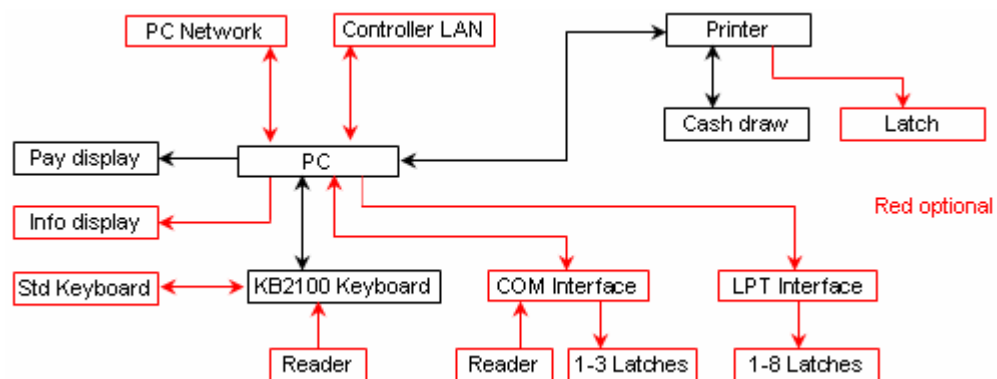
10.18.1 Pay on exit – Access system

A pay on exit option to access control allows 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 is logged to the card database. The exit reader only grants exit when the time present (after entry or after pay) is free. A parking fare data table sets the amounts payable for the present intervals. Park display readers indicate the present time and the amount payable and pay readers displays the time present, the amounts due and resets the entry time to the current time (the amount due is logged).

10.18.2 Counting system

The access control system can be set to control parking area(s) for multiple tenants (companies), limiting access based on a maximum count per tenant. Available parking for the appropriate tenants automatically decrement and increment when cards enter and exit. Visitors are 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. Overall counters can be set 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 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 can be vehicle colour, registration and number of occupants and can be set as required, optional or not required per vehicle type. Administrators can override these settings

Parking tariffs are 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 can 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 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 are only be available when the keyboard is in supervisor mode via a key setting or set via a management PC.

The amount payable is 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 use access cards that are issued on entry and retrieved on exit. These cards are be tagged at readers in the access control system or at readers connected directly to the PC (serially or integrated with the keyboard). Readers are 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.

10.18.4 Pay on scan – POS system

A card (typically a barcode) is read and the number in entered in to the card database. Exit is granted on reading the card at the exit reader. Settings are available to rotate the card database where the card is stored. All above options of payment is available.

10.19 TIME ACCUMULATION, T&A

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

10.19.1 Accumulation

The system can be set to perform an overall time accumulation of how long each cardholder was “on site”. Full time and attendance is available by linking to T&A systems.

The provided accumulation functions 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 are kept: a daily, weekly and a monthly total. The daily total is 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, are logged and cleared of daily and weekly or monthly totals. On other day ends, only cards with daily totals are logged and cleared of daily totals.

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

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

10.19.2 T&A Systems

Numerous Time and Attendance and payroll systems interface to Softcon Access systems and vary on functionality and features. Generally the Softcon system provides 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.

Event Log Files. As all events are stores in log files, the clock times can read in the daily log files. The clock in/out events have the following data in the fields as indicated:

Date_time	yyyy-mm-dd hh:mm:ss.
type	1 (reader).
Sysno	reader number (specific readers are set to clock in/out, referenced to ACCESS.MDB reader_status.reference). The table field reader_status accume set to 1 for clock in, 2 for clock out.

Status	22 (card entered).
Xref	card reference number (reference field in the card database CARD.MDB card_data.reference).
Employ	employment number.

Additional data for the card is available in table card_data in CARD.MDB, e.g. employ, ID, department, etc.

Clock In/Out Files. As an alternative, a special SW driver can be set which logs the clock in/out events in dedicated file(s). A variety of drivers are available which have been specifically tailored to the T&A system requirements. These log files are typically "flat ASCII" files, with a line per clock in/out.

A typical format of the line is:

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 can replace the employment number. Separating character can 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 set-up as required. If the file does not exist, a new file created when a card clocks in/out. The T&A system renames the file before reading the data.

An integrated T&A system will be added to the system in the future and will be available as on optional extra.

10.20 ASSET MANAGEMENT

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

An asset database 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 sets the hour periods 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 can be displayed and edited: Purchase price and date, supplier, maintenance period, next maintenance date and responsible person.

Asset management options are:

10.20.1 Asset issue/return

An asset issue/return menu is integrated in the client system or run as a separate program. All functions are password protected and generally users only have access to the system via asset and card readers.

Assets are 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 cannot be issued. Start date/time is automatically entered when issued.

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

On issue and return, slips containing all relevant information (configurable) can be printed automatically, or on request. All events are logged and contain date/time, logged on-operator, user issued to, user returned and charged data. Reports are 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) are via external systems or via asset tag readers connected directly to the Softcon CR355 controllers. The last reported tag location, date/time, battery measurement, alarm status and alarm date/time are automatically recorded.

These options are being integrated.

10.21 MESSAGE DISPLAYS

Events can be set to open a message window. A set default file is opened 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 is in .RTF format and can 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) can automatically be inserted in the display.

10.22 OPERATOR OCCURRENCE LOG

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

10.23 AUDIO WAVE FILES

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

10.24 SMS

Message are set 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 are sent on algorithm of event triggers (time groups can be used in an algorithm, with messages only being sent when the time group is active). A message can automatically include event and event-referenced data (e.g. controller number and controller name). SMS activities are logged as events.

10.25 EMAIL

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

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

10.26 TELE-CALL CONTROL

By linking a cell-modem, events can be generated 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 are set to be logged per input level, output level and per reader and can 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 are logged. Logging is done in database files, with a new file being created per day. Optional log fields and the length of such fields can be set (e.g. card holder's name and employee number). The oldest day files are automatically deleted when the server's disk becomes 80% full.

Editing of data, including the adding and deleting of records is logged in an audit file, recording the operator, the old and the new data. Audit data is stored in database files, with a new file being created per day.

10.28 REPORTS

A comprehensive separate reporting system generates reports from data files. A report is 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 include all set-up, audit, accumulation and events. Parameter requested of the operator can be configured.

The report forms are generated utilizing Seagate Crystal Report (Crystal Reports is not provided, the forms are). Report forms contain the site name and totals of the number of records found. Reports are available 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) can be generated via any PC linked to the system. Reports can 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 is logged.

10.29 INTERFACING TO HOST PROGRAMS

10.29.1 Event linking.

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

10.29.2 Data sharing.

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

Shared database. The common fields of data are located in a central database, which is accessed by both systems. The Softcon system must be able to access this data in real time, i.e. the database must always be available when transactions take place. The database type can 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 can 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 can be set or can be done on event.

Converters. A variety of convert programs are 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 are updated accordingly. A configurable LDAP converter is available that imports data to the card database.

10.30 BACK-UP STORAGE DATA

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

10.31 ON-LINE HELP WINDOWS

The system has a built in comprehensive help and contains all Software and Hardware set-up and installation related issues. Pop-up help (in the selected language) is 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 are available that limit certain functions and quantities. The versions are protected via encrypted installation files and by HW keys on the MUX card. Access to more options is via appropriate keys.

The included column indicates which SW packages (may require additional controller HW) contain the option as standard, with AS380 (mini), AS381 (lite), AS382 (standard), AS383 (super), AS388 (free) and cardmaker, indicated with 0, 1, 2, 3, 8, C.

FUNCTION	DESCRIPTION	SW
Accumulation	Enables the accumulation of time attendance calculation of cardholders.	1, 2, 3
Asset Track	A future option of linking asset tags to cardholders and manages assets.	None
Attendance	A future option of time and attendance functions.	None
Audio	Enables the playing of audio files on the occurrences of set events.	2, 3
Card Makers	The number of card maker programs that can run (requires a connection setting and network enabled if SCS_Server is not on the same PC). 0 disables Card Maker.	C
Card program	Enables card to be programmed via the card maker or via a card edit menu.	3
Cards (x100)	The number multiplied by 100 of access cards in the system.	8=1, 0=10, 1=20, 2=50, 3=n, C=50
Connections	The number of programs that can connect to the SCS_Server (on the same or different PCs). Should a program no be on the same PC, the network option must be enabled.	8=1, 0=2, 1=4, 2=8, 3=16
Controllers	The number of controllers connected to in the system.	8=2, 0=5, 1=12, 2=60, 3=200
Crystal	Yes enables additional special reports.	8=5, 0=30, 1=60, 2=100, 3=n
Distribution	Yes enables the synchronization of databases using the distribution server. Also requires network or Modem distribution setting.	None
Drawings	Enables SCS_Drawing that displays events and allows operator control graphically. Requires the connection option.	1, 2, 3
E-mail	Enables the automatic email of events and reports (future option).	3
External File	Enables clock in and clock out data to be sent to data files.	None
External Link	Enables the linking to external programs to get or send data and/or events.	None
FP Access	Enables the fingerprint access control via TCP readers.	None (option to 1, 2, 3)
FP Capture	Enables the fingerprint capture via TCP and USB readers.	None (option to 1, 2, 3)
Fuel manage	Enables the fuel management functions.	None
Guard Tour	A future option of patrolling guards control.	None
Inputs	The number of inputs.	8=32, 0=80, 1=240, 2=960, 3=n
Messages	Enables messages to be displayed when set events occur.	None
Modem Cntrls	Enables modem communication directly via dial-up modems.	None
Modem Distr	Enables the synchronization of databases between systems via dial-up modems. Requires the distribution option.	None
Mux Cards	The total number of mux cards in the system.	0=1, 1=2, 2=4, 3=8, 8=1
Network	Enable programs to connect to SCS_Server via a PC network.	2, 3
Occ. Log-Book	Enables the editing of a logbook when wet events occur.	2, 3
Outputs	The number of outputs.	8=10, 0=25, 1=60, 2=300, 3=n
Parking Pay	Enables the pay on exit parking functions.	None
Photo capture	Enables the capture of photos in card edit, card maker or visitor capture menus.	C, 2, 3
Photo display	Enables card photos to be displayed in drawing, card maker or card edit menus or in visitor capture.	C, 2, 3
POS	The number of Point Of Sale programs (requires a connection setting and network enabled if SCS_Server is not on the same PC). 0 disables POS.	None
PPOS	The number of pay on entry Parking Point Of Sale programs (requires a connection setting and network enabled if SCS_Server is not on the same PC). 0 disables PPOS.	None
Random search	Enables random search functions.	2, 3
Readers	The number of readers in the system.	8=4, 0=10, 1=24, 2=120, 3=n
SMS	Enables the sending of SMS messages on events.	None
SWin3 Version	The maximum version number that updates are enabled for. Versions after the set maximum may have options that are disabled.	All
Transl. AZG	Enables the area zone group converter to run. Requires the connections option.	2, 3
Transl. Spec	Enables special converters to run (other than AZG converter). Requires the connections option.	3
Vending	Enables the vending functions.	3
Video control	A future option of camera and video control.	None
Visitor Capture	The number of Visitor capture programs (requires a connection setting and network enabled if SCS_Server is not on the same PC). Excludes photo capture. Includes print.	2=1, 3=4
Vis. Pre-registr	Enables the future visitor pre-register option.	None
Visitor/host cntrl	Enables cards to be linked to host cards (follow me).	2, 3
WWW	A future option allowing the system to be access via the WWW.	None

A demo version is available that requires no mux card (also for lap top computers).

An expiry date is initially set, after which the SW is automatically blocked and new test keys must be obtained from Softcon. The default is 90 days.

Updates are available from Softcon or on the Internet. Most updates are free, additional functions could be charged for. When updating a system, the installation set-up is not lost, the new functions are simply added. Changes to field types are reported and can be updated or accepted. Updating from the DOS version to the Windows version requires updating the EPROM and a PAL on the MUX card. Updating from DOS and

SoftWin versions to SoftWin3 may require the re-setting of certain data – converters are provided where possible.

10.33 VIDEO LINKING, *VIDEO /CAMERA CONTROL

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

A configurable snap-shot viewer is 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 is possible to freeze Windows, save-as and delete.

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

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

10.34 *CONTROL VIA WWW

Options to be available in future versions.

10.35 *GUARD TOUR

Options to be available in future versions.

11 TESTING – SIMULATION AND MONITORING

11.1 HW OFF-LINE

All controllers and modules have SW versions for testing (a different EPROM version) and are 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 are available. Test results indicate passed or where errors are encountered.

11.2 SW ON/OFF-LINE

The following monitors and simulators are 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.

Simulation files are provided for all controller types. These are text files that can be edited and new files can be created. Simulation commands for simulation speed and to create execution loops can be set. Parameters such as PC time and literals such as MUX and node numbers can be set in commands, simplifying the use of stored simulation files. Single line can be executed or files can be run continuously.

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

12 FUNCTIONS / OPTIONS SUMMARY

The following tables are summary lists of the possible requirements detailed above. The suggested general minimum requirements are indicated as 'yes' in the requirements column. The included column indicates which SW packages (may require additional controller HW) contain the option as standard, with AS380 (mini), AS381 (lite), AS382 (standard) and AS383 (super) indicated with 0, 1, 2, 3. Where included, the quantities vary for the packages. **Included or not are subject to change** – please contact Softcon.

12.1 SYSTEM

Para	Description	Require	Included
5,8.2	Controllers function in stand-alone mode	Yes	0,1,2,3
5, 8.1	Battery backup memory (set-up and card database), real time clock	Yes	0,1,2,3
5	Directly to 2 readers	Yes	0,1,2,3
5	Door modules	No	0,1,2,3
5	Fiber controller LAN	No	0,1,2,3
5	PC network – TCP via UTP or fiber, linked via hubs	No	2,3
5	LAN comms via intelligent interfaces with error detection and repeats	Yes	0,1,2,3
5	Comms to controllers TCP and USB	Yes	0,1,2,3
5	Sub-LAN between controllers and LAN controller	Yes	0,1,2,3
5	1,000 transaction buffer in backup memory, time and day of month stamped by controller	Yes	0,1,2,3
5	Dial-up between PC and controllers on schedules or alarm	No	No
5	PC SW in server/ client architecture	Yes	0,1,2,3
5	Server/ clients on multiple PCs	No	2,3
5	Clients continue functioning off-line if server not available	Yes	0,1,2,3
5	Database synchronization between PC systems on set schedules, on alarm	No	No
5	Dial-up between PCs	No	No

12.2 HW

Para	Description	Require	Included
6	Cards directly printable	No	No
7,8.2	Opto-isolated Wiegand reader interface	Yes	0,1,2,3
7	Serial, data/clock, touch reader interface	No	0,1,2,3
7	Wiegand 30 bit cards with facility code and checksum verification	Yes	0,1,2,3
7	Wiegand 26, 32, 34, corporate 1000	No	0,1,2,3
7	Smartprox (read and write)	No	No
7	ISO MAG cards with settable data location and checksum verification	No	0,1,2,3
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	0,1,2,3
7	Fingerprint or palm readers integrated with system	No	
7	Pin pads with/without card readers on time group, duress alarm	No	0,1,2,3
7	3-LED readers (Flash amber=ready, Red=reader disabled/denied, Green=access)	Yes	0,1,2,3
8.1	Monitored 6AH UPS integrated in controller	Yes	0,1,2,3
8.1	Controller RTC synchronized with PC on on-line and every hour thereafter	Yes	0,1,2,3
8.1	Earthed steel enclosures with lockable, hinged, monitored lids with covered high voltage	Yes	0,1,2,3
8.1	Filtered, tranzorbed mains supplies	Yes	0,1,2,3
8.1	LAN protected via tranzorbs and resistors, screens earthed per segment	Yes	0,1,2,3
8.1	Terminal, link, switch diagrams and installation booklet per controller. Unpluggable connectors	Yes	0,1,2,3
8.1	Controller diagnostic LEDs	Yes	0,1,2,3
8.1	HW version and electronic ID available at PC	Yes	0,1,2,3
8.1	Time groups (schedules) for I/O, access, reader/PIN enable in controllers, with 30 holidays	Yes	0,1,2,3
8.1	I/O expansion via modules	No	0,1,2,3
8.1	Controller SW and HW (power monitored) watchdog reset circuits	Yes	0,1,2,3
8.1	On-line, off-line, power-up reported to PC	Yes	0,1,2,3
8.2	Supervised inputs with short and open circuit alarms	Yes	0,1,2,3
8.2	Relay outputs, or capable to drive relays	Yes	0,1,2,3
8.2	Configurable inputs (action complete, egress, capture, presence, reader enable, latch, auxiliary)	Yes	0,1,2,3
8.2	Configurable output (capture, latch, auxiliary, booth busy, buzzer)	Yes	0,1,2,3
8.2	Counting inputs in controller	No	0,1,2,3
8.2	Local control of APB, ATB, illegal attempts (reader disabled)	Yes	0,1,2,3
8.2	Mantrap controlled directly by controller with presence, door, latch monitors and busy output	Yes	0,1,2,3
8.2	Readers and egress enabled via local inputs, time groups and from PC	Yes	0,1,2,3
8.2	Local alarms to buzzer	No	0,1,2,3
8.2	Controller hand programmer	Yes	0,1,2,3
8.2	Reader/door modules with PIN pad and LCD (displaying date-time, accumulation, messages)	No	0,1,2,3
8.3	Mimic drivers with accept alarm and lamp test	No	0,1,2,3

12.3 SW

Para	Description	Require	Included
10.1	Windows 2000, XP	Yes	0,1,2,3
10.1	Modular SW with server/client architecture	Yes	0,1,2,3
10.1	MS Access databases accessed via SQL	Yes	0,1,2,3
10.1	Automatic database compression and correction on start-up	Yes	0,1,2,3
10.1	Setting of table names and locations, field names, type, size, indexed, unique	Yes	0,1,2,3
10.1	Database encryption	No	0,1,2,3
10.1	Event driven PC SW	Yes	0,1,2,3
10.1	Virtual objects	Yes	0,1,2,3
10.1	Windows date/time format	Yes	0,1,2,3
10.2	Multiple users in multiple user groups. Passwords and users expire. Auto log-off	Yes	0,1,2,3
10.2	User groups set to view, select, edit data and select items / do control	Yes	0,1,2,3
10.2	Log on via card reader	No	
10.2	Log on via finger print reader	No	
10.2	Application settings per user	No	0,1,2,3
10.3	Language settings per user	No	0,1,2,3
10.4	15 time groups, 8 time zones per function type (access, reader- PIN used, input, output, buzzer)	Yes	0,1,2,3
10.4	Week day, 30 holiday selection per time group for each time zone	Yes	0,1,2,3
10.5	Audit operator changes	Yes	0,1,2,3
10.5	Changes sent automatically appropriate controllers	Yes	0,1,2,3
10.5	List displays configurable to be updated in real time	Yes	0,1,2,3
10.5	Lists referenced to databases	Yes	0,1,2,3
10.5	List columns set to change color according to status, sizable, ordered, column names editable	Yes	0,1,2,3
10.5	List records filtered, sorted by selected column(s)	Yes	0,1,2,3
10.5	Print selected rows in displayed list	Yes	0,1,2,3
10.5	Generation of new lists, grouped in status, card, set-up, vending menus	Yes	0,1,2,3
10.5	Property sheets with data ordered in tabs	Yes	0,1,2,3
10.5	Editing aids – batch load/search, find, copy/paste, delete, add, default	No	0,1,2,3
10.5	Setup wizards	No	0,1,2,3
10.6	Scrolling activity lists with filters. Columns selectable, sizable. Pause, copy, print, restart selections	Yes	0,1,2,3
10.6	Input, output, counter, reader events set for display on time group	No	0,1,2,3
10.7	Events display graphical symbols (bmp/tiff/jpg) flashing when in alarm on drawings	Yes	1,2,3
10.7	Drawings with alarms displayed on top of the desktop	Yes	1,2,3
10.7	Drawings contain editable database items linked to objects	No	1,2,3
10.7	Drawing display photos (bmp/tiff/jpg) linked to readers	No	2,3
10.7	Drawings contain selectable objects that generate events, execute programs (exe, batch, scripts), select other drawings	Yes	1,2,3
10.7	Editable symbol library	Yes	1,2,3
10.7	Integrated drawing WYSIWYG editor, with font, align, space, copy, rotate, order and undo functions	Yes	1,2,3
10.8	Events set to be alarms on active time groups	No	0,1,2,3
10.8	Events set to be logged, displayed, printed, used as triggers. Optionally only on active time groups	Yes	0,1,2,3
10.8	Event generated on time schedules	Yes	0,1,2,3
10.8	Event start applications, generate new events (real or virtual) on algorithm of triggers	No	0,1,2,3
10.8	Algorithms are settings of logical (and, or) events, statuses, time groups and sequenced events	No	0,1,2,3
10.8	Algorithms can use virtual objects, virtual cards used as a card mask (filter)	No	0,1,2,3
10.9	Input, output, reader events running total counts are kept. Reset on events	No	0,1,2,3
10.9	Events increment/decrement / sum / set virtual counters, generating max, min, available count events	No	0,1,2,3
10.10	Timers generate events on time-out. Algorithm of triggers start, stop, reset, load and cycle timers	No	0,1,2,3
10.11	Readers set with in and to area zones, with zone linking for APB	Yes	0,1,2,3
10.11	Card allocated shared, own or multiple area groups. Groups could be disabled, batch loaded	Yes	0,1,2,3
10.11	APB and enforced zone control set per reader, overwritten per card	No	0,1,2,3
10.11	Area groups set to time-out cards in area zones	No	0,1,2,3
10.11	Card statuses settable as disabled, enabled, capture for normal, expired, zone count full, inactive	Yes	0,1,2,3
10.11	Zones added and deleted for expired, zone count full, inactive	No	0,1,2,3
10.11	Overall and period zone counter set per card, with reload and period settings	No	0,1,2,3
10.11	Databases optionally set in reader or only in PC	No	0,1,2,3
10.11	2 card numbers set per holder. Cards linked to master cards, to temporary cards (master disables)	No	0,1,2,3
10.11	Cards linked to control cards (virtual cards)	No	0,1,2,3
10.11	Card masks set for access and serial readers	No	0,1,2,3
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	0,1,2,3
10.11	Cards allocated a trigger group for event/counter trigger filtering	No	0,1,2,3
10.11	Random search set per reader, superseded by card setting. Search disabled, enabled or forced with events	No	2,3
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, citizenship	Yes	0,1,2,3
10.12	Card access data included location and time, card and issue numbers, PIN, random %, pass back, counters and linked to master-, temporary-, visitor- cards	Yes	0,1,2,3

10.12	Card are linked to the groups: time-, area-, capture-, control-, trigger-, host-, group	Yes	0,1,2,3
10.12	Capture groups set where cards set with the group are captured	Yes	0,1,2,3
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	3
10.14.1	Visitor(s) linked to host(s)	No	2,3
10.14.1	Visitor registering system	No	2,3
10.14.1	Identifying visitor using finger print reader	No	
10.14.1	Linking visitor card to card database via card reader	No	2,3
10.14.1	Cards allocated to visitor logged with visitor reference	No	2,3
10.14.1	Visitor photo capture, integrated WYSIWYG label designer, print	No	2,3
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	0,1,2,3
10.15	Outputs set with function type and activation time group	Yes	0,1,2,3
10.16	Vending, POS, cash-loaders, add cash applications, with token, subsidy, value, discount set per item	No	3
10.16	Vending product and service management with low level and time to service alarms	No	3
10.16	Fuel management	No	
10.17	PPOS, pay on exit	No	
10.18.1	Time accumulation	No	1,2,3
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	2,3
10.21	Events open an occurrence log-book	No	2,3
10.22	Events sound audio wave files	No	3
10.23	Events generate SMS messages	No	
10.24	Events generate Email	No	3
10.25	Tele-call control	No	
10.26	Daily log files for events and audit	Yes	0,1,2,3
10.27	Crystal reports generated to display, printer, file. Operator selections or fixed	Yes	0,1,2,3
10.27	Status, events, set-up reports with site name, number of records, sorting sums and totals	Yes	0,1,2,3
10.27	Creation / design of new reports	No	0,1,2,3
10.27	Reports generated automatically	No	0,1,2,3
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	2,3
10.29	Backup via batch files, triggered on events (operator, timed, external)	Yes	0,1,2,3
10.30	Integrated help files and pop-up help	Yes	0,1,2,3
10.31	Access to additional SW functions via encrypted keys	No	0,1,2,3
10.32	Video linking, snapshot. (Video / camera control options available in future versions)	No	
10.33	Control via www options available in future versions	No	
10.34	Guard tour options available in future versions	No	
11.1	Off-line testing of HW	Yes	0,1,2,3
11.2	On-/Off-line SW monitors with filters and simulators with pause, save, clear, go to, speed, literals, parameter settings	Yes	0,1,2,3