Softcon

SOFTWARE CONTROL SERVICES (PTY) LTD

475 King's Highway, Lynnwood
P.O.Box 36675, Menlo Park
Pretoria, South Africa
0102

(t) +27 12 348 7301
(f) +27 12 348 1129
(e) techsupport@softconserv.com
www.softconserv.com

Softcon BMS Specification

Version 2.23

07 February 2017

Revision History

Version	Date	Person	Reason For Changes
2.00	2010-2-20	MTL	Update to new standard document format. Add RF modules, CR375 Remove discontinued DF355/6, CR372 and CR374
2.01	2011-08-20	MTL	Updated computer specs and standard specs (removed UL approved). Added CR390 to and system architecture, removed MUX cards.
2.10	2014-12-12	MTL	Replace controllers with CR391/2 Add mKnock SW
2.20	2015-10-15	MTL JAB	Update CR391/2 specification Update mKnock specification
2.21	2017-01-29	MTL JB	Remove C392 Add CR393, CR394, IO392 Add Universal functions Update SW3, remove mKnock specification
2.22	2017-02-03	MTL	General formatting changes
2.23	2017-02-07	MTL	General formatting

CONTENTS

1 OVERVIEW

The system provides the following building management functions:

- Access control.
- Vehicle control.
- Visitor Control registration.
- Vending control and Cash Load, including Point Of Sale.
- ID Card generation.
- Alarm monitoring and intrusion detection.
- Control of doors, gates, sirens, lighting, etc.
- Time accumulation.
- Link to Time attendance systems.
- Asset management.
- Random check/search.
- ❖ Video – link with external video system.

❖ Continual development - available for certain products, additional on request.

2 REFERENCES

Since 1989, Softcon systems have been installed at more than 15,000 sites in 35 countries, using more than 70,000 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 CR391 controller is CE certified. 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. Numerous functions such as multiple outputs can be controlled locally by controllers, e.g. on card events, booth / mantrap sequence, random check, intrusion, etc.

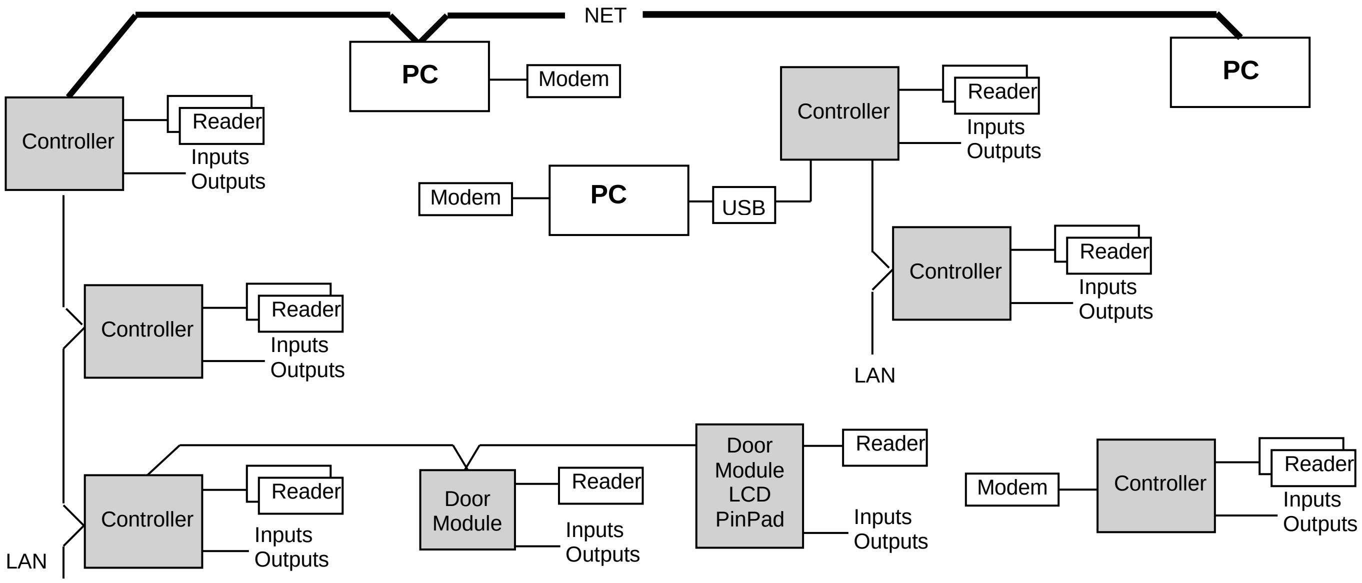
Controllers can simultaneous effect multiple applications such as Access Control, Vending, Intrusion, Programmable Logic Control (PLC), see applications below.

The only non-standalone functions are global functions where multiple controllers effect the same function – e.g. where multiple controllers give access to the same zone, hence affecting counting, time-out, inter-controller anti-pass back (APB) and zone enforcing functions. Controllers contain all relevant set-up and card databases in local battery backed-up memory. Access controllers interface to 1 to multiple card readers directly, or via door control modules, serial readers / locks on RS485 links.

Data between the controllers and PC(s) is transferred via Local Area Network(s) (LAN) or PC networks (NET) and PCs are linked via PC networks (NET). The LAN uses a multi-drop RS485 interface via shielded twisted pair cables. The NET uses TCP protocol via UTP or fibre cables, linked via hubs.

Communication on a LAN is via controllers connected to a master LAN controller that links to the PC via TCP. LAN and NET data packets are encrypted and 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. It is possible to connect up to 127 controllers per LAN and Front-LAN controllers are available, adding I/O and readers to a controller. LAN communication is at 9600 or 19200 baud and data transfer is maximized with off-line controllers only being re-polled at a settable interval, typically 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 up to 10,000 transactions (see controllers below) in battery backed-up memory. Controller's time and day of month stamp all transactions.



Where LAN cables are not available, communication is via GSM modems, dial-up or Access Point Name (APN) on-line. Schedules are set for each PC and for controllers with modems. Alarms at controllers or PCs result in auto connect. When connection is made, the databases are synchronised and events are transferred to the server.

Controllers directly connected to PCs via TCP/IP can also serve as LAN master controllers, transferring data between the PCs and the controllers on the LAN.

Controllers have wireless communication options on-board or external: WiFi, GSM and BlueTooth.
These link controllers to other controllers, PCs and to external systems via internet or SMS.

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 client(s) 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 NET and 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 stored at the client and the server updated when the link is re-established.

In multiple server systems where PCs function independently (with own server programs), systems are synchronized (by a distribution server) 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). 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 thereafter. 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 a password protected menu, not requiring access to the operating system.

6 ACCESS CONTROL CARDS

The cards are passive and, with the exception of MAG cards, are generally permanently factory encoded with numbers & facility codes (cards are available that allow reprogramming of sectors that are used as card numbers).

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 to card / tag readers with the following interfaces:
2-wire Wiegand.
Data/clock.
1-wire Dallas.
Serial – RS485 or RS232 (settable baud rates and bit formats, see serial options below).
Serial RS232 or module GSM / cell modems – Cell caller ID (clip).
Wireless via RF modules.

Via RS485 serial interfaces, additional readers (maximum total of 8 readers) can be connected via expansion controllers / module / serial readers, locks or interfaces. The number of readers are enabled with licencing keys.

Card code structures that can be read are:

- Wiegand – numerous formats of 26, 30, 32, 34, 35 (Corporate 1000), 36, 37, 38, 40, 44 and 52 bit are integrated.
  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 12 hex digits.

On-board or external cell modems give caller ID (CLIP) that is used as card number. The call is not answered, hence no call charge. To prevent inactive-disconnect of the sim-card by service operators, configurable SMS messages are sent on set times.

Biometric Readers (such as finger print, palm, iris, 3d face and vein readers) are interfaced between card readers and controllers, verifying the cardholder – i.e. if print matches the card, the card is passed to the controller. Alternatively, there is no card and the fingerprint is identified and the linked reference is given to the controller, i.e. the fingerprint reader is a reader to the controller.
All fingerprints are stored in the readers (typically up to 100,000, reader dependant). The addition of these readers requires no addition setting to the normal access system. These readers connect via TCP networks to PCs, reading and registering fingerprints. Controllers 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/or 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.

The following lists general information of the Softcon controllers. The physical specifications, number of I/O, readers, buffer sizes, serial options, etc. are listed for each controller below.

8.1.1 ENVIRONMENTAL

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

8.1.2 POWER SUPPLY

Controllers are supplied with 110 or 220VAC (10W, excluding latch and reader power). Optionally, controllers can have an integrated UPS 7 AH, or can be supplied with 12 VDC (700mA, excluding latch and reader power). CR393 controllers are supplied with 12 or up to 35VDC with vending module.

8.1.3 HOUSING

Controllers are contained in white powder coated steel metal housings; with key locked hinged lids (lid opening can be monitored). CR393 controllers can be supplied in aluminium extrusion boxes. Additional cover plates, with appropriate high voltage warnings, protect power supplies. When in metal housings, 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.

8.1.4 COMMUNICATIONS

Communications with controllers is TCP, RS485 (data, /data and RTS, /RTS), RS232 or optionally GSM, Wifi Blue Tooth.
RS485 lines are tranzorb protected and have serial protection resistors.

External fibre optical interfaces (RS485 and TCP) and additional resistor/ capacitor/ inductor/ tranzorb/ surge arrestor interface are available where greater distance and protection is required.
The fibre interface can be mounted in the enclosure and powered by the controller.
The additional protection interfaces are mounted externally.

Certain controllers have on-board wireless modules.
Additional modems and modules can be installed within the housing where required.

Serial ports have configurable baud (up to 38k4), bits (7,8,9) and parity (none, even, odd, high, low, control byte). Depending on the serial interfaces on the PCB, each serial port has a type setting:

SERIAL TYPES	
LAN master	RS485 to sub-controllers
LAN slave	RS485 to master
Front LAN	RS485 to Softcon expanders
PC direct	RS232 slave
Basic	RS232 ASCII, no handshake
Modem	RS232
Test	RS232 – test and diagnostics
Reader	RS232/485 single reader (e.g. barcode)
ControlSoft	RS485 multi-drop readers
Salto	RS485 multi-drop readers / latches
SIA OSDP	RS485 multi-drop readers
Cash loader	Note / coin readers
DEX	RS232 vending machine management
Vending	20mA MDB/EXEC vending machines dispensing
WiFi module	
BlueTooth module	
RF module	
GSM module	

1-wire bus adds relay output expanders and temperature sensors on a multi-drop configuration.

A Software Development Kit (SDK) is available for TCP communication to CR391 and CR393 controllers, facilitating development of systems by uses of these controllers.
Licencing keys enable applications and quantities connected.

8.1.5 CONNECTIONS

Most connections are via un-pluggable, high quality terminals.
Terminal connections, link and switch options are listed within the housing and an installation booklet is provided with each controller.

LAN screens must be earthed per segment and the segment screens must be isolated from one another.

Total LAN cable lengths are limited to 2000m (9k6 baud) or 1000m (19k2) for RS485, 30m for RS232 and 100m for 1-wire bus. RS485 cables must be terminated at the two ends with the characteristic impedance (typically 120 ohm).

Data/clock and Wiegand reader interfaces are tranzorb protected and the maximum cable length is 50m for 12V readers. Reader cables screens, metal housing and mountings must be earthed.
Readers are supplied with 12VDC and can be current limited, preventing security issues then the power is short circuit.
Readers interfaces have 2 or 3 LED control.

8.1.6 FIRMWARE

C programming language is used in Firmware (FW) development where possible, with machine code only used when speed is critical. All FW is structured in to functional libraries, facilitating the re-use and synchronization of functionality, corrections / enhancements / updates, hence products can have same functionality.

FW applications are either specific (e.g. access or vending) or universal (access and vending).
Applications enabled and maximums can be queried and are controlled by keys that can be changed.
See applications below.

The CR39x controllers are updated using programmers or via built in 'Bootloader' programs via the TCP network or RS485 LAN connections.

Controllers have a unique electronic ID (MAC address) and all have FW version information.

These are reported to the PC.

Controllers contain FW and HW (power monitored) watchdog reset circuits.
Controller status changes are reported to the PC, these include on-line and off-line (of the PC communication interface) and power-up (by the controller).

8.1.7 MEMORY / RTC

Set-up and card dB is locally stored in non-volatile memory (EEPROM and / or battery backup memory).
Set-up is locally via Hand programmers, RS232/USB terminals, USB memory sticks or via external linked PC systems.

All set-up, card database and buffered data and real time clock are battery backed up (2 year with the power off). UPS mains power failure can be monitored.

The real time clock is synchronized to the PC RTC when the controller goes on-line and within every hour thereafter.

8.1.8 TIME / COUNT

60 time-groups, each with 8 time zones (start and end time) are available to enable:

- Access - when card may enter.
- Inputs - when monitored.
- Outputs - when automatically active.
- Pin Pad - when must be used.
- Readers - when enabled, when must be used.

Groups are enabled for time zones per day of week and holidays.
30 holidays, the time zones and time groups are stored in the controllers.

The controller has integrated timers and counters, performing functions such as latch times, door open too long, anti-passback. Illegal attempts, event statistics (see controllers below).

Additional timers and counters can be configured to trigger on events - start, stop, pause and generate events when set conditions / counts / timeouts occur.
Counters can increment and decrement.
See controller application PLC functionality below.

8.1.9 INPUTS

Controllers have on-board inputs that are mostly supervised (short circuit, closed, open and open circuit). Each input can be configured as:

- Active level - open or closed (polarity).
- Alarm type - depending in input type, selects the alarm type when input active. See intrusion below.
- Counting input - reporting counted values on request or after pre-set time-outs after change.
- Debounce - time in level before taken as active.
- Enabling input - input only monitored when another input is active, system on/off switch.
- Supervised - enables monitoring of short and open circuit.
- Time group - when monitored.
- Timeout - alarm when input is active longer than set timeout, e.g. open too long.
- Type - enables the input for specific functionality (see input type table below). e.g. door 2 monitor, for the appropriate application selection (see applications below).

The number of inputs can be expanded with multiple serial linked controllers (via RS484 Front LAN) and modules (via 1-wire multi-drop bus). For example, CR394 each with 32 supervised inputs and temperature sensors on 1-wire.

Certain readers can add inputs (e.g. door and latch monitor, tamper, etc.).

INPUT TYPES			
Auxiliary input	Action complete	Check 0%	Intrusion Ena Arm
Battery monitor	APB enable	Check 100%	Intrusion Ena Arm/disarm toggle
Mains monitor	Booth call	Check continue	Intrusion Ena Disarm
Tamper	Booth occupied	Check fail	Intrusion Ena Stay
	Card capture detect	Check pass	Intrusion Ena Stay/disarm toggle
Vend cleaned	Egress,		Intrusion Ena Sleep
Vend do	Reader enable	Level call	Intrusion Ena Sleep/disarm toggle
Vend done	Reader tamper	Level bottom	Intrusion input panic
Vend failed	Latch monitor	Level top	Intrusion input alarm
Vend Filled/cleared	Last card	Level maintain	Intrusion input stay
Vend I/O in	Reset APB	Level now	Intrusion input sleep
Vend serviced	Reset ATB	Level occupied	
	Reset Tg Count	Level alarm	Temperature degrees C
			Temperature alarm Lo
			Temperature alarm Hi

8.1.10 OUTPUTS

Controllers have on-board outputs that are generally relay or open collector outputs.
Each input can be configured as:

- Active level - open, closed, toggle (change over) or pulse (with pulse length).
- Active input - output active when activating input active, e.g. panic button activates siren.
- Active output - output is active when activating output active, e.g. siren switches on light.
- Enabling input - output only controlled when another input is active, e.g. enabling key is switched on.
- Time group on - when automatically active, e.g. gate open 7:00 to 8:00 weekdays.
- Time group lock - when output cannot be controlled.
- Type - selection (see output type table below) enables the output for specific functions for the appropriate application (see applications below).

OUTPUT TYPES			
Buzzer	RD isolate (virtual)	Check-Search	Intrusion Alarm
Off-line	RD LED green		Intrusion Beep/chime
	RD LED red		Intrusion en Arm
Vend Out	RD LED yellow	Level go down	Intrusion en Stay
	Rd out hi / clock	Level go up	Intrusion en Sleep
Count full	Rd out lo / data	Level latch	
Count available	Capture	Level light	Temperature normal
Count empty	Interlock busy	Level now	Temp alarm Lo
	Latch	Level alarm	Temp alarm Hi
			Temp cool down
			Temp heat up

Virtual RD isolate is set by PC commands. The controller does is not allocate the output to a port.

All relay contacts must be protected against fly-back (RC-network for AC loads and diode for DC loads) at the load (externally to the controller).

Multiple outputs can be activated locally by controllers as result of card activity, time setting, event / status algorithms. Card to multiple outputs is effected by the allocation of any of the output groups available in access controllers to cards. Reader-to-output activities are settable per reader, linking reader events to outputs to be controlled.

Outputs can be expanded via multiple expansion controllers (e.g. CR394 with 16 relays) on a RS485 Front LAN and via modules (e.g. IO392 with dual relay) on a multi-drop 1-wire.
Certain readers can add outputs (e.g. latch, LEDs, etc.).

8.1.11 APPLICATIONS

The controller can have one or more of the following applications installed and activated as required.

Changes within applications (e.g. enable changes, state changes) can be set to report:

- SMS - Controller, application names, name of resourced changed (door, temperature, reader, alarm enable) and state (illegal open, low alarm, out-are, armed) is sent with date time.
- Apps - all relevant data as required by all linked Apps.

APPLICATION - ACCESS CONTROL

The controller functions in a stand-alone mode with a local card database of up to 130,000 randomly numbered cards, with PIN. Searching for a random card at location 130,000 is typically within 150msec.

All access functions are controlled locally, and access granted, denied, card captured, card not captured, door not opened, etc. are reported to the PC.

Integrated local access functions are:

- Cards are enabled for readers, allocated a time group (when enabled), capture, APB and ATB override.
- Anti-pass back (APB) is controlled locally between readers (access denied if requesting access to the same area zone). Settings are for locally disable reader(s) / enable other or disable all. APB reset enables all cards for all readers if enabled for any or regardless of current enable.
- Anti-time back (ATB) function are controlled locally between the readers (access denied for timeout to the same area zone) – with time settings for each reader and selection of clearing other readers ATB for the current card.
- Multi-badge can be set per reader (2 to 9), access only after set number of enabled cards are badged within timeout period. If a not enable card is badged or timeout occurs, all cards in multi-badged queue are cleared. When successful number have badged, access is granted and all cards in the badged queue are reported as entered, queue is cleared.
- When access is granted, latch outputs are activated according to the output setting.
- Inputs configured as access inputs (see column 2 in input type table) are monitored for the appropriate function - with timeouts (open too long), time groups (when monitored), enabling inputs, etc.
- Mantrap controls 2 doors, monitoring door, latch and occupied statuses and timeouts.
- Interlock setting prevents other doors to the same area zone opening.
- 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.
- Readers can be disabled, door can be permanently locked / unlocked on command from the PC, on linked inputs or on time groups.

Reader events generated (with card number) are:

- Captured.
- Duress.
- Entered.
- Reversed (to and from areas swapped).
- Last card – triggered by input (e.g. breathalyser pass and fail).
- Not captured.
- Not opened.
- Out-of-area (not found or disabled).
- Out-of-time (enable, but time group does not allow access).
- Wrong facility (site and client code does not match).
- Wrong format (wrong number of bits or checksum error).
- Wrong PIN.

Door event generated are:

- Illegal open.
- Opened too long.

Up to 4 random check / search functions can be configured per controller:

- % check is set for each search and can be overwritten by card settings.
- Overriding inputs for 0% (check disabled) and 100% (check all) can be configured.
- Inputs can be configured to link to external sensors (e.g. breathalysers) to trigger pass and fail. Outputs controls search indications, enable external devices, open alternative doors when the check fails.

Multi-output control (typically lift control, alarm activation) functions as follows:

- Output groups are allocated functions.
- A function is a reader number of the controller, the output controlled and a time group when the output can be controlled (e.g. reader 2 actives output 2, 3 and 5).
- Outputs are controlled as per the output set-up (e.g. pulse for 5 seconds).
- Cards are allocated an output group (e.g. group 2 at reader 3 activates outputs 1,4 ,5).

APPLICATION - BOOT LOADER

Updates FW in controllers on slave LAN. FW data is received from the PC on a UDP link and passed to a controller on the LAN. Responses from controller being updated is passed to the PC.

APPLICATION - CASH LOADER

The controller connects to note / coin acceptors is via serial interfaces.
Money deposited is reported to the PC with the access card number.
Appropriate messages are displayed on a LCD (e.g. R100 added).
Messages from the PC (e.g. updated cash total) are displayed.
Cash draw and housing are monitored for tamper.
Auto cash-up report is sent to PC when cash drawer is opened legally.

APPLICATION - INTRUSION

By defining input and output types for intrusion (see input / output above), alarm (intrusion) system functions are controlled.
Via inputs, external commands (via any of the communication links, e.g. Blue Tooth) or by LCD / keypad selection, the intrusion application is set to one of the following enabled states:

- Disarmed - system off (except panic inputs).
- Armed - all inputs monitored.
- Stay - non- stay and sleep inputs monitored.
- Sleep - all non-sleep inputs monitored.

Input(s) can be configured to enable the intrusion system state (as defined above):

- Arm
- Disarm
- Toggle arm/dis - switch between arm / disarm.
- Stay
- Toggle stay/dis - switch between stay / disarm
- Sleep
- Toggle sleep/stay - switch between sleep / disarm.

Output(s) can be set to show the enabled status of the intrusion:

- En-arm - Armed.
- En-stay - Enabled for stay.
- En-sleep - Enabled for sleep.

Sensors (passives, beams, panic buttons, door sensors) are connected to inputs, enabled as follows:

- Panic - always generate alarm.
- Alarm - when system is enabled for arm, stay or sleep.
- Stay - not enabled when stay or sleep.
- Sleep - not enabled when sleep.

The input timeout setting can be set for exit delay and denounce setting for entry delay.
The input Tg settings can set when the input is monitored (e.g. outside beams not monitored on Wednesdays 8:00 to 12:00 when garden is serviced).

As result of the input current status (active or not) and the input's alarm type configuration, intrusion system can be in the following alarm state(s):

- Alarm
- Buzz
- Chime
- Silent
- None

Outputs can be set to be active for the current alarm state:

- Alarm - See input alarm state setting below.
- Buzz - See input alarm state setting below.
- Chime - Will always chime, regardless of enable. See alarm setting.

To activate the alarm state of the system, the alarm type for each intrusion input is configured to one of the following:

- Alarm - alarm always (e.g. panic inputs).
- Buzz - buzz if system armed.
- Alarm, buzz - alarm when armed, buzz when stay/sleep.
- Chime - chime always.
- Alarm, chime - alarm when armed, always chime.
- Buzz, chime - buzz when armed, always chime.
- Alarm, buzz, chime - alarm when armed, buzz when stay/sleep, chime always.
- Silent - no output.

APPLICATION - LEVEL / LIFT
By defining input and output types for level (see input / output above), lift control functions are performed (lift up or down to levels).

Inputs are:

- Level call - for each level, lift goes to level when all doors closed and lift not in use.
- Level door - for each level, door status.
- Bottom - lift at bottom level alarm.
- Top - lift at top level alarm.
- Maintenance - doors are unlocked.
- Now - for each level, lift at level.
- Occupied - lift occupied (beam, pressure or motion detector).
- Alarm - panic / error input

Outputs are:

- Level latch - for each level, door unlocked if lift at that level.
- Level now - for each level, where lift is (connect to indication lamp).
- Up - activate motor up till required level reached.
- Down - activate motor down till required level reached.
- Light - on when door open, moving, occupied, till timeout.
- Alarm - error condition, alarm input. Cleared when any door opened.

APPLICATION - PLC
Numerous Programmable Logic Control (PLC) type functions are integrated by setting input and output types (e.g. Lift control, intrusion, temperature, output groups, activate output on activating output).

Other event can be triggered when events occur and other resources are in certain statuses (set algorithm of statuses the must be true).
These trigger and resulting events and resource statuses include inputs, outputs, counters, timers, time groups and reader events. For example, door opens (the trigger) and after hours, and no one is on the premises (occupancy counter – counts up on enters and down on exit, is zero) and alarm is enabled, activate alarm output.

APPLICATION - TEMPERATURE
Inputs are defined as temperature sensors, each with a required, minimum and maximum values (degrees C or F).
Additional inputs can be set as high and low alarms and as temperature normal.

The following outputs can be linked to the temperature input:

- Temp up - when temp too low and active when output’s Tg is active.
- Temp down - when temp too high and active when output’s Tg is active.
- High alarm - when temp exceeds maximum set value or when high level alarm input active.
- Low alarm - when temp below minimum set value or when low level alarm input active.
- Normal - when temp between min and max no high or low alarm input active.

APPLICATION - VENDING CONTROL

The controller functions in a stand-alone or in PC controlled mode.

When a card is badged, the available funds are displayed from local dB in stand-alone mode or by the PC in PC mode. This enables the vending machine, allowing a selection to be made.
Dispensing is done when the controller is in “Free Vend” mode, the item is free or if sufficient funds (or tokens) are available for the card holder for the selected item (from local or PC dB).

On successful fend, the remaining funds are updated.

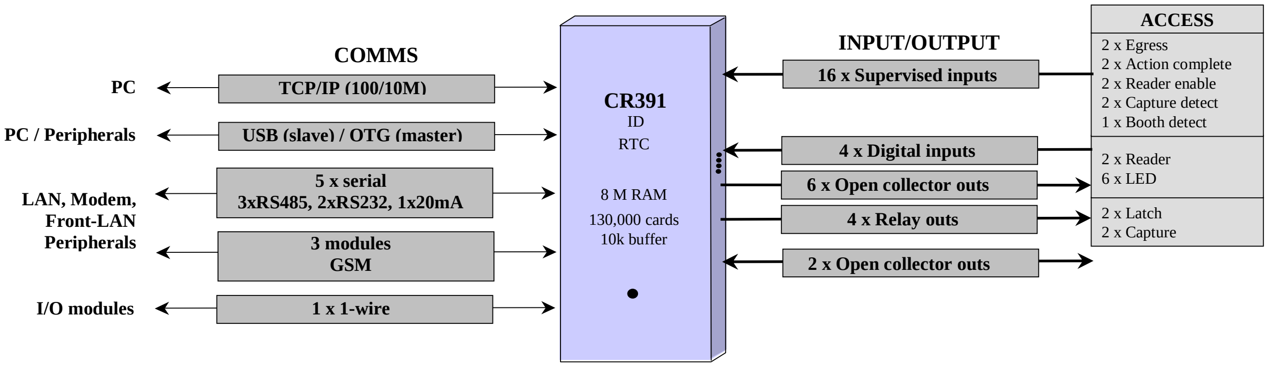
Vending interface is either:

- Serially EXEC / MDB with vending machines.
- Selection is via keypad.
- Access reader badging (e.g. reader 1 is item 1, reader 2 is item 2).
- I/O vend by selection of inputs linked to outputs (input to output control, e.g. soda fountains).

8.1.12 DIAGNOSTICS

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. Ticking twice a second indicates communication with sub-LAN controllers. 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. 2 on-board LEDs indicate TX and RX on a selectable serial port. Additional on-board LEDs indicate selectable diagnostics.

8.2 CR391 UNIVERSAL CONTROLLER



8.2.1 COMMS

Five serial ports are available and linked to the following interfaces are required:

- 3 x RS485.
- 2x RS232.
- 1 x 20mA interface - source or slave.
- 2 x expansion modules.

The serial type, rates and bit structure are set for any port.

The 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).

Communication to extender modules in via a 1-wire bus.

Communication with the PC is via RS485 (multi-drop), RS232 (modem), GSM module, optical fibre interface (additional via TCP/RS485 to fibre), TCP/IP (10/100MHz) or USB.

The CR391 can also serve as a LAN controller, interfacing controllers via RS485 multi-drop to the PC.

8.2.2 INPUTS / OUTPUTS

All Input and output functions described above can be implemented (see inputs and outputs above).

- 16 supervised input ports with tranzorb protection (short and open circuit, contact open or closed).
- 4 tranzorb protected digital input ports (2 x readers).
- 12 output ports (4 relays, 2 normally open, 2 normally closed, with 28VDC/250VAC, 3A rating.
- 8 open collector Darlington with 500mA/50VDC rating)
- I/O expansion is via up to 8 * CR394 (each with 32 supervised inputs and 16 relays).
- Additional remote I/O can be expanded to 8 * IO392 modules and 8 * temperature sensors via a multi-drop 1-wire bus. Inputs are limited to 300 and outputs to 150.
- Capture units can be set at any readers.

8.2.3 READERS / CARDS / DB

- Up to two reader port can be set on-board (tranzorb protected) ports (Wiegand, Data/clock, touch).
- Readers each with 3 LED control.
- 130,000 card database in battery backup SRAM.
- RS232 / RS485 serial readers can be added via the peripheral serial ports.
- Up to 8 readers can be connected (on-board, serial and/or via external controllers / interfaces / modules, e.g. CR375).
- 64 Output groups with 128 output functions.
- Data buffering is 10,000 transactions.
- Data in the controller can be viewed and edited with a CR375 hand programmer that is connected via a FLAN or via RS232 terminal.

8.2.4 TIMERS / COUNTERS

- 16 inputs can be counting inputs, reporting counts after a set timeout.
- Card event statistic counters are integrated.
- 8 additional counters and 8 additional timers are available for PLC.

8.2.5 APPLICATIONS

The controller functionality is multipurpose, and is configurable for one or more of the applications listed above.

System SW keys can also be stored in the controller non-volatile memory, with the PC setting and retrieving the keys when required.

8.2.6 DIAGNOSTICS / TEST

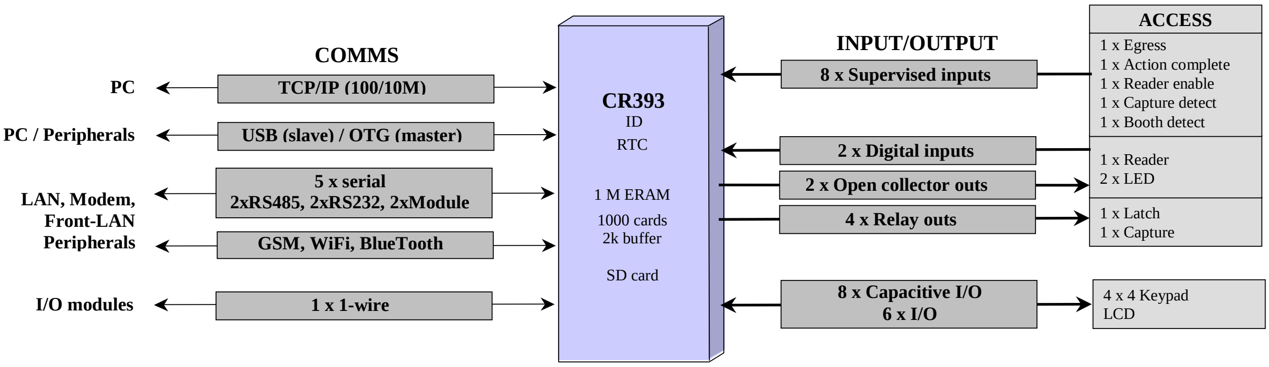
Test modes are available to simulate multi-slave nodes and to generate multi-events.

- Communication monitor, test and statistic options can be set and configured.
- 4 LEDs, visible outside the house indicate running, communication and reader activity.
- 4 additional on-board LEDs are configured to show peripheral and other activities.
- Built in Transaction statistics can be reported to and set by the PC, typically the following info:

Communication:	On/off line, In/out/clear of transaction buffer.
Access:	Entered, Reversed, Duress, Out-time, Out-area, Wrong PIN, Not-opened, Format-, Facility-, Pin-error.

- Built In Test (BITE) via a Terminal (e.g. HyperTerminal) runs tests on all I/O, readers, peripherals, memories.

8.3 CR393 (IOT CONTROLLER)



The CR393 Internet Of Things (IOT) controller has a variety of on-board interfaces, peripherals and communication options, providing numerous applications for monitor and control – locally and remotely.

8.3.1 COMMS

Five serial ports are available and linked to the following interfaces are required:

- 2 x RS485.
- 2x RS232.
- WiFi on-board module.
- GSM on-board module.
- sBlueTooth on-board module.
- 2 x expansion modules.
- 20mA module with 35VDC power supply can be mounted as a piggy back (used in vending applications).
- A second module can link to an external power-line communication interface.

The serial type, rates and bit structure are set for any port.

The 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).

Communication to extender modules in via a 1-wire bus.
Communication with the PC is via RS485 (multi-drop), RS232 (modem), GSM / WiFi modules, optical fibre interface (on-board module), TCP/IP (10/100MHz) or USB. The CR393 can also serve as a LAN controller, interfacing controllers via RS485 multi-drop to the PC.

8.3.2 INPUT / OUTPUT

All Input and output functions described above can be implemented (see inputs and outputs above).

- 8 supervised input ports with tranzorb protection (short and open circuit, contact open or closed).
- 2 tranzorb protected digital input ports.
- 6 output ports (4 relays, normally open, with 28VDC/250VAC, 3A rating).
- 2 open collector Darlington with 500mA/50VDC rating).
- 12 I/O lines can connect directly to a 4x4 touch keypad and an LCD.
- I/O expansion is via up to 4 * CR394 (each with 32 supervised inputs and 16 relays).
- Additional remote I/O can be expanded to 4 * IO392 modules and 4 * temperature sensors via a multi-drop 1-wire bus. Inputs are limited to 200 and outputs to 100.
- Capture units can be set at any readers.

8.3.3 READERS / CARDS / DB

- 1 reader port can be set on-board (tranzorb protected) ports (Wiegand, Data/clock, touch).
- Readers each with 2 LED control.
- 3000 card database in EERAM.
- RS232 / RS485 serial readers can be added via the peripheral serial ports.

- Up to 4 readers can be connected (on-board, serial and/or via external controllers / interfaces / modules, e.g. CR375).
- 32 Output groups with 64 output functions.
- Data buffering is 2,000 transactions.
- An SD card can be added on-board for memory expansion.
- Data in the controller can be viewed and edited with a CR375 hand programmer that is connected via a FLAN or via RS232 terminal.

8.3.4 TIMERS / COUNTERS

- 16 inputs can be counting inputs, reporting counts after a set timeout.
- Card event statistic counters are integrated.
- 8 additional counters and 8 additional timers are available for PLC.

8.3.5 APPLICATIONS

The controller functionality is multipurpose, and is configurable for one or more of the applications listed above.

System SW keys can also be stored in the controller non-volatile memory, with the PC setting and retrieving the keys when required.

8.3.6 DIAGNOSTICS / TEST

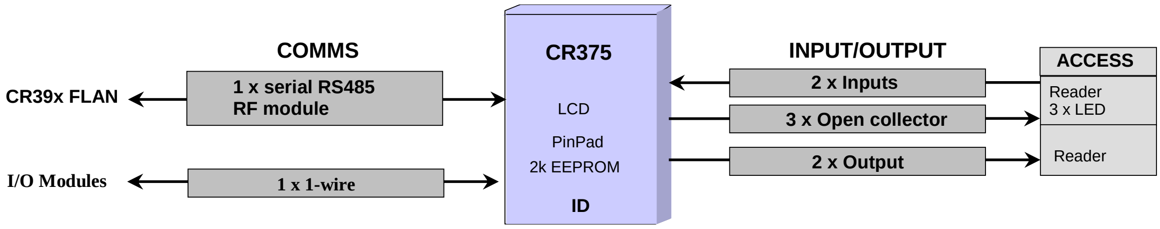
Test modes are available to simulate multi-slave nodes and to generate multi-events.

- Communication monitor, test and statistic options can be set and configured.
- 6 Diagnostic LEDs, visible outside the house, indicate running, communication, reader and other activities.
- Built in Transaction statistics can be reported to and set by the PC, typically the following info:

Communication:	On/off line, In/out/clear of transaction buffer.
Access:	Entered, Reversed, Duress, Out-time, Out-area, Wrong PIN, Not-opened, Format-, Facility-, Pin-error.

- Built In Test (BITE) via a Terminal (e.g. HyperTerminal) runs tests on all I/O, readers, peripherals, memories.

8.4 CR375 (DOOR CONTROLLER WITH PIN PAD AND LCD)



The CR375 controller is a front-end door controller for the CR39x controller with:

LCD	- 2 line, 16 or 20 character, directly to the PCB.
Pin Pad	- 3x4 or 4x4, directly to the PCB.
Reader	- Wiegand or data/clock
2 x inputs	
5 outputs	- 4 open collector Darlington with 500mA/50VDC rating, 1 TTL.
I/O expanded	- to via multi-drop 1-wire interfaces.

Input and reader data is read and changes passed to the CR39x. The CR39x controls the outputs.

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.

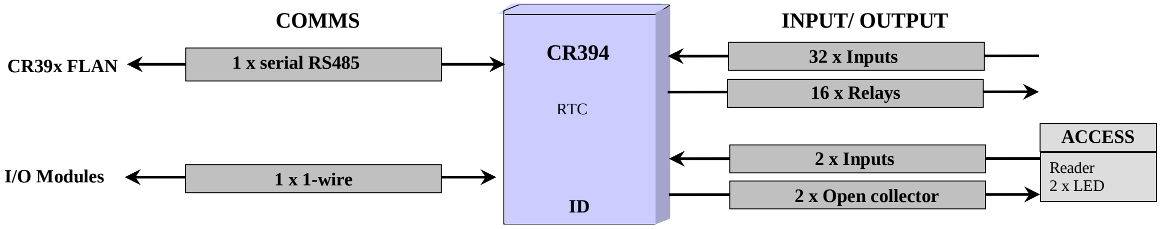
The CR39x controller displays the real time and the access status (e.g. “denied” or “proceed”). The PC can display additional data such as the cardholders name, available subsidy, accumulation time, messages, etc.

Communication between a CR375 and a CR39x is via a multi-drop RS485 FLAN cable with a maximum of 8 CR375 connected to the cable. FLAN shared with CR394s.

A 2k EEPROM is incorporated on the PCB in specialized stand-alone applications.

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

8.5 CR394 (I/O EXPANDER, READER)



The CR394 controller is a front-end expander controller for the CR39x:

- Reader via 2 input ports, 2 LED outputs (Wiegand, data/clock).
- 32 supervised inputs.
- 16 relay outputs (normally open with 28VDC/250VAC, 3A rating).
- I/O can be expanded to via multi-drop 1-wire bus interface.

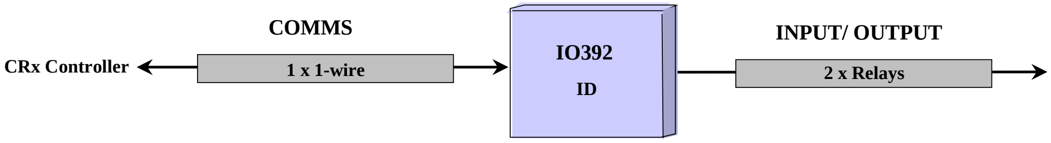
Input and reader data is read and changes passed to the CR39x. The CR39x controls the outputs.

Communication between a CR394 and a CR39x is via a multi-drop RS485 FLAN cable with a maximum of 16 CR394 connected to the cable. FLAN shared with CR375s.

A 2k EEPROM is incorporated on the PCB in specialized stand-alone applications.

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

8.6 IO392 (1-WIRE I/O EXPANDER)



Multiple IO392 modules communicate on a 1-wire bus with CR39x controllers. The CR39x controls 2 relays (change over with 28VDC/250VAC, 3A). On-board LEDs show the relay status.
The CR39x can also read temperature sensors connected to the 1-wire bus.

9 COMPUTER SPECIFICATIONS

HW Requirements:
- I3 2.3GHz
- 2 Gig Memory
- 250 Gig HDD Space
- CDROM
- TCP/IP
- 1024 X 768 resolution Screen

Software Requirements:
- Windows 7 32/64 Bit Professional
- Windows 8.1 Professional
- Windows 10 Professional
- Windows Server 2008
- Windows Server 2012

Database:
- SQL Server 2008
- SQL Server 2008 Express
- SQL Server 2012
- SQL Server 2014

10 SOFTWARE

10.1 GENERAL

The PC SW has been developed by Softcon in South Africa using Visual C++ 2015 and incorporates COM object modules. The development platform is Microsoft Windows 8.1.

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 (a service) 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 (see list above), with authentication or not).

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.
Point of sale (POS) can be incorporated in the system 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 OPERATOR INTERFACE

10.2.1 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.

10.2.2 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.

10.2.3 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 can be:

- invisible, displayed and editable according to the logged on user.
- selectively set to be updated in real-time.
- data referenced to other databases are displayed and selections made via list (details below) 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).

DISPLAY 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). Holding the mouse pointer on a column heading display a pop-up with a short description (these descriptions can be changed in configuration data bases).

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. A pop-up displays a short message by holding the mouse pointer on a description (pop-up are editable in configuration data bases).

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 some search criteria (what must match) and load data (what is overwritten).

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

DATA READ / SCAN. Serial or USB card / finger / barcode / scanners and 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.

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

10.2.4 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.

10.2.5 GRAPHICAL DISPLAYS

Pixel based animated graphical drawings with symbols (icons) linked to each status of inputs, outputs, readers, etc., indicate the status of all monitored and controlled objects in the system as follows:

- When objects (input, reader, etc.) change status, a different icon (e.g. door open).
- If in alarm, the icon flashes in inverse video until accepted (by clicking on the flashing symbol).
- An accept alarm event can be generated (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 (icons) 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.

10.2.6 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.

10.2.7 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.

10.2.8 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.

10.2.9 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.

10.3 EVENTS

The “real time” functioning of the system is event driven, resulting in very flexible and configurable systems.
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 grouped into a variety of objects (resources) that are available in the system, namely:

- Base products - vending product remaining, calculated from recipe set per vend item.
- Controllers - reset, on-, off-line.
- Counters - start and stop events, count up / down, event generated when full, empty.
- Event buttons - generates event when button on drawing selected.
- EXE buttons - runs .exe when button on drawing selected.
- Inputs - see inputs below.
- Outputs - see outputs below
- Readers - see readers below.
- System - log-on /off.
- Timers - starts, stop, pause and continue events, event generated when timeout.
- Vend items - item per vender, prices, discounts.
- Venders - product dispensed.

Objects could be virtual objects (memory based) or allocated to hardware and the status of these are set / reset / incremented / decremented, etc. via other events.

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.
- Start, pause or stop timers.
- Trigger new events.
- Start programs (on set PCs), batch files or run scripts (with set parameters).
- Set / reset the status of objects.
- Change card properties– status (en- / disable / capture), area group and time group.
  Changes are automatically sent to controllers and the changes are audited.
- Start audio files.
- Open and change graphical indications, photos (bmp/tiff/jpg), database items on display.
- Open messages to the operator must accept.
- Open formatted activity logs that the operator must fill in.
- Send SMSs.
- Send emails.
- Send data to external systems (e.g. vending, video, parking).

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.

All access control functions generate events or are as a result of events (see Access events below).
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.
The controllers report reader and I/O changes on active time groups.

10.4 OBJECTS / RESOURCES

The system, applications and event have the following resources that can be used:

10.4.1 COUNTERS

Integrated 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 new event:

- Count minimum (the new count is equal or below a set minimum).
- Count maximum (the new count is equal or above a set maximum).
- 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 counting inputs, 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.

10.4.2 READERS

Readers linked to controllers are set as per the options listed under the reader section above.
Each reader is allocated to ports on a controller.

Readers connected directly to the PC enters the card number to cursor (editing, searching). Card masks are set each 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).

10.4.3 SCHEDULES (TIME ZONES AND GROUPS)

Time related functions (e.g. when access is granted) are set via time groups.
There are 60 groups each with 8 time zones (start and end time).

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.

10.4.4 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.
- Continue with current value.

Timers can be pre-set to cycle, reloading the pre-set value and continuing on time-out.

10.4.5 INPUT / OUTPUT

Every input, output and level is set with a name and allocated to an appropriate port on a controller.
All setting as listed for I/O in the controller section is set and sent to the controller.
I/Os are set for active time group for each detection level.

Each input is set with an alarm time group (when the level change is an alarm) and activity on level change (log, display, trigger other events, print).

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 output can be set to be controlled automatically.
Multiple output control on card read is as listed in Multi-output control above.

10.4.6 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.

10.4.7 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.

10.5 CARD HOLDERS (PROFILES)

The number of cards in the system is configurable.

Cards are used by various applications (e.g. by access and vending).

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 dependent) is listed below. Editing aids and batch loading is as described in the editing section.

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).

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 nor content, 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 (used by all applications using cards). See additional setting for access control.

- **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.
- S**tatus** (disabled, enabled or capture) is set for normal operation, when expired and when the cards counts are not available.
- S**tart/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 start/expire, the alternative status is used and add/delete area groups are checked.
- **Absent** (on leave) start and end date-time with area zones added / deleted and an absent status when within absent period.
- C**apture group** sets where the card is captured.
- **Time Group**. Defines when a card may be granted access.
  One of 60 time groups are selectable (each with 8 time zones), e.g. “Time group 1 - managers” with 24 hr access.
  Selecting time group 0 sets that the time groups set per area zone in the cards area group is used.
- **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.

- **Number**. Two card numbers can be set for a card (e.g. prox and MAG 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).
  Using master card link (see below), a card holder could have multiple cards.
- **Pin code**. 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.
- **Pass back**. 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).

Card dB linking
A card can be linked to another 3 cards in the Db.

- **Linked to**. 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.
- 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.
  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).
- A **master card** links the cards 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.
  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.

Trigger Group. Selects a group that is added to the cards events and is used to trigger events and/or counters.

Accumulation. Day, week and month totals since the last day-, week- and month-end, 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.

Counters. 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.

Previous. 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.

Visitor ref. 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.

Licence. 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 license expires, access is denied to certain areas).

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.

10.6 APPLICATIONS

The system has the following applications available. Details for each are given below:

- Access control.
- Asset management.
- Bootloader – updates FW in controllers.
- Cash Add. Incorporated in the Client program or available as a separate exe client program.
- Card Access – zone display.
- Card maker.
- Converters.
  Adding or removing areas / zones.
  dB cleanup.
- Data distribution. Synchronize data bases, log, photos on distributed systems.
- External links.
  Adding or deleting card data (importing) via files.
  Log of clock in/out data for external T&A systems.
  On-line exchange of data to external systems.
- Parking point of sale (PPOS).
- Point of sale (POS).
- Time accumulation.
- Vending applications such as canteen and vehicle park entry control, cashless vending, Photostat-, Laundromat-, Car wash control, cash loaders, etc.
- Visitor control.

10.6.1 ACCESS CONTROL

Card setting for access control are listed for the card data – access.
Card settings are integrated with the following:

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”.
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.

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.

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.

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 with up to 130,000 cards (see controllers above) in controller memory (facility and card number), 12 character (HEX) random number.
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

ACCESS EVENTS are generated for specific access activities and by the controller and expanded to (e.g. controller out of area could be not found, expired, out of area).
In the order, events are:

- 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.
- Enabled.
- Entered.
- Duress.
- Captured.
- Not opened.
- Opened too long.

DUAL (multi) BADGING function is settable per reader – linking a reader to another (or to itself), requiring the badging of multiple cards that have access within a settable time period to gain access.

RANDOM CHECK (e.g. alcohol, drug, search search) function is triggered automatically when cards enter via readers set for random search. Up to 4 random checks can be set per reader.
A check % 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 locally in the controller or via the operator clicking on drawings) to disable or enable random check 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 check can optionally be via PC control or function within the controller.

MULTI-OUTPUT CONTROL. 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-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.
Each output group is allocated function(s).
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).
See controller – multi-output for activity.

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.

10.6.2 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 returened 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:

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).

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

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 recoded.

10.6.3 BOOTLOADER

Controllers are updated with the latest or specific FW.

Schedules are set for when specific controllers are updated, with selected hex file.
TCP linked controllers are updated directly and controllers on RS485 LANs are updated via the LAN master.

A command is sent to the SCS_CLIENT program that is linked to the controller being updated, sending the controller into its bootloader. TCP controllers or the LAN master (when updating a LAN controller), opens a UDP link to the PC bootloader application to transfer the FW. On completion, the controller resets and SCS_CLIENT is set to send set-u data to the controller.

10.6.4 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.

10.6.5 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.

10.6.6 PARKING

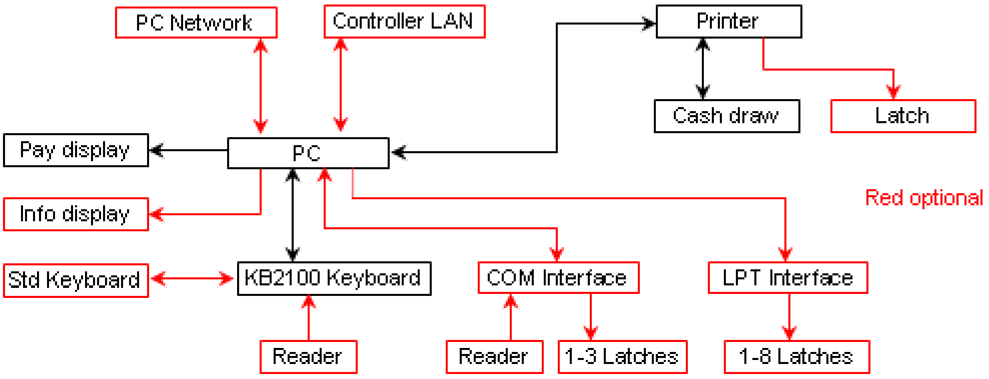
PAY ON EXIT – ACCESS SYSTEM

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).

COUNTING SYSTEM

The access control system can be set (using events) 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).

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.

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.

10.6.7 POINT OF SALE

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.

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.

10.6.8 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 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.

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 contain 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.

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
```

Format for the following T&A systems are integrated, more can be added on request:

- Access 2000
- Clock watch.
- Eco Time Tech.
- Eds,
- Lavies.
- Sap.
- Sap standard.
- Sentri.
- Softcon.
- Super Time.

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.

10.6.9 VENDING

The vending option controls vending machines and Photostat machines 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 (Executive and MDB 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.

10.6.10 VISITOR CONTROL

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

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.
>
> ***Fingerprint.*** 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.

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.

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.

10.7 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.

10.8 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.

10.9 INTERFACING TO HOST PROGRAMS

10.9.1 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. Details are given in the external link document.

Clock in and out events 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 (see T&A above).

10.9.2 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 were 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 or 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.

dB clean. A dB clean-up program can be used to remove unused area zone, area groups and unused cards.

10.10 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).

10.11 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 LAN controller 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
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). Exculdes 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 hardware (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.

10.1 VIDEO LINKING, *VIDEO /CAMERA CONTROL

Linking to external video systems is via TCP or serial links using the external link interface.

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.

10.2 *CONTROL VIA WWW

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.
- Comms messages monitor – shows data to and from the comms interfaces, i.e. data sent and received from the NET and LAN.
- Comms out simulator – sends data to the comms interfaces (no events are generated).
- Comms in simulator – send data to the system as if it was received from the comms 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 comms interfaces 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.