Softcon BMS Specification

Revision 2.34

01 September 2023

Revision History

Version	Date	Person	Reason For Changes
2.00	2010-02-20	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 CntrP 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
2.24	2017-09-30	MTL	General formatting Add Denis, biometric readers list, SDK, diagnostic modules
2.25	2017-10-13	MTL	Swap order of output Tg/linked I/O
2.26	2018-07-39	MTL	Add PoPI Act info to standard specification
2.27	2019-01-22	MTL	Remove CR393, CR375. Add CR395, SCS_Wizard, SCS_Controller, Scanner and number plate readers. Add device linked to token and device data event. Alter - 128 time groups with 32 time slots
2.28	2019-04-23	MTL	Expand on CR394, CR395 Add MO310 Add Visitor options
2.30	2020-01-20	MTL	Expand on CR395, remove COM363 Expand on Visitor options, barcode Detail on biometric readers
2.31	2020-09-25	MTL	Include ABC, Breathalysers Update ATB, Biometric Alter document to use terms of IEC60839 (see appendix: Terms and definitions) Cards/Tag now Tokens. Card holders now Users. Operators has access to PCs Door now Portal. Egress now REX. Action Complete now Portal Sense. Latch now Lock. Time zones now Time slots. LAN now SLAN. Reorganize document sections. Indicate option not available Add Block List
2.32	2021-09-03	MTL	Add Windows Server 2019 (run as administrator)
2.32a	2021-10-05	MTL	Add legacy / Universal Additional resources to CR391
2.33	2022-03-15	MTL	Add Windows 11 Add SOC 2 non-certification
2.34	2023-09-01	MTL	Add HikVision

CONTENTS

1 OVERVIEW

In this specification, the ❖ icon indicates that development is in progress and that all functions may not be available – please confirm completion status with Softcon.
This document is subject to alteration – final implementation may differ (please confirm requirement with Softcon).

The system provides the following building management functions:

- Access, Visitor and Vehicle control.
  - Card (token, ID) generation.
  - Asset management.
  - Random check/search.
  - Time accumulation.
  - Link to Time attendance systems.

- Vending control and Cash Load, including Point Of Sale.
- Input monitoring (status / alarm / intrusion detection)
- Control of portals, sirens, lighting, etc.
- Video – link with external video systems, directly link events to TCP cameras (snapshot, live).

2 REFERENCES

Since 1989, Softcon systems have been installed at more than 6,000 sites in 35 countries, using more than 80,000 control panels (CntrP) and have been proven to be stable and reliable. Contactable references are available.

The latest version of this document is available on www.softconserv.com.
The video Softcon BMSS Specifications, available on YouTube (search for Softcon BMSS and find the Softcon YouTube directory of Softcon videos – find the logo on the left) is a short presentation of this document.

3 OWNERSHIP / GUARANTEES

All Hardware (HW) designs and circuit diagrams, Firmware (FW) and Software (SW) code is the property of Softcon and are not provided. These 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 because of product errors or failures.
Softcon does endeavor 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

STANDARDS
The CR391 CntrP is CE certified. The tests are available on www.softconserv.com.
All warning notifications, dielectric tests (alternating current potential of 1200V is passed through the transformer for 1 second) and radiation requirements are adhered to.

DataBase security / PoPi ACT / SOC 2
The SQL databases are password protected (MSAccess no passwords).
Operators of the systems have password logons that allow viewing and editing of selected setup and personal data according to the password rights allocated by system administrators.

All Operator passwords can be altered by the system administrators, as and when required.
Operator passwords can be set to auto expire.
Passwords and operator access to data are encrypted.

All user personal information resides in system data bases on the server PC.
No personal information is transferred to control panels.

Access to the PCs is not controlled or limited by the Softcon systems and if required, this by be added by the system administrators.

Softcon products are not certified or audited for compliance to the American SOC 2 standards.
Security of access to data in Softcon systems is as given in this section.
Additional security to Softcon systems must be implemented externally.

5 APPLICATIONS

The system can be configured to execute multiple applications.
Certain App are PC based, done within control panels or in both.
Apps can be subsets of the main App (described in the sections below) and Apps can share and interlink resources.

Apps are:

- Access Control, includes:
  - Asset management
  - Card (Token) maker
  - Time accumulation
  - User Access – zone display
  - Visitor Management

- Bootloader – updates FW in CntrP.

- Data Apps include
  - Bootloader – updates FW in CntrP
  - Converters
    Adding or removing areas / zones
    dB cleanup.
  - Email and SMS (on event, on report).
  - External links.
    Adding or deleting users (importing) via files.
    Log of clock in/out data for external T&A systems.
    On-line exchange of data to external systems.
  - Reports

- Input / Output Apps include
  - Elevator management
  - Intrusion
  - Programmable Logic Control
  - Temperature management

- Operator interface (edit, status)
  - Drawing

- Vending, includes:
  - Cass Add
  - Point of Sale (POS)
  - Parking POS (PPOS)

6 SYSTEM ARCHITECTURE

Intelligent field control panels (CntrP) perform all functions in a stand-alone mode. CntrP 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 CntrPs, e.g. on token events, booth / mantrap sequence, random check, intrusion, etc.

CntrP can simultaneously effect multiple applications (App), such as Access Control, Vending, Intrusion, Programmable Logic Control (PLC), see applications below.
Multiple of the same App can be active (e.g. multiple intrusion Apps).

The only non-standalone functions are global functions where multiple CntrP effect the same function – e.g. where multiple CntrP give access to the same zone, hence affecting counting, time-out, inter- CntrP anti-pass back (APB) and zone enforcing functions. CntrP contain all relevant set-up and user databases in local battery backed-up memory. Access CntrP interface to one to 8 token readers directly, or via portal control modules, serial readers / locks on RS485 links.

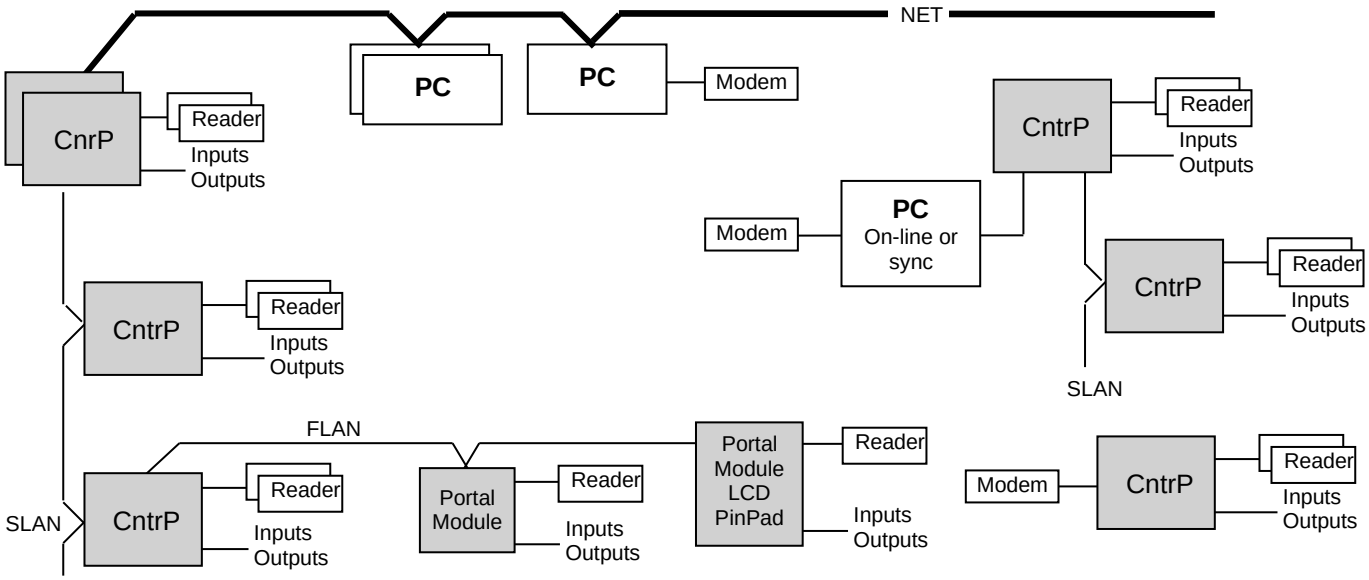
Data between the CntrP and PC(s) is transferred via Softcon Slave Local Area Network(s) (SLAN) or PC networks (NET) and PCs are linked via PC networks (NET). The SLAN uses a multi-drop RS485 interface via shielded twisted pair cables. The NET uses TCP protocol via UTP or fiber cables, linked via hubs/switches.

Communication on a SLAN is via CntrPs connected to a master SLAN CntrP that links to the PC via TCP.
SLAN 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 CntrP does not affect RS485 communication to other CntrP.
It is possible to connect up to 127 CntrP per SLAN.
CntrP and modules can be connected on Front-LANs (FLAN), adding I/O and readers to a CntrP.

SLAN communication is at 9600 or 19200 baud and data transfer is maximized with off-line CntrP 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

SLAN speed and protocol not the limiting factor. When SLAN communication is stopped or not available, CntrP buffer up to 10,000 transactions (see controllers below) in battery backed-up memory.
CntrP time and day of month stamp all transactions.



Where SLAN cables are not available, communication is via GSM modems, Access Point Name (APN) on-line (not provided by Softcon). These are on-line or independent (synced via distribution server – below).

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

- CntrP have wireless communication options on-board or external: WiFi, GSM and Bluetooth.
  These link CntrP to other CntrP, 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 CntrP, 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 CntrP.

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 CntrPs via the NET (master SLAN CntrPs to CntrPs on SLAN) 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 CntrP 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 CntrP being synchronized. Setting of the time and date is performed via a password protected menu, not requiring access to the operating system.

Input, output and reader resources are system based (not CntrP) based and are simply addressed to a CntrP.

7 ACCESS CONTROL TOKENS

Cards, fobs, discs
Generally, the tokens are passive and, with the exception of MAG cards, are generally permanently factory encoded with numbers & facility codes (tokens are available that allow reprogramming of sectors that are used as token numbers).

Tokens are of robust PVC material and construction and are credit card sized or fobs (e.g. on key holders, discs on mobiles). Most token types are suitable for direct printing, those that are thicker, can be detailed by sticking on specialized printed sticky labels. All tokens have printed numbers. Various clips and holders are available.

Types
Multiple token types can be used in the system, in multiple combinations. These are listed in the reader section below.
Random token numbers / Biometric IDs can be up to 12 hex digit token.

8 READERS

The system can use multiple reader types simultaneously as required.

Read ranges will vary from type of token. Passive Proximity (prox) tokens read range depends on the reader used (typically 5 to 750mm).

Up to 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 portal is open and red when access is denied or the reader is disabled. Both red and yellow indicate incorrect token type or facility code or parity error. In 2-line control, amber is created by both red and green on.

For simplicity, data read from a reader is referred to as a token, i.e. the number given by the reader.
Token code structures that can be read are:

- Wiegand – more than 55 formats from 26 to 56 bit (including Corporate 1000) are integrated.
  Tokens can have a facility code and coding can be binary or in binary coded decimal (BCD).
  Checksums can be verified.
  Data can be received starting with the least or most significant bits (card swiped in either direction).
  New token 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 tokens.
- Any popular 1D and 2D barcodes that can be decoded via the appropriate readers / scanners (including drivers licenses and ID cards).
- Hitag, Mifare or ISO 14443 smartprox, read/write, including ID- Credit- and SASSA cards.
- Mobile Bluetooth and Clip (caller id).
- Remotes – unique or programmable numbers.
- Camera to Wiegand vehicle number plate readers.
- Token (disks, keys, fobs) receivers.

Per reader, the following can be set as required:

- Facility code – checked, ignored, part of token number (allows multiple facility codes at a reader).
- Check sum – checked or ignored.
- Number of facility code and number digits (structured token number - allows multiple facility codes at a reader).
- Facility code and number location, with bit stuffing for too few bits.

BARCODE READERS
Most barcodes can be read, including 2D driver licenses (also temporary and learners) and ID cards.
These can be used for access control (e.g. at gate entrances) or can be linked to the user (e.g. assets such as laptops). As linked assets, the asset can also be recorded as a token doing an access movement, hence when the asset entered and exited – with whom.

CLIP READERS
CntrP on-board or external cell modems give caller ID (CLIP) that is used as token 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.

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. Users can be given a zero pin, requiring only a token 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.

WIEGAND READERS can read single or multiple format lengths (tokens with different lengths at a reader).

BIOMETRIC READERS (such as fingerprint, palm, iris, 3d face, Face, Wave, palm and vein readers) corrected to the CntrP via any of the interfaces listed above.

When a biometric reader is interfaced between a token reader and CntrP, the biometric reader verifies the user, i.e. if print matches the token, the token is passed to the CntrP.

Readers can be biometric only, with token or token only. The fingerprint is identified, and the linked reference is given to the CntrP, i.e. the fingerprint reader is a reader to the CntrP. Readers can have multiple biometrics, e.g. face, finger and palm.

All fingerprints are stored in the readers (typically up to 100,000, reader dependent). 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. CntrP grant or deny access according to normal access control functions.

The PC has integrated applications to read and register biometric templates (registering readers connected via TCP or USB). Multiple biometrics can be registered per user, for multiple reader types / manufacturers – includes multiple and duress fingers (reader dependent).
The PC maintains the templet database in each biometric reader.

The following biometric readers can be used (more can be added on request):

TYPE	BIOMETRIC	DB SIZE	CntrP Interface
Morpho MA100 / MA200 / MA300	Fingerprint	500 / 500, 3k / 500, 3k, 10k	Wiegand
Morpho MA500	Fingerprint	500, 3k, 10k, 50k	Wiegand
Morpho MAJ	Fingerprint	500, 3k	Wiegand
Morpho Sigma Lite (Lite +)	Fingerprint	500, 3k, 10k	Wiegand / OSDP
Morpho Sigma	Fingerprint	500, 3k, 10k, 100k	Wiegand / OSDP
Morpho Extreme	Fingerprint	500, 3k, 10k, 100k	Wiegand / OSDP
Morphosmart	Enrolment RD		USB
Morpho FVP	Vein Fingerprint	5k, 10k	Wiegand
Morpho FVP Enroll	Vain Enrolment RD		USB
Morpho 3D Face	3-Face	3k, 100k with token	Wiegand
Idemia Wave	Wave	20k, 40k	Wiegand / OSDP
Suprema BioStation L2	Fingerprint	100k	Wiegand
ZK	Fingerprint	4k FP, 10k token	Wiegand
ZK Enroll	Enrolment RD		USB
ZK FP & Face	3-Face & Fingerprint	1k5	Wiegand
ZK Speed Face, palm	Face, Palm	6k Face, 3k palm, 10k card 30k Face, 5k palm, 50k card	Wiegand
ZK FP, Palm, Fast Face	Finger, Palm, Face	6k Face, 3k palm, 6k finger, 10k card	Wiegand
HiKVision Face 341CNFW / 341BMW	Face	3k Face, 3k card / 1k Face, 5k card	Wiegand / OSDP
HiKVision Face 673DWX	Face	100k Face, 500k card	Wiegand / OSDP

9 TIME SLOTS / GROUPS

The system can use up to 128 Time Groups that each are enabled per weekday and holidays of up to 32 times slots in a day (start and end hour:minute).These are allocated to any function that needs to be set for when enabled.
These are:

Reader enabled
Input monitored
Output controller
Access allowed
Reader and/or Pin must be used
Logged
Mode changed

10 CONTROLLERS

10.1 GENERAL

All CntrPs are intelligent, microprocessor-based control panels that function within the system architecture as described above.

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

10.1.1 Universal / Legacy

Older CntrPs (CR391 to CR390) are referred to as Legacy products, with Legacy Firmware (FW):

- Limited Single applications (Access, Cash or Vending)
- Limited functions (does not do added functions listed below for Universal)
- Less resources (e.g. 2 readers, 16 inputs, 64 Time groups)

No new development. HW discontinued.

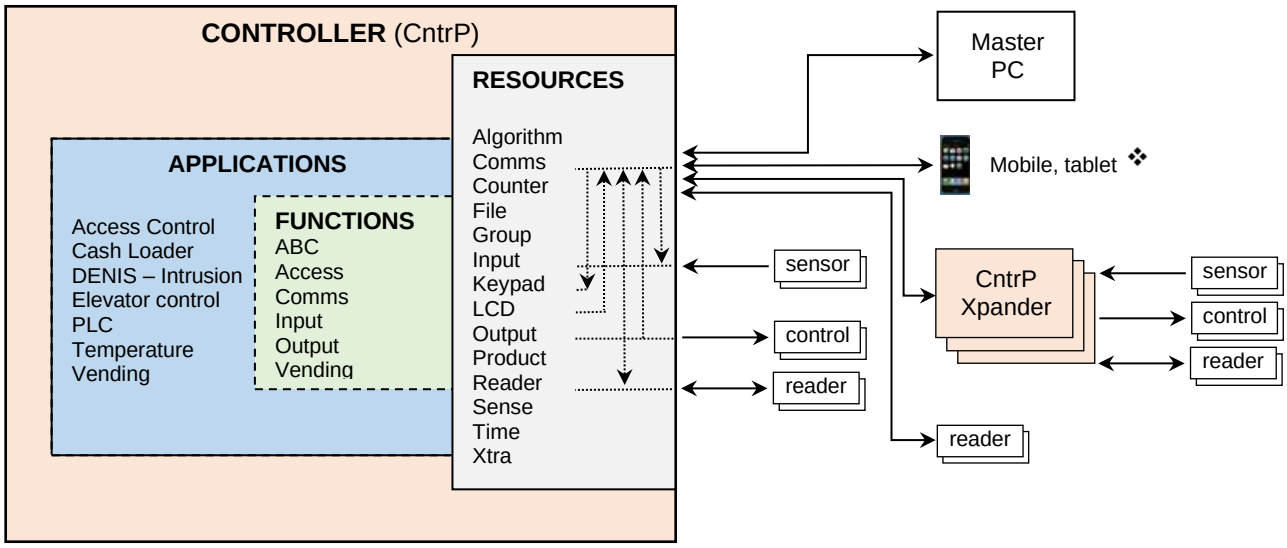
New products are Universal, with universal FW (certain universal products such as CR391 can be set to function as Legacy products).

Universal modes add numerous functions and more resources – some enabled with license keys.
Universal mode requires later versions Software (SW3 = 1.4.62 or above).
This document refers to Universal.

Universal adds the following (these are all specified in this document):

- More (see below) and Multiple application (e.g. Access and Vending)
  - DENIS intrusion
  - Elevator control
  - PLC
  - Temperature
- Added functions
  - ABC Events to output
  - I/O enabled I/O. Output following I/O
  - Random search
  - Polarity on any I/O
  - Pulse and more timeout settings in I/O
- More resources
  via Serial ports to I/O expanders, additional Comms options.
  Moving of resources to these via addressing.
  - 32 Time slots
  - 128 Time groups
  - 256 Inputs
  - 128 Outputs
  - 8 Readers

10.1.2 Architecture



APPLICATIONS

CntrP can simultaneously execute one or multiple app(s), typically:

Access Control, Cash Loader, Intrusion, Elevator control, PLC, Temperature, Vending, etc. (see apps below).

CntrP can execute one or more of the same app, typically access control of multiple portals (each with own token reader and lock) and e.g. multiple DENIS apps (each with own set of sensors and controls).

FUNCTIONS

Apps use functions to execute the application requirements, typical functions:

- ABC Interlinking Access and inputs to control additional outputs Alarm, Buzz and Chime.
- Access APB, ATB, Interlock, Mantrap, Token Capture, Random check, etc.
- Comms FLAN, SLAN master, MDB, OSDP, etc.
- Input Request to exit, reader enable, portal monitor, Intrusion sense, Intrusion mode select, etc.
- Output Lock, capture, control, etc.
- Vending Done detect, select timeout, etc.

RESOURCES

Apps and function use CntrP resources to do the functions and to execute the app, typical resources:

- Comms RS232 port 1 and 2, RS485 port 1 to 3, GSM, Ethernet, etc.
- Input Polarity, EOL supervised, bounce, timeout, enabling input and output, etc.
- Output Polarity, timeout, enabling input and output, controlling input and output, etc.
- Reader Token, Biometric, Mobile or Wireless readers request access, output control or vending.
- Time group Time slots (start and end) and up to groups (when active for zone per weekday, holiday).
- Time Real time, holidays.

Resources can use resources – e.g. time groups use time resources real time and holidays.

Reader, input, output, LCD and keypad resources can be connected to the local CntrP or to externally linked CntrP, extenders or modules. The connection location settings of Com.Node.Port addresses the resource. Com and Node set to zero locates the resource locally and for external locations, Node is the address on the serial Com port the resource is connected to. Port is port on the CntrP / extender the resource is connected. Resources could be virtual (Com, Node and Port set to zero) functioning as normal, without any connection (e.g. input reader enable – active on time group, output – intrusion enabled).

For example, readers:

0.0.1	on-board reader 1.
1.1.1	Reader 1 on the CR395, node 1 connected to ComB.
3.0.0	direct serial RS232 reader connected to ComC.
4.3.2	2nd Salto reader of node 3, connected to SLAN to ComD.

LICENSE KEYS

FW restrictions and license keys limit the Apps, functions and resources and the number thereof.
SW keys enable devices such as scanners, biometric readers, etc.
The keys can have expiry dates. Keys can be changed via the system.

10.1.3 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 CntrP.

RS485 cable (FLAN, SLAN, ODBC, etc.) screens must be earthed per segment and the segment screens must be isolated from one another.

Total RS485 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.

10.1.4 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 into 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).
Apps enabled and maximums can be queried and are limited by license keys that can be changed.

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

CntrP have a unique electronic ID (MAC address) and all have FW version information.
These are reported to the PC.

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

10.1.5 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-condensating. Where CntrP are mounted within enclosures, sufficient external ventilation must be provided.

10.1.6 Power Supply

CntrP are supplied with 110 or 230VAC (10W, excluding lock and reader power). Optionally, CntrP can have an integrated UPS 7 AH, or can be supplied with 12 VDC (700mA, excluding lock and reader power). CR393 CntrP are supplied with 12 or up to 35VDC with vending module.

10.1.7 Housing

CntrP is contained in white powder coated steel metal housing (to be discontinued) or in
ABS-flame retard moulded enclosure; with key locked hinged lids (lid opening can be monitored).
CR392 CntrP can be supplied in aluminium extrusion boxes.
Additional cover plates, with appropriate high voltage warnings, protect power supplies.
Adaption plates allow newer (smaller) PCBs to be installed in the larger metal housings.
ABS and power coated housings are available for the smaller CntrPs and modules.

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.

Moulded housing has Patented Slide cable entries – with cable tie down.
The housing and lid are appropriately earthed to the mains earth and terminals are provided to earth cable screens.

10.2 APPLICATIONS

The CntrP can have one or more of the following Apps installed and activated as required.

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

- SMS CntrP, application names, name of resourced changed (portal, 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.

10.2.1 App – Access Control

The CntrP functions in a stand-alone mode with a local credential database of up to 125,000 randomly numbered tokens, with PIN. Searching for a random credential at location 125,000 is typically within 150msec.

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

Integrated local access functions are:

- Tokens 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 tokens 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 or setting other readers ATB for the current token. Up to 30 tokens are timed out per reader (oldest overwritten).
- Multi-badge can be set per reader (2 to 9), access only after set number of enabled tokens are badged within timeout period. If a not enable token is badged or timeout occurs, all tokens in multi-badged queue are cleared. When successful number have badged, access is granted and all tokens in the badged queue are reported as entered, queue is cleared.
- When access is granted, lock 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 portals, monitoring portal, lock and occupied statuses and timeouts.
- Interlock setting prevents other portals to the same area zone opening.
- Local events can be set to activate additional local outputs (see ABC).
- Multiple illegal requests can be set disable the reader.
- Random check/search with % setting and overrides can be set per reader.
- Device readers can be set to act as completion of the badge request – the device data is linked to the token. The device data can be sent as an additional token event, linked to the badge token (details below).
- Readers can be disabled, portal can be permanently locked / unlocked on command from the PC, on linked inputs or on time groups.

Reader events generated (with token number) are:

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

Portal event generated are:

- Illegal open.
- Opened too long.
- Not Opened.

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

- % check is set for each search and can be overwritten by token 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 portals when the check fails.

Device data linked to badged Token:

- A device reader (typically weight scale, barcode scanner) can be linked (serially) to a reader.
  The token is badged at the reader, data from the linked device functions as the portal sense to the badge.
  The entered event adds the device data read (e.g. the weight, laptop number, project number) to the token with reports for token badged, devices linked.
  The device can be set to generate an additional token event – device number then the token number (must be in the user database) and the token badged is reported with the event – reports for device, which tokens were linked.

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

- Output groups are allocated functions.
- A function is a reader number of the CntrP, 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).
- tokens are allocated an output group (e.g. group 2 at reader 3 activates outputs 1,4 ,5).

10.2.2 App – Boot Loader

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

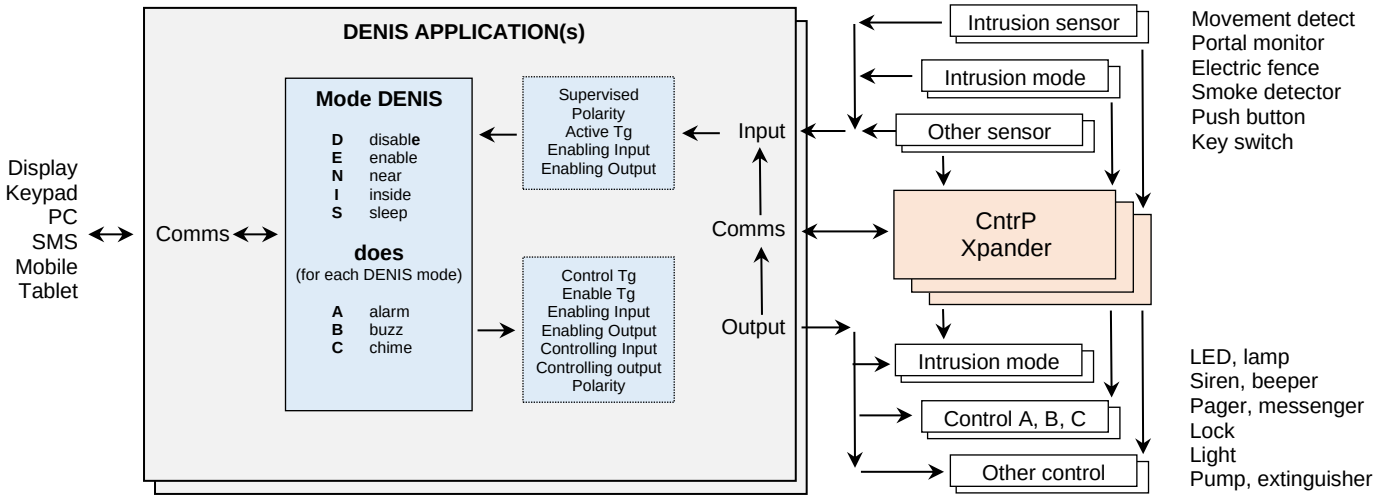
10.2.3 App – Cash Loader

The CntrP connects to note / coin acceptors is via serial interfaces.
Money deposited is reported to the PC with the access token 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.

10.2.4 App – DENIS (intrusion)

Intrusion is the integrated application that serves as an intrusion alarm panel.
Functioning is “DENIS does ABC”
The app is set to one of the following modes via inputs, via comms commands (SMS, GSM, PC) or by LCD/keypad:

DENIS	MODE	TYPICAL	SENSORS
D	Disabled	Off	Only panic
E	Enabled	Away	All on
N	Near	Gardner	Inside on
I	Inside	Home	Outside on, Inside off
S	Sleep	Sleep	Only bedroom on



By defining input and output types for intrusion (see input / output above), alarm (intrusion) system functions are controlled.

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

- DENIS mode Disable.
- DENIS mode Enabled, Enabled / disable toggle.
- DENIS mode Near, Near / disable toggle.
- DENIS mode Inside, Inside / disable toggle.
- DENIS mode Sleep, Sleep / disable toggle.
- DENIS mode toggle (though all the modes).

By setting time group to inputs (real or virtual) that set DENIS modes, DENIS can automatically change mode on an active time group (e.g. NEAR mode on Wednesday mornings (if not holiday).

When the mode is changed, a message is set to the PC.

Outputs can be set to show the DENIS mode:

- DENIS mode Enabled.
- DENIS mode Near.
- DENIS mode Inside.
- DENIS mode Sleep.

Intrusion sensors are connected to input set as Intrusion input.

All inputs can be set with time groups and can be linked to Enabling input (e.g. overriding key switch) and enabling output (e.g. fire alarm disables sensors).
Each input can be set with bounce time (input not monitored for the bounce period - e.g. entry inputs).
Each input can be set with timeout time (input not monitored for timeout period after mode change - e.g. exit inputs).

Each input is can be set to do Alarm, Buzz and / or Chime for each of the DENIS modes, e.g.
Panic and Fence inputs set to Alarm for all modes (including Disabled mode).
Outside sensors set to Alarm and Buzz for Enabled, and Sleep, set to Chime for Inside mode.

The following action (does) outputs can be configured:

- Alarm, e.g. siren
- Buzz, e.g. SMS / radio
- Chime, e.g. beeper on terminal

Interlinking outputs can add actions, e.g.

In Near mode, pool pump on.
If Near mode and garden shed open, electric fence off.

Each output is also set for pulse (on-off bleep period) and time out (period on).

As every input and output is set with a type reference, multiple DENIS app can be set, each with own mode, mode inputs and indicators and ABCs.
The maximum number of DENIS applications are dependent on FW compile and license key restrictions.

10.2.5 App - Elevator ❖

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 portals closed and lift not in use.
- Level portal — for each level, portal status.
- Bottom — lift at bottom level alarm.
- Top — lift at top level alarm.
- Maintenance — portals are unlocked.
- Now — for each level, lift at level.
- Occupied — lift occupied (beam, pressure or motion detector).
- Alarm — panic / error input.

Outputs are:

- Level lock — for each level, portal 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 portal open, moving, occupied, till timeout.
- Alarm — error condition, alarm input. Cleared when any portal opened.

10.2.6 App - 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 (see ABC, input/output enable, follow), and other resources are in certain statuses (set algorithm of statuses the must be true).

These triggers and resulting events and resource statuses include inputs, outputs, counters, timers, time groups and reader events. For example, portal 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.

10.2.7 App – 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.

10.2.8 App – Vending Control

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

When a token is badged or voucher number entered, 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 CntrP is in “Free Vend” mode, the item is free or if sufficient funds (or tokens) are available for the user for the selected item (from local or PC dB).

On successful vend, the remaining funds are updated.

Vending interface is either:

- Serially 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).

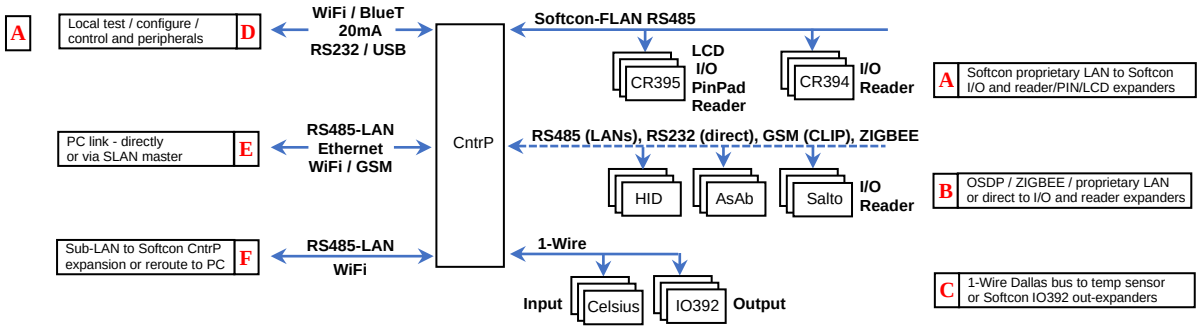
Using the CR395 as keypad interface, the Vending machine’s keypad can be shared for entering voucher numbers.

The following configuration setting are set on the Server:

- Interface type.
- Cashless reference / vend monitor (monitor note/coin other cashless devices).
- Share keypad, Key selection offset and type.
- Selection and vend timeout.
- Free and credit settings.
- Detect done, display new value remaining

10.3 FUNCTIONS / RESOURCES

10.3.1 Communication



Multiple Softcon expansion CntPs CR395 (reader, LCD, PinPad) and CR394 (reader, 32 inputs and 16 outputs) are added via the Softcon proprietary RS485 Front LAN (FLAN).

B Readers, inputs and outputs can be added via direct link (RS232) or via specific LAN RS485 networks, these include OSDP, Zigbee / BT mesh (future), ControlSoft, Salto, AssaAbloy and Matra LAN. More could be added on request.

C All Softcon CntrPs and expanders have a 1-wire expansion bus (100m length) that adds multiple IO392 (2-relay) extenders and temperature sensors.

D Test / debug options are available and local setup / control communication can be used in on and off-line modes. Peripherals such as printers, note/coin reader and vending machines can be connected.

E Communication options between PC and CntrP is either Ethernet or serial (GSM, WiFi or RS485).
This is used for set-up, control and reporting,
Via a Softcon RS485 SLAN, CntrPs can link as slaves to a CntrP SLAN master that routs data to PC.
When communication if off-line, transactions can be set to be buffered in non-volatile memory (stored when powered down), in volatile memory (data in buffer is lost when powered down) or dumped (data is not sent to the PC).

F Serial SLAN connections are available to SLAN CntrP, redirecting data to/from these CntrPs to PC).
These connections can be used to update / change FW in SLAN CntrP.

External fibre optical interfaces (RS485 and Ethernet) and additional resistor/ capacitor/ inductor/ tranzorb/ surge arrestor interface are available where greater distance and protection is required.
The additional protection interfaces are mounted externally.

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	
Basic	RS232 ASCII, no handshake
Front LAN	RS485 to Softcon expanders
SLAN master	RS485 to sub- CntrP
SLAN slave	RS485 to master
Modem	RS232
PC direct	RS232 slave
PassThru	Pass to/from Test port
Test	RS232 – test and diagnostics
ControlSoft	RS485 multi-drop readers
LMI scale	RS232 weight scale
OSDP	RS485 multi-drop readers
Reader	RS232/485 single reader (e.g. barcode)
Salto, Assa Abloy	RS485 multi-drop readers / locks
ID barcode	RS232 (RSA ID card, driver's licenses
Cash loader	Note / coin readers
DEX	RS232 vending machine management
Vending	20mA MDB vending machines dispensing
BlueTooth module	
GSM module	
Power Line Data (Comms)	Via AC mains power supply (under development)
RF module	
WiFi 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 CR392 CntrP, facilitating development of systems by uses of these CntrP.

Ethernet CntrPs can link to the program SCS_Controller running on a PC on the network - via an additional TCP socket. SCS_Controller reads the setup in the CntrP and can be used to alter the setup (overwritten by the SW3 SW).
SCS_Controller and SCS_Client (SW3) have “Discover” functions – listing all CntrPs detected (shows MAC, IP, Mask and Node – these can be altered via the “Discover” functions.

Licencing keys enable applications and quantities connected.

10.3.2 Memory / RTC

Set-up and user 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, user 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 (RTC) is synchronized to the PC RTC when the CntrP goes on-line and within every hour thereafter.

10.3.3 Time / Count

Up to 128 time-groups, with up to 32 time slots (start and end time) are available to enable:

- Access when token 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 slots per day of week and holidays.
30 holidays, the time slots and time groups are stored in the CntrP.

The CntrP has integrated timers and counters, performing functions such as lock times, portal open too long, anti-pass back. Illegal attempts, event statistics (see CntrP 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 CntrP application PLC functionality below.

10.3.4 Readers / Tokens

CntrPs can accommodate 0 to 8 readers (depends on CntrP type, limited by FW and license keys).

Reader interfaces:

- Dual line Wiegand.
- Data/clock.
- 1-wire Dallas.
- Serial RS232 / RS485 / GSM (clip). Settable baud rates and bit structures.
- Protocols – ASCII, AssaAbloy, ControlSoft, HRC, Matra, MagTech, OSDP, Salto, etc.

Tokens

- 'Any' Wiegand format…. (26 to 52 bits, 55 format structures). Indala, Prox, Hi-Tag, EM, iClass, Mifare, Biometric.
- Barcode, Drivers licences, ID- Credit- SASSA-cards, Mobile Clip / BlueTooth, remote controls.
- Settable Parity, Client and site codes, Bit locations, Number of Characters, Hex/BCD/Decimal.

Each reader can be configured for:

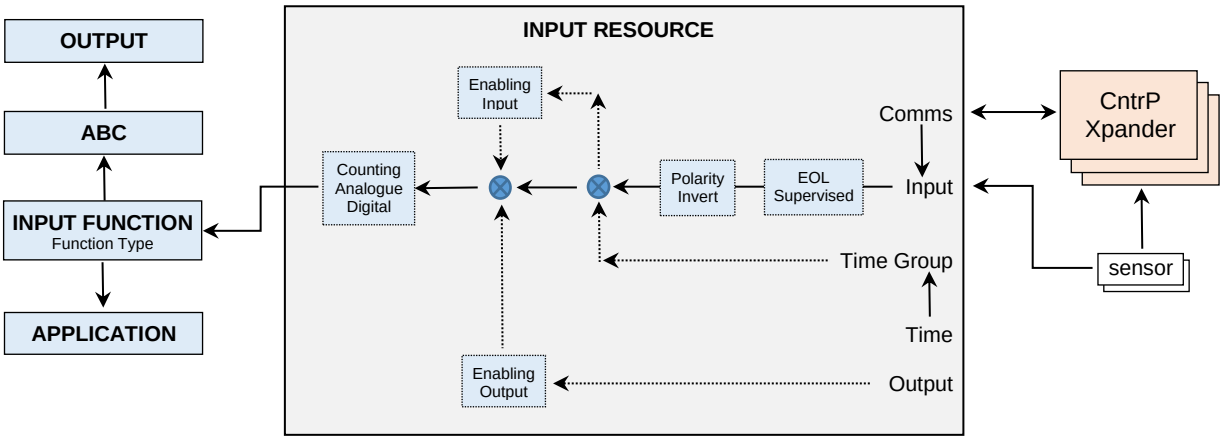
- App — App linked to.
- ABC - OFRID — Alarm, Buzz, Chime outputs for events Ok, Failed, Random, Illegal, Duress (see ABC).
- APB, ATB — Anti- Pass, Time Back (link to clear / set other readers).
- Capture — Token capture of capture tags, capture disable.
- Com.Node.Port — Where reader is connected (Com=0 for local, other=Com port).
- Duress — Type.
- Clock polarity — Invert the clock pulse.
- Illegal attempt — Number or failed requests, reader disable time.
- Inter-link — Ref to reader for interlock.
- Device-link — Serial port is linked to reader.
- LCD ref — Where messages are displayed.
- LED type — 1, 2 or 3 LEDs, flash yellow.
- Multi-badge — Badges required.
- Name — Reader description (used for LCD display and SMS events).
- PC display time — Display timeout for PC messages.
- Random Check — % check.
- Reader voltage — 0 or 12V, current limit/not.
- Report — Facility, format errors.
- Token display — Displays token number on LCD.

CntrPs can accommodate 0 to 8 readers (depends on CntrP type, limited by FW and license keys).

10.3.5 Inputs

CntrP have on-board inputs that are mostly supervised (short circuit, closed, open and open circuit).
The number of inputs can be expanded with multiple serial linked CntrP (via RS484 FLAN) 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. portal and lock monitor, tamper, etc.).

Input location (where connected) is set with Com.Node.Port (the port on the CntrP or extender).
If local, Com and Node is zero.
If no Com Node Port settings, the input is virtual (e.g. reader enable, Tg enables).



Each input can be configured for:

- Active level — Open or closed (polarity).
- ABC — Certain input events can be set to trigger additional outputs (see ABC below).
- Counting input — Reporting counted values on request or after pre-set time-outs after change.
- Bounce — Time in level before taken as active.
- Enabling input — Input only monitored when another input is active, e.g. system on/off switch.
- Enabling output — Input only monitored when another output is active, e.g. siren on.
- Name — Input description (used for SMS events).
- Supervised — Enables monitoring of short and open circuit – event reported, ABC output activated.
- Time group — When monitored.
- Timeout — Alarm when input is active longer than set timeout, e.g. open too long.
  For intrusion sensor inputs, the exit delay (after DENIS mode change)
- Type, ref — Enables the input for specific functionality (see input type table below).

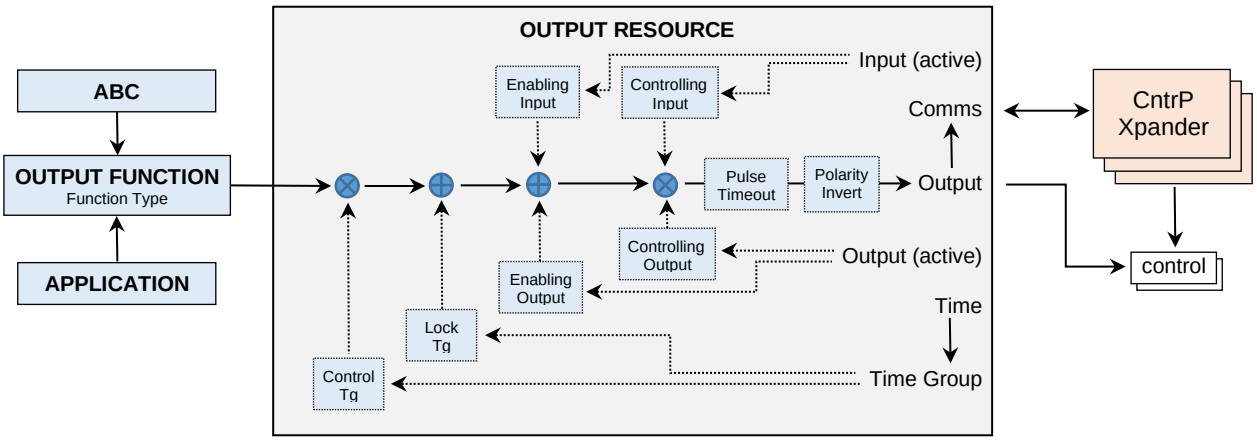
The Input type setting results in events by integrated functions for linked applications
e.g. type REX activates the corresponding lock output.

INPUT TYPES			
Auxiliary input	Action complete (portal sense)	Check 0%	Denis mode Disable
Battery monitor	APB enable	Check 100%	Denis mode Enable
Mains monitor	Booth (mantrap) call	Check continue	Denis mode Enable / disable toggle
Tamper	Booth (mantrap) occupied	Check fail	Denis mode Near
	Token capture detect	Check pass	Denis mode Near / disable toggle
Vend cleaned	Egress/Request to exit (REX)		Denis mode Inside
Vend do	Reader enable	Level call	Denis mode Inside / disable toggle
Vend done	Reader tamper	Level bottom	Denis mode Sleep
Vend failed	Lock monitor	Level top	Denis mode Sleep / disable toggle
Vend Filled/cleared	Last token	Level maintain	Denis modes toggle
Vend I/O in	Reset APB	Level now	Denis input sensor
Vend serviced	Reset ATB	Level occupied	
	Reset Tg Count	Level alarm	Temperature degrees C
			Temperature alarm Lo
			Temperature alarm Hi

10.3.6 Outputs

CntrP have on-board outputs that are generally relay or open collector outputs.
Outputs can be expanded via multiple expansion CntrP (e.g. CR394 with 16 relays) on a RS485 FLAN and via modules (e.g. IO392 with dual relay) on a multi-drop 1-wire.
Certain readers can add outputs (e.g. lock, LEDs, etc.).

Output location (where connected) is set with Com.Node.Port (the port on the CntrP or extender).
If local, Com and Node is zero.
If no Com Node Port settings, the output is virtual.



Each output can be configured for:

- 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 lights.
- Enabling input — Output only controlled when another input is active, e.g. enabling key is switched on.
- Enabling output — Output only controlled when another output is active, e.g. siren on.
- Name — Output description (used for SMS events).
- Pulse — Output pulse period while active.
- Time group on — When automatically active, e.g. gate open 7:00 to 8:00 weekdays.
- Time group lock — When output cannot be controlled.
- Time out — Active time (e.g. lock time).
- Type, ref — Selection (see output type table below) enables the output for specific functions for the appropriate application (see applications).

The Output type setting results in activation by integrated functions for linked applications (e.g. type lock is activated to the corresponding request to exit input or to the reader when access is granted).

OUTPUT TYPES			
Alarm	RD isolate (virtual)	Temperature normal	Count full
Auxiliary	RD LED green	Temp alarm Lo	Count available
Buzzer	RD LED red	Temp alarm Hi	Count empty
Chime	RD LED yellow	Temp cool down	
Off-line	Rd out hi / clock	Temp heat up	Level go down
	Rd out lo / data		Level go up
Denis mode Enable		Check-Search	Level lock
Denis mode Near	Capture		Level light
Denis mode Inside	Interlock busy	Vend Out	Level now
Denis mode Sleep	Lock		Level alarm

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 CntrP).

Multiple outputs can be activated locally by CntrP as result of token activity, time setting, event / status algorithms. Token to multiple outputs is effected by the allocation of any of the output groups available in access CntrP to users.
Alarm, Buzz and Chime (ABC) outputs can be set to be active on certain events (see ABC below).

10.3.7 ABC

Additional local control can be configured using ABC outputs.
Any number of ABC outputs can be set to be active on any of the following events:

Access events (OFRID) for each reader event:

Ok	Access granted
Failed	Access denied
Random	Random check failed
Illegal	Exceeded number of access denied requests
Duress	Pin or finger duress

Intrusion input events (DENIS) active when the Intrusion App in mode:

Disable
Enable
Near
Inside
Sleep

Non-intrusion input (ANILF) events:

Active	
Normal	
Illegal open	portal sense
to Long open	active longer than timeout
Failed to open	portal sense, not active within timeout

Events that activate Alarm outputs can also send SMS messages to users set for alarm reporting.

10.3.8 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 CntrP is on and running. Ticking twice a second indicates communication with SLAN CntrPs.
A **red** LED indicates on-line (via NET if TCP, or via SLAN is slave), with on indicating communications is correct.
A **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 communication or diagnostics.
Certain CntrP and expanders have LEDs indicating output status.

Plug-in test modules available for CR391:

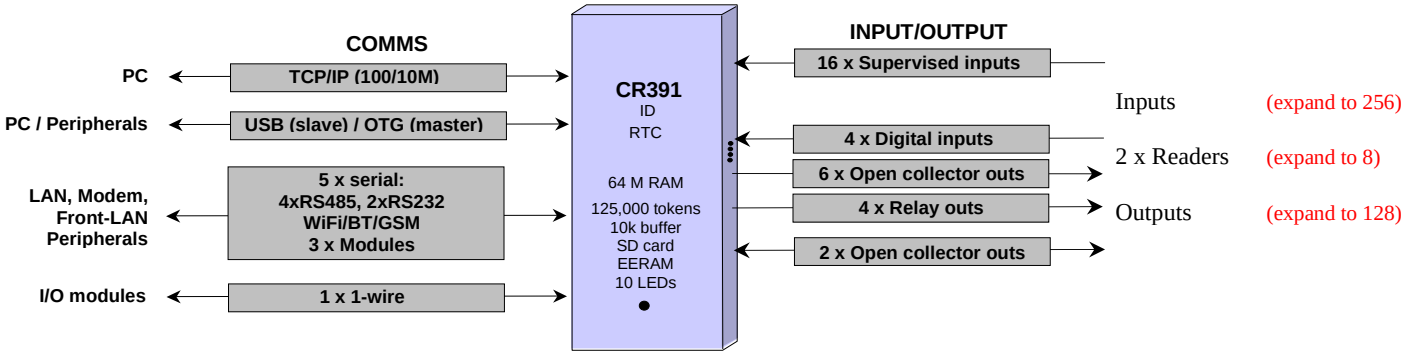
- 8x Input switch.
- 4x Output LEDs.
- 16x Input switch, 4x Output LEDs, 2xReader LEDs.

System modules with the following can be used for any CntrP or expander:

- 8x Input switch.
- 4x Output LEDs.
- Power switch.
- Reset link.
- HH link.
- 2x Reader connect (Wiegand, Data/Clock), with 3x LEDs

11 CONTROLLER TYPES

11.1 CR391 UNIVERSAL CONTROLLER



Comms

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

- 4 x RS485.
- 2x RS232.
- Onboard - GSM, WiFi/Blue Tooth and Zigbee (future).
- 3 x expansion modules.

The serial type, rates (up to 56k) and bit structure are set for any port.

The serial ports can communicate to readers (with Pin Pads, and LCD displays), token 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 SLAN CntrP, interfacing CntrP via RS485 multi-drop to the PC.

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 255 and outputs to 128.
- Capture units can be set at any readers.

Readers / Tokens / Db

- Up to two reader port can be set on-board (tranzorb protected) ports (Wiegand, Data/clock, touch).
- Readers each with 3 LED control.
- 125,000 user 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 CntrP / interfaces / modules, e.g. CR395).
- 64 Output groups with 128 output functions.
- Event buffering is 10,000 transactions.
- Data in the CntrP can be viewed and edited with a CR395 hand programmer that is connected via a FLAN or via RS232 terminal.

Timers / Counters

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

Applications

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

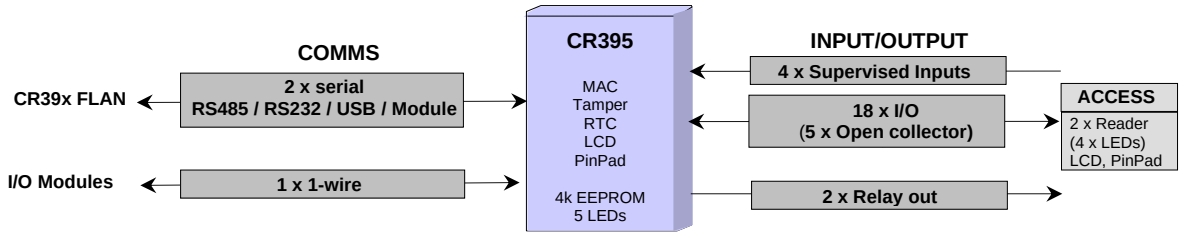
System SW keys can also be stored in the CntrP non-volatile memory, with the PC setting and retrieving the keys when required.

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.
- 8 LEDs, visible outside the house indicate running, communication and reader activity.
- Built in Transaction statistics can be reported to and set by the PC, typically the following info:
  - Communication: On/offline, 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.

11.2 CR395: CntrP, Expander, Rd Converter, SLAN Master



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

Application options:

FLAN Expander

The CR395 CntrP is a front-end portal CntrP for the CR391 CntrP with:

- LCD — 2 line, 16 or 20 character, directly to the PCB.
- Pin Pad — 3x4 or 4x4, directly to PCB, with Local or External Column/Row, External Row En-disable. External control by CR391 or linked input.
- 2 x Reader — Wiegand or data/clock (2 LEDs each)
- 4 x Supervised Inputs
- 5 x OC Outputs — Open Collector Darlington with 500mA/50VDC rating.
- 2 x Relays — 3A.
- I/O expanded — to via multi-drop 1-wire interfaces.

Input and reader data are 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 (4 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 CntrP displays the real time and the access status (e.g. “denied” or “proceed”). The PC can display additional data such as the username, available subsidy, accumulation time, messages, etc.

Communication between a CR395 and a CR39x is via a multi-drop RS485 FLAN cable with a maximum of 8 CR395 connected to the cable. FLAN can be shared with CR394s.

CntrP

Stand-alone CntrP with:

- RTC, 16 x Time slots, 32 x Time Groups, 30 x Holidays.
- Access control for 50 Tokens, 2 x readers.
- 4k EEPROM for specialized stand-alone applications.

typically – Portal controller, PLC.

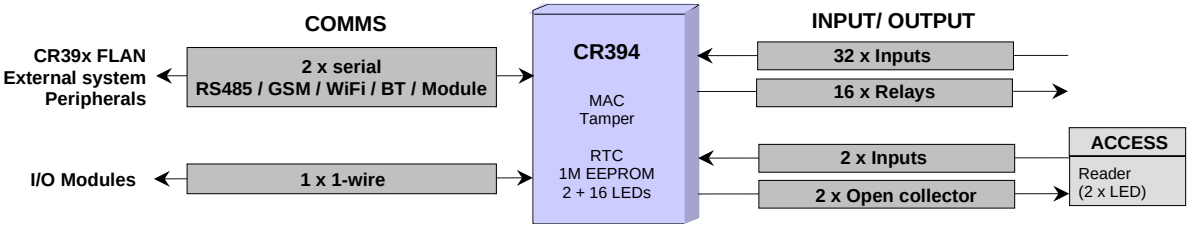
SLAN Master ❖

Control of RS485 SLAN, interfacing to external system via RS232 or USB.
Holds external system Licensing Keys.

Reader Converter

Converts Wiegand / Mag / Serial reader data to any other (e.g. Mag to Wiegand, Wiegand to Serial).
RS232 or USB communication to external systems (e.g. to Point Of Sale).
Relay control by external system (e.g. open barrier, open money drawer).

11.3 CR394 (I/O EXPANDER, READER, CNTRP)



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

Application options:

FLAN Expander

The CR394 CntrP is a front-end expander CntrP 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 are 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 CR395s.

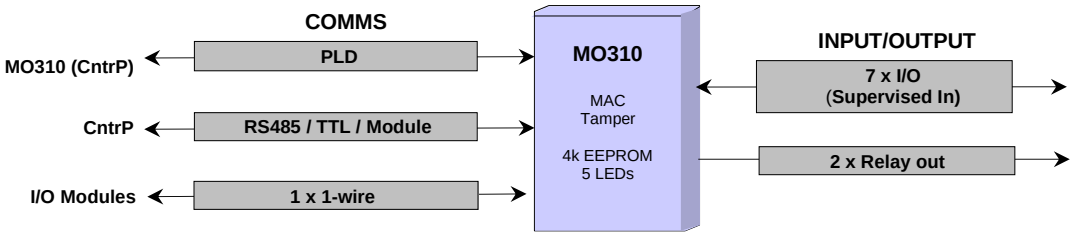
CntrP

Stand-alone CntrP with:

- RTC, 16 x Time slots, 32 x Time Groups, 30 x Holidays.
- Access control for 500 Tokens, 1 x readers.
- 32 supervised inputs, 16 relays (3A).
- 1M EEPROM for specialized stand-alone applications.

typically – Intrusion (DENIS), Irrigation, I/O vender, PLC.

11.4 MO310: Modem, Expander ❖



Multi-drop power line (mains 220VAC) communications

Application options:

Power Line Modem
Between CntrP (SLAN) or between CntrP and Expanders (FLAN).

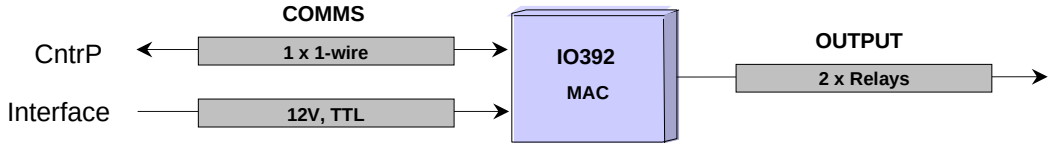
FLAN Expander
Front-end portal CntrP with:

- 1 x Reader — Wiegand or data/clock (2 LEDs each)
- 7 x I/O — Supervised Inputs
- 2 x Relays — 3A or 20A
- I/O expanded — to via multi-drop 1-wire interfaces.

2 x Geyser, Pool (light, pump)

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

11.5 IO392 (1-WIRE I/O EXPANDER)



Multiple IO392 modules communicate on a 1-wire bus with CR39x CntrP. 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.

12 SDK

A Software Development Kit (SDK) is available for developers of SW interfacing to Softcon CntrP.

- XML on Windows or Linux.
- The SDK drivers communicate with the CntrP via TCP networks.
- The SDK has integrated test and simulation tools and provides sample programs.
- License keys control the function available to the SDK.

The Softcon SW3 programs listed below use the SDK.

13 COMPUTER SPECIFICATIONS

The Softcon software programs listed in the following sections, require the following minimum PC:

Software Requirements (any of):

- Windows 7 Professional.
- Windows 8.1 Professional.
- Windows 10, 11 Professional (new installations)
- Windows Server 2008, 2012, 2016, 2019 (run as administrator)

Database:

- MS Access.
- SQL Server 2008, 2012, 2014, 2016, 2018.
- SQL Server 2008, 2012, 2014, 2016, 2018 Express.

Faster PCs with more RAM and Hard Drive speed (optimally solid state) is suggested.

HW minimum requirements:

- I3 2.3GHz.
- 2 Gig Memory.
- 250 Gig HDD Space.
- TCP/IP.
- 1024 X 768 resolution Screen.

HW minimum requirements for SQL Client PC:

- I5 3.0GHz.
- 8 Gig Memory.
- 250 Gig HDD Space.
- TCP/IP.
- 1024 X 768 resolution Screen.
- Windows 10 Professional

HW minimum requirements for SQL Server PC:

- Intel Zeon 3.2GHz or equivalent AMD.
- 32 Gig Memory.
- 1TB SSD or M.2 SSD.
- 10 GB TCP/IP.
- Windows Server 2016 and up.
- SQL Server 2017 Standard and up.

14 SOFTWARE

14.1 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, token 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.

14.2 APPLICATIONS

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

- System (see below).
- Access control.
- Asset management.
- Bootloader – updates FW in CntrP.
- Cash Add. Incorporated in the Client program or available as a separate exe client program.
- User Access – zone display.
- Token (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 users (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:
  Canteen and Vehicle park entry control, Cashless vending, Photostat-, Laundromat-, Car wash, Cash loaders, etc.
- Visitor control.

14.2.1 System (SCS_Client)

This is the main application, incorporating the following:

- Links to the Server – Reading and configuration system data.
- Links to CntrPs:
  - Can detect all Softcon CntrPs on the local TCP network:
    - Shows MAC and shows and allows editing of TCP settings and node address.
  - Sending configuration, token information and control commands.
  - Receives events.
- Edits of all data.
- Event management (display, logging, generation of new events).
- Executes the Access control and Vending applications.
- Links to all other App, exchanging events.

14.2.2 Access Control

User setting for access control are listed for the user data – access.
User 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 users are set to only exit via reader A (which has a token 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 token.
If APB is used on staff users, the two “OUTSIDE” areas need to be linked to prevent APB problems.

AREA GROUPS are a selection of area zone(s) to which user(s) have access.
Each user is allocated an area group, which can be unique to the user, or users can share groups (e.g. cleaner group, admin group).

Area groups can be batch loaded with area zones.
An area group can be disabled.
Users can be allocated multiple groups, e.g. parking group and 1st floor group.

ANTI-PASS BACK: APB is settable per reader.
The last area zone entered by each user, via an APB reader – the last APB location, is stored.
Access is denied when a non-pass back tokens requests access at an APB reader, and the last APB location of the user is the same as the zone the reader grants access to.

The PC updates token enable/disable between CntrPs as a result of APB (CntrPs do local update)

ANTI-TIME BACK: ATB is settable per reader (minutes and reader linking – linked readers can be configured to be set or cleared).
ATB is limited to readers in a CntrP (no inter CntrP changes).

TOKEN NUMBERS: Users can be allocated two tokens (e.g. a prox and a MAG card), with token 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 users 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 user 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 user 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.
Users 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 token database or not.
When set with a database (generally set), the CntrP effectively does access control functions in an off-line mode, granting access only if the portal is not permanently locked, the reader is enabled, token facility codes is correct, the token is found and is enabled for the reader and the time group is active (correct time of day holiday setting pass).

On entry, the token becomes disabled for the reader if APB is set.

When reader does not contain database, only the facility code is checked by the CntrP, all other functions are done by the PC. APB, enforced zone control, zone counting, users linked to hosts, random search and expiry functions are always controlled by the PC which updates the CntrP as required.

Should a CntrP be off-line, these functions are not active for that CntrP. Where systems are configured to function independently, changes to user 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 tokens with correct facility code when the CntrP is off-line (token database settings are not checked).

READER DATABASES are set to use with up to 125,000 tokens (see controllers above) in CntrP memory (facility and token number), 12 character (HEX) random number.
Tokens not in the CntrP memory are reported as out of area and if access is granted, the oldest token to have been granted by either reader is replaced in the CntrP by the new token.
CntrP can be set to require a PIN code (on time schedule), with or without token (on time schedule).

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

- Wrong format, Wrong facility.
- Not found, Disabled, Expired
- Wrong PIN.
- Out-of-count
- APB error, Strictly from error, Out-of-area, Out-of-time.
- No host.
- Enabled.
- Entered, Captured, Duress,
- 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 tokens that have access within a settable time period to gain access.

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

RANDOM CHECK (e.g. alcohol, drug, search search) function is triggered automatically when users 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 user, i.e. the users set % is used or if zero, the reader setting is used.
Events could be generated (e.g. by inputs locally in the CntrP 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 CntrP.

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 CntrP – or via event in the PC.
Multi-control (typically lift control, alarm activation) – can be done via relays controlled by outputs of the CntrP – locally by the CntrP or by events in the PC.

When controlled locally, a token 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 CntrP, 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 CntrP relays or receives command via a serial link with the CntrP. The reader and CntrP is generally mounted in the lift – the user enters lift, badges token and selects one of the floors available to the user.

14.2.3 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 tokens):

- Reference — Running index number.
- Name — Descriptive name.
- Code — Barcode or Asset token 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 token location (reader area zone to).
- *Detected — Date/time token last detected.
- *Battery — Last reported token battery measurement.
- *Alarm status — Last reported token alarm status.
- *Alarm date — Date/time last token 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 token readers.

Assets are issued by selecting or reading the item code (barcode reader or asset token reader tied to the PC) and selecting the user issued to (token 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 token readers connected directly to the Softcon CntrP. The last reported token location, date/time, battery measurement, alarm status and alarm date/time are automatically recoded.

14.2.4 Bootloader

CntrP are updated with the latest or specific FW.

Schedules are set for when specific CntrP are updated, with selected hex file.
TCP linked CntrP are updated directly and CntrP on RS485 SLANs are updated via the SLAN master.

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

14.2.5 Card (token) Maker

A Token maker system is client application that is integrated in the client system or is run as a separate program. Data captured with the Token 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.

Biometrics (fingerprint, vein, face) can be captured for use in access control, with settings of 1 or 2 fingers, (or duress) finger per person.

Any numbers of token designs are made via the integrated WYSIWYG drawing design module described in the graphical display section. A token design is selected for each Token. Token encoding information can be set on the token design, linked to database data.

Issue number can be set to automatically incremented on token 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, TCP cameras, etc.
Photos can be colour or black & white, file imported.
Pixel resolution is as defined by the installed interface.

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

14.2.6 Parking

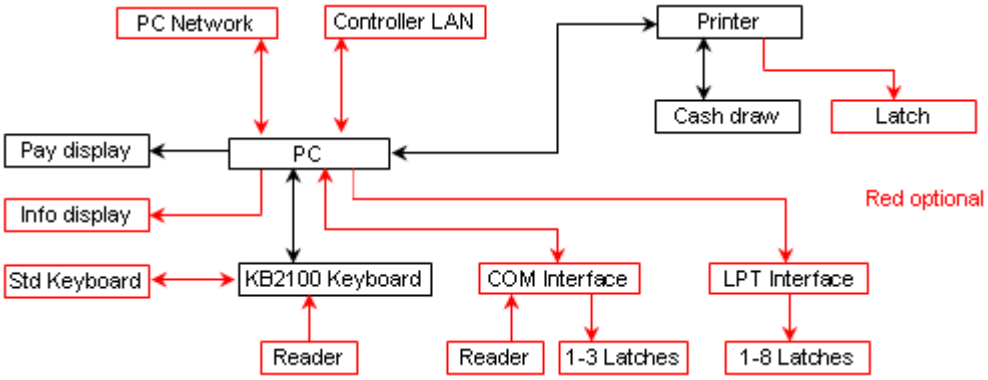
PAY ON EXIT – ACCESS SYSTEM

A pay on exit option to access control allows the setting of readers tied to access CntrP as Park Entry, Park Display, Park Pay or Park Exit readers. On entry, the date and time is logged to the user 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 user 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 pre-set values (e.g. car, taxi, bus, lost token, pedestrian) per entry lane and can vary on time of day/week. A configurable slip containing the selected data can be printed.

Visitor tokens 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. Visitor tokens 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 tokens that are issued on entry and retrieved on exit. These tokens are be badged 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).

Portals (linked to vehicle type) and the cash draw shall be controlled via relays connected to serial or USB CntrP (COM ports) or via the slip printer.

EXIT ON SCAN

A token (typically a barcode) is read and the number in entered into the user database.
Exit is granted on reading the token at the exit reader.

14.2.7 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 user and/or users and manage cash via a cash draw.

A POS functions as a vending machine (all vending functions apply). A token is read via a reader connected to the PC (or the token 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 users 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.

14.2.8 Reports

A comprehensive separate reporting system generates reports from data setup and log files.
A report could be generated to the display, a printer or to a file or can be emailed automatically.
Reports (password per report) can be generated via any PC linked to the system and can be automatically generated on certain times of the day, on certain dates, when specified events/alarms occur or on operator request.

A report could be a simple extraction of data from a single database (e.g. list all users that belong to a specific department). Complex reporting extracts 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.
The operator could be requested for parameters.

Report forms are generated utilizing Seagate Crystal Report (Crystal Reports is not provided, the forms are). 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.

Who generated what report is logged.

14.2.9 SCS_Controller

This application executes as a separate program, linking to a CntrP via a second TCP socket.
It can detect all Softcon CntrPs on the local TCP network and links to a selected CntrP – showing the Mac, IP settings and node numbers.

The setup in the CntrP can be read and changed (written back to CntrP or saved to file).
Setting can be read from file, edited and sent to a CntrP (or save to file).
The IP settings and node number can be changed in the CntrP.

Changes to the CntrP are overwritten by the setting sent by the Server (main socket).

14.2.10 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 user). Users 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 users name and accumulated time.

ACCUMULATION

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

The provided accumulation functions as follows:

When a user enters via any reader in the system that is set as a clock-in reader, accumulation for that user starts and ends when the user 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 users with totals for the week or month respectively, are logged and cleared of daily and weekly or monthly totals. On other day ends, only user’s 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 user’s that have accumulation totals. These accumulation files contain the user number, and the current day, week and month totals and are used in generating accumulation reports.

Users that equal 24 hr accumulation for the day (which indicates that the user 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 (user entered).
Xref	user reference number (reference field in the user database CARD.MDB card_data.reference).
Employ	employment number.

Additional data for the user 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 token 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 user clocks in/out. The T&A system renames the file before reading the data.

14.2.11 User Access Zone Display

The application SCS_Zone.exe serves a terminal that user can badge tokens and view areas that the user has access to. The general user info - Employee and ID numbers, First and Surname, Mobile and Email and Car registration and the access info – Status, Time group, Issue and Expiry dates are displayed and all area zones the user has access to. The display is password controlled, en/disabling the edit of data and zones.

14.2.12 Vending

The vending option controls vending machines and Photostat machines via CntrP and Point Of Sale (POS) PCs. All functions are controlled via access tokens that request CntrP /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.
Items can be linked

Users 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 user, on periods set per user.
Reload time can be synchronized to time, date, day of week or month.
Users can optionally be allocated to cost groups that share token, value and subsidy.

Machines are interfaced to via CntrP with electro-mechanical interfaces or with serial interfaces (MDB protocols are accommodated as standard).
CntrP settings are

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.

14.2.13 Visitor Control

Controlling of Visitors is limited to two aspects, User access control and Visitor register system.

USER ACCESS CONTROL

Visitors are either issued tokens (or finger print registered) simply as staff by editing of the user database, or by a visitor registering system, which transfers visitor data to the user database. Once in the user database, the token is a normal access control token, adhering to all normal functions of access control, i.e. user 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:

Token Capture. Tokens can be set as capture tokens, to be captured at readers that have capture units. Tokens 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 user is set to capture at that reader, a control signal opens the capture bin and once the token is "dropped" in the bin, the portal is opened.
For tokens that are not to be captured, the reader functions as if no capture bin is present.
Tokens captured are logged as being captured and the tokens can automatically be disabled at the reader (set per reader), the user is disabled.

Link To Hosts. A visitor 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 if the host is present in the area to which access is requested. Should the host be a virtual user, the host token is used as a mask to find present users that match non zero settings (e.g. setting a dummy host user with department x and all other parameters to zero, access is granted to the visitor if any user with department x is present).
The PC grants access to user that are linked to hosts, i.e. visitor data does not reside in the CntrP 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 (token 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 visitor has access to. Any of the fields can be password protected, allowing only certain operators to change data (e.g. where the visitor has access to).
Editing aids described in the data display and editing section are available.

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 token (card) maker.

A fingerprint can be saved to be used for search when the visitor revisits.

The visitor data is copied to the active access user database by allocating an access token to the visitor. Data that was not editable is not transferred, facilitating the pre-setting of visitors with certain parameters (e.g. to where that visitor has access).
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 token number (if the function is enabled) or by presenting the token 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 user's 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 token maker. A token design is allocated to the visitor.

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

Operators can click on icons that generate event to open portals.

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

14.3 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 USER OUT-OF-AREA event is received from a CntrP and the user is checked as not out of area, a USER 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.
- CntrP — 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 user properties– status (en- / disable / capture), area group and time group.
  Changes are automatically sent to CntrP 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 users triggers referencing virtual users, use the referenced user as a mask to match user events tested as valid trigger (allowing specific users as triggers or a group of users).

Sequences are set to occur within set time-outs (HH:mm:ss) between events.
Sequencing can typically be set to require a sequence of tokens (specific and/or group) before portal open 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 users that are linked to host), access is granted or denied by the CntrP that contains a local database.

The CntrP report reader and I/O changes on active time groups.

14.4 OBJECTS / RESOURCES

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

14.4.1 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 portal 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 CntrP.
A timeout of 0 to 99 seconds can be set after which the change in count is reported by the CntrP (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.

14.4.2 Readers

The readers section above lists all readers that can be used in the system.

Readers connected directly to the PC (via TCP or USB) enters the token number to cursor (editing, searching). The Softcon interface CR395 converts any Wiegand, Data/Clock or Touch reader to serial / USB as required by the PC.

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

Biometric readers, connected via USB or TCP interfaces, are used to register the templets.

The PC maintains the token and templet database in each CntrP and biometric reader.

Every CntrP reader is set with a name and allocated to an appropriate port on a CntrP.
All setting as listed for reader in the CntrP section is set and sent to the CntrP.

14.4.3 Schedules (Time slots and groups)

Time related functions (e.g. when access is granted) are set via time groups.
There are up to 128 groups with up to 32 time slots (start and end time).

A group is set active for time slots 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.

Users 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 users 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.

Time Slots and Groups allocated for Access, to Readers, Inputs and Output (when used, when reported, when active) are sent to the CntrPs (license keys set the number of slots and Groups in each CntrP).

14.4.4 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.

14.4.5 Input / Output
Every input, output and level is set with a name and allocated to an appropriate port on a CntrP.
All setting as listed for I/O in the CntrP section is set and sent to the CntrP.

14.4.6 SMS
Message are set that are sent as SMS messages to mobile 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. CntrP number and CntrP name). SMS activities are logged as events.

CntrPs with GSM modems connected can be configured to send SMS messages directly for event and reports (see CntrPs above).

14.4.7 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.

14.5 USERS (PROFILES)

The number of users in the system is configurable.

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

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

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

LOCATION, TIME. The current location of the user (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 user 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 user 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 mobile 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 tokes). See additional setting for access control.

- **Area groups**, **slots** added and deleted when user has expired and when either of the user counts are not available (full or empty), set where the user has access to.
- S**tatus** (disabled, enabled or capture) is set for normal operation, when expired and when the user counts are not available.
- S**tart/expire** time-dates set when the user 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 token is captured.
- **Time Group**. Defines when a user may be granted access.
  One of 128 time groups are selectable (each with 8 time slots), 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 user's area group is used.
- **Inactive**. An inactive time-date period can be set per user.
  When last movement exceeds the time-date period, a different user status setting is used (e.g. the token could become a capture token).
  Area zones can be added and deleted from the user's access zones when not active is not within the inactive time-dates.
- **Zone Counters**: Each user 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 user status is used, and area zones can be added or deleted from the user's area groups.
  A count period is set per user and the period counter is automatically re-loaded when the token 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 token numbers can be set for a user (e.g. prox and MAG card).
  These numbers are the true number encoded in to, or on to the token.
  Readers are set to which token number must be used (e.g. a holder could have a PROX and a MAG tokens).
  Using master user link (see below), a use could have multiple tokens.
- **Pin code**. A 1 to 6-digit pin number can be allocated to tokens when Pin Pads are installed.
  Depending on the set-up of the Pin Pad and reader time groups, access is via either token or pin code or both. Users set with a pin code of zero gain access only by token and no pin is required.
  A duress alarm is generated (access is granted if the token normally has access) when the code is entered proceeded with a zero digit.

- **Pass back**. A user set as for pass back, overrides APB, i.e. the token can be used for multi-access to the same area zone without the requirements to exit the zone (as is required for APB).

USER DB LINKING.

A user can be linked to multiple user in the Db.

- **Linked to**. The user can be linked to a host user; 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 users linked to hosts is by the PC (data not in CntrP).
  If the host user is a virtual user, it is used as a mask to find uses present that match non-zero settings of the host user.
- A **control group** links the user to a user that serves as group control – user settings of zero use the corresponding settings of the linked group control user.
  For example, users belonging to a trade specific trade union are linked to a specific user control group, with the user setting for status (en- disable) and area group set to zero, thus using the users control group settings and should the trade union be "locked out", only the area group and status of the user control group is changed.
  Any user in the database can be used as a user control group by setting the virtual user option (token is not set to CntrP).
- A **master user** links the users to a master user (used to give a user multiple tokens) **-** user settings of zero use the corresponding settings of the linked group control user.
  Typically, a user linked to a master user only has the token number set.
  Whereas control group are set as virtual, a master user is not a virtual user and can be used as an access user.
- **Temporary user link** (typically used when a user has forgotten token at home):
  A user can be linked to a temporary user and while the temporary user has a master user link back and the temporary user status is enabled, the master user is automatically regarded as disabled (the set status is not changed).
  The temporary user functions as a user with a master user link and typically only has a token number.

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

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

TRIGGER GROUP. Selects a group that is added to the users 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 user 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 user can be enabled or disabled from clocking.

COUNTERS. Two counters are available for a user, an overall counter and a period counter (which limits entries within the period set for the user).
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 users set limit, area zones (via an area group) can be added and deleted from the user's access zones and an alternative user status is used.
The users available period count is automatically reloaded when the token 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 token number the user used and is only used for documentation purposes and does not affect the functioning of the system.

VISITOR REF. If the user is a visitor, as entered by the visitor system, the last visitor reference (i.e. the visitor that last was allocated to use the user) is displayed. If a normal user, 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 user (typically when a medical license expires, access is denied to certain areas).

VEND DATA. Token, subsidy and values are used in POS and vending applications. Amounts available, remaining and periods are set per user. Users 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 token is presented to park display, park pay and park exit readers.

14.6 BLOCK LISTING

The block listing (blacklist) database contains profiles that are flagged as ‘undesirable’.
When these profiles are entered into the visitor or user databases - these are highlighted in red.
The ID number is used as the data to identify the block listed person.
Date/time when blocked / unblocked are set.

14.7 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. user’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.

14.8 INTERFACING TO HOST PROGRAMS

14.8.1 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).

14.8.2 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 user database directly and mark the record as changed, resulting in the update of remote PC databases and CntrP. 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 user database and to the area zone-group database (setting where users have access to). When run, all databases are updated accordingly.

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

14.9 BACK-UP STORAGE DATA

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

14.10 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 SLAN CntrP. Access to more options is via appropriate keys.

The included column indicates which SW packages (may require additional CntrP 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 users.	1, 2, 3
Asset Track	A future option of linking asset tokes to users 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 users 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 CntrP 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 user edit, card maker or visitor capture menus.	C, 2, 3
Photo display	Enables user photos to be displayed in drawing, card maker or user 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 users to be linked to host users (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.

14.1 VIDEO LINKING, VIDEO /CAMERA CONTROL

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

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

The system can be set to link TCP cameras to I/O and reader events, resulting in:

- Snap shots store, optionally with database information (typically user's name, reader name) imposed over the photo.
- Video display on drawings.

14.2 CONTROL VIA WWW

Remote sites are interlinked via TCP networks and can be on-line or synchronized via distribution server.
PC applications such as Remote Desktop can be used to access remote sites.
The Visitor Scan system is web-based.

- A full web-based system will be available in the future.

14.3 OPERATOR INTERFACE

14.3.1 Security Levels

Any number of operators can be set as members of multiple operator groups. Operator 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.

Operators can be set with start and expire date/times. Passwords can be set to expire, forcing the operator to change password. Logging off reverts to a default group whose access rights are configured. Operators 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 operator. 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.

14.3.2 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.

14.3.3 Data Display and Editing

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

All set-up and user 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 operator.
- 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 colour 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, user 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. user data is divided into 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 user/users) or paste record or field(s) from clipboard or selected user.

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 token / 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, tokens and barcodes are read to find users and items and used to edit token 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 token reader can be used.

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

14.3.4 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 token 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 portal opening, not closing).
- Displays can be time selected (e.g. certain portal openings are only displayed after hours).
- Settings are available to select which PC(s) activities are to be displayed.

14.3.5 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. portal 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 tokens presented to readers.
- Clicking on certain display items can generate events (e.g. disable a reader, open a portal), 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 operator 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.

14.3.6 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 colour 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.

14.3.7 Operator Occurrence Log

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

14.3.8 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.

14.3.9 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.

14.3.10 Wizard

SCS_Wizard is a SoftWin3 add-on application that configures or reconfigured SW3 list and property displays.

- This is done According to general configuration selections and included pre-configured files.
- And is Applied to selected list displays and property sheets.
- All unused parameters are hidden.

Typically

- Use End Of Line cable detection
- Not use Portal sense (Action complete)
- Configure Mantrap

DEFAULT OPTIONS.

- A variety of optimally configured default display options are included with the Wizard

Typically

- Activity displays for access – specific a token, for a department, biometric readers, a zone or readers.
- Alarms in displayed red, Access control events in green.

Functions such Copy of a controller setting to another controller is integrated in SW3

Typically

- Mantrap settings to another controller.

15 TESTING – SIMULATION AND MONITORING

15.1 HW OFF-LINE

All CntrP and modules have SW versions for testing (a different EPROM version) and are used to test all functions of the CntrP 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.

15.2 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 SLAN.
- 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 CntrP 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.

APPENDIX A - TERMS AND DEFINITIONS

Terms and definition are set to match the IEC62642 standards – abbreviations are added in brackets to simplify the document. Highlighted data below are used by Softcon and not defined by IEC62642.

access Control System (ASC)
part of an access control system that interfaces with readers, locking devices and sensing devices,

access Control Unit (ACU), Controller (CntrP)
part of an access control system that interfaces with readers, locking devices and sensing devices, making a decision to grant or deny access through a portal

access level
set of rules used to determine where and when a credential has authorized access to one or more portals, and which may include special passage conditions such as specific portal allowed open times

access point, portal
physical entrance/exit at which access can be controlled by a door, turnstile or other secure barrier

access point forced open, portal forced open (illegal open)
alert signal generated when an access point is opened without access being granted

access point locking device portal locking device (lock, latch)
assembly associated with the access point, which performs the function of holding an access point in the closed position and capable of releasing the access point in accordance with pre- set rules

access point open time, portal open time (lock tmout)
maximum time an access point door may be held open after access is granted and before an access point opened too long alert is generated

access point opened too long, alert portal opened too long alert (open too long)
signal generated when an access point open time is exceeded after access is granted

access point sensor, portal sensor
electrical component used to monitor the open or closed status of an access point, or locked/unlocked status of a locking device, or the secure/unsecure status of an electromagnetic lock or armature plate

access request
reading of a credential at a portal initiating the decision process for granting entry to or exit from the area controlled by the portal

anti-passback (APB)
operating mode which requires user validation when leaving a security controlled area in order to be able to re-enter and vice versa

anti-passback overriding, anti-passback disabling
system feature disabling the anti-passback

authentication
process used to verify the integrity of the recognition of credentials

biometric(s)
any measurable, unique physiological characteristic or personal trait that is used as a credential to recognize and verify the identity of an individual's dynamics

blocked access
passage through an access point is prevented even when valid credentials are presented

credential
information either memorized or held within a token
number from reader / device to identify the user

dual credential, multiple credential
function of electronic access control systems, which requires two or more sequential authorised access requests within a configurable time period to grant access

duress alert
function of an electronic access control system related to the silent warning initiated by system users entering a duress code when subject to coercive activity in order for unauthorised persons to gain access

elevator control
function of electronic access control systems restricting the use of lifts or elevator cars

event
change occurring within an electronic access control system
any change in the CntrP

man trap
combination of two or more portals required to be used in sequence in order to gain access to a security controlled area

release time
period of time access points unlocked by the system according to pre-set rules

request-to-exit device (REX)
device local to an access point used to initiate free exit

stand-alone mode
mode of operation of the access control system without the communication between the access control unit and monitoring console

tampering protection
method used to protect an access control system or part thereof against deliberate interference

timed anti-passback (ATB)
system feature which traces an individual credential access request to a given area for which an access granted was not followed by an exit granted, or an exit granted was not followed by an access granted within a predetermined time period

time slot (was time zone, Ts)
interval of time between two given moments indicating the beginning and the end of a valid period within a time zone

time zone (use time group, Tg)
one or more time slots combined with calendar information

token
portable device containing a readable unique identifier (credential) that can be associated with a user's data and access rights stored within the electronic access control system (includes cards)

user
person requesting access through an access point