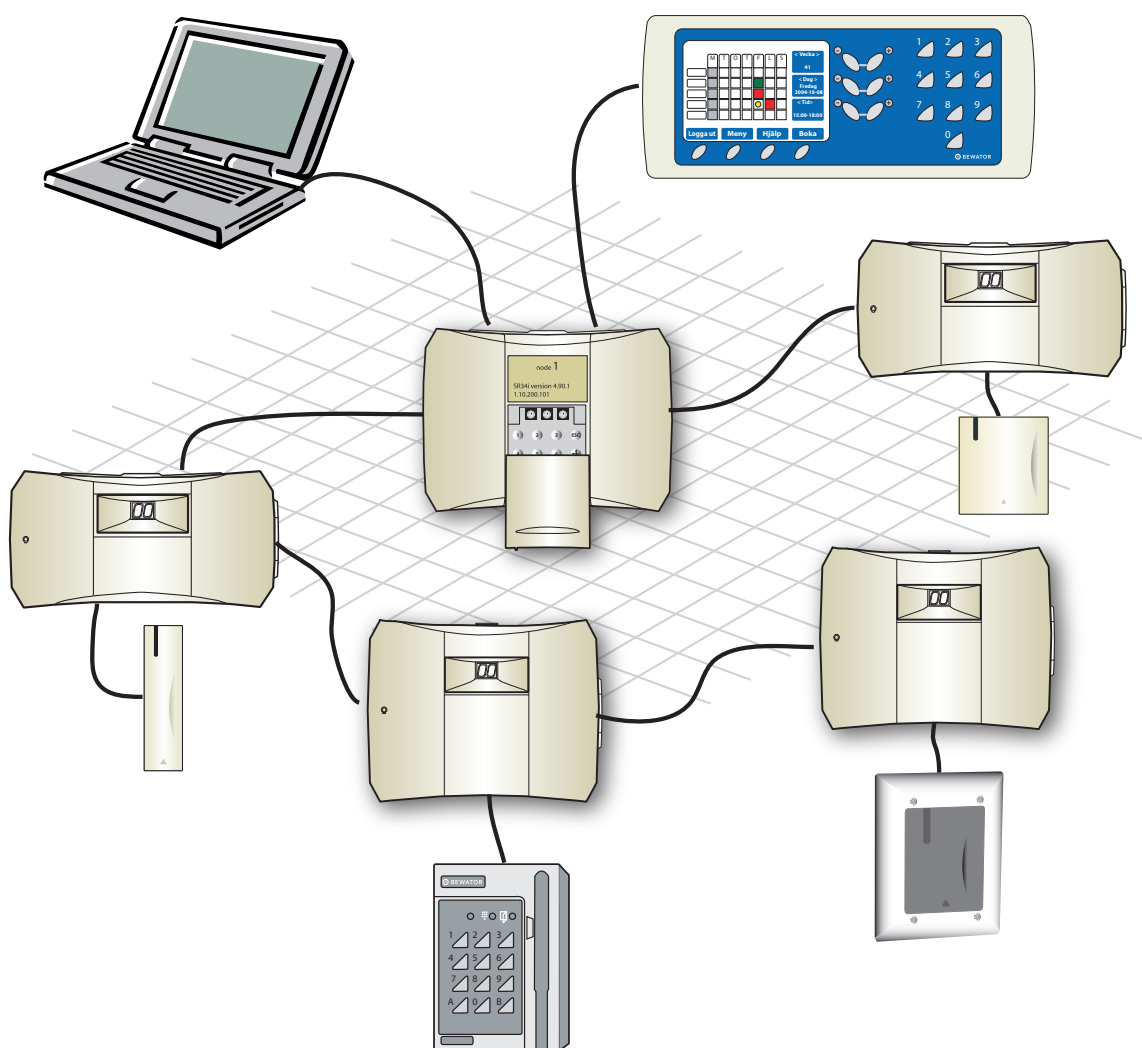




Bewator Entro

Project Design Manual

EN



BEWATOR

A Siemens Business

Copyright © 2006 Bewator AB, Solna.

Material from this document may only be copied with the consent in writing of Bewator. Bewator reserves the right to alter both the content of the manual and the design of the product.

Document number: **81184-10b Entro 5.1Proj-EN**

Bewator AB develops and markets a complete security product range that includes access and alarm management systems. Sales, installation and servicing are handled by a national dealer network.

Actions (such as unauthorised manipulation, copying etc.) must not be carried out with the software contained in the products and systems. Such actions are regarded as copyright violation and may result in imprisonment or fines and may likewise lead to an obligation to pay damages and compensation for using the software.

Content

How to plan a Bewator Entro System	5
Where to find more information?	5
Method	5
Media (type of cards/tags)	6
Security levels	6
What is Bewator Entro?	7
Small applications – without LAN	7
Larger applications – with/without LAN	8
How to communicate between units?	10
Advantages and disadvantages.....	10
Designed housings	11
Cables	12
Cable for power supply.....	12
Cable for RS485.....	12
Cable for network (TCP/IP).....	12
Cable to PC	12
Earthing & screening for RS485.....	13
Power Supply.....	14
Local Power Supply	14
Central Power Supply	15
Voltage drop	16
Example of an insufficient dimensioning.....	17
Example of correct cable sizing	18
Several power supplies in the same cable section	19
Alarm Control.....	20
Monostable alarm by-pass	20
Bistable alarm control (level or pulse)	21
Alarm zones	21
Alarm indications.....	22
Intelligent Alarm status feedback (ASF)	23
SR34i Segment Controller	24
RS485 – in two levels	24
Ethernet and LAN	24
SR34i – different capacity.....	25
SR32, SR32i or SR34i?	25
Door environments.....	26
Proximity or magnetic card reader – or both?.....	27
BCLINK or CLOCK&DATA interface.....	28
Compact or split mount?.....	28
Door Monitoring	29

Motor lock and lock strike plate	29
Functions in the IOR6.....	30
Common alarm	30
Emergency exit.....	30
Power failure warning	30
Timer controlled	30
Machine & door control in Reservation	30
Lift Control.....	31
Example.....	31
Software.....	32
Several PC's on the same site	32
Reservation system.....	33
Necessary components.....	34
Web browser or touch-screen terminal.....	34
InfoPoint IP811/IP810 Reservation terminal.....	34
Machine and door control	34
Example 1 – three doors without LAN.....	35
Suggestion	35
Example 2 – three floors with three SR34i (without LAN)	36
Suggestion	37
Example 3 – LAN in same property	38
Example 4 – a LAN system located both inside outside the property.....	39
Security aspects.....	39
Suggestion	40
Example 5 – Reservation system	41
Suggestion	41
Example 6 – two PC in the same network.....	43
Advanced information about LAN.....	44
What redundancy is there in the system?.....	46
Technical data.....	47
Notes.....	52

How to plan a Bewator Entro System

The Bewator Entro Access Control System is designed to be easy, safe and convenient to use. The same applies for the planning and installation of the system.

Years of experience of working on functions, user-friendliness and preventive service aspects are built into different parts of the product.

This means that system planners find it easy to separate the different concepts such as cabling, power supplies, control units and door environments (readers). This makes for a strong, effective modular concept!

Focus is concentrated on the End-Users by using Bewator Entro it is very easy to fulfil their requirements at a reasonable price.

NOTE! The description of the Reservation system in this manual applies to the Bewator Entro software version 5.0 - onwards.

Where to find more information?

You will find more information on specific functions and how to install and programme Bewator Entro in the following documentation:

- Bewator Entro Installation Manual.
- Bewator Entro User Manual.
- Technical Installation notes for each product (e.g. readers).

The best way to find these is on the Bewator web site.

Method

As with all security systems the goal is to prevent unforeseen events. This can be achieved by minimising risks, but also by achieving a way of finding out what has happened, and where.

When starting a security project it is advisable to investigate the existing situation for the facility project. Investigate the level of potential infringement and any consequences. What type of locks and keys are used? Are some doors locked and not in use? Who should have access to which doors? Etc.

This includes knowledge about the buildings' external and internal doors, which may require dedicated access by certain people. An example of this is in computer rooms. Where and when people have access to the building must be determined.

Other functions such as the need for integration of an existing intruder alarm system, door entry phones and visitor management should all be taken into account at this stage. As soon as the system needs are outlined, the planning of Bewator Entro can begin.

Media (type of cards/tags)

Access control systems differ from codelocks, as every individual using the system must have their own identity. There are two main ways of achieving this – by using **magnetic** or **proximity cards or tags**.

The application area is wider for the use of proximity cards. For example when gaining access to apartment blocks, using proximity cards can be seen as an advantage. This is because of the more robust handling of the cards and readers due to the lack of mechanical parts. The Bewator Entro system has built-in solutions for both types of reading technology and even a combination of both card and pin!

It is the buyer/end-users decision as to which option to use. They must also consider which door(s) will require PIN-codes, which can also be used to activate or deactivate intruder alarms.

For more information on specifying suitable readers. See chapter *Door environments*.

Security levels

The security level determines what action is needed to open a door. See security levels below:

- **Door unlocked.** The door is unlocked.
- **Group code.** The door can be opened using a four-digit code, shared by a group of people.
- **Card only.** To open the door, a personal access card should be swiped through the card reader. If the card is lost or stolen it is easy to cancel the card.
- **Card + PIN.** The door is opened when the access card is swiped and a personal code belonging to this particular card has been entered.
- **Toggle – Group code.** Similar to Group code above. When the code is entered the first time, the door is opened and remains unlocked until the code is entered the second time.
- **Toggle – Card.** When the card is swiped the first time, the door is opened and remains unlocked until the card is swiped the second time.
- **Toggle – Card + PIN.** When the card is used and the code is entered the first time, the door is opened and remains unlocked until the card is used and the code is entered the second time.
- **Accompanied Access Card.** Two people, each swiping their cards within 15 seconds, are needed to open the door.
- **Accompanied Access Card +PIN.** Two people, each swiping their cards and entering their codes within 15 seconds, are needed to open the door.
- **Closed door.** The door cannot be opened by the card reader, but only from an exit request button from the inside.
- **Locked door.** The door is completely disconnected from the system, which means that not even exit request operates.
- **Personal code without card.** Bewator Entro can be set so that users may choose a PIN code instead of a card. This will disable the Group code operation.

Using the security levels, you can determine the suitable type of protection for your property. During the day, when there are people in the property, Group code or Card only may be sufficient. During the night, the Card + code security level is often more suited.

What is Bewator Entro?

The system below is shown on three levels:

- **PC** (with software) to send/receive information to/from the system via direct cable or network.
- **SR34i** controllers hold information and make decisions as to the access granted at the doors.
- **Door environments** where door controllers, readers, keypads etc. are installed together with electrical locks.

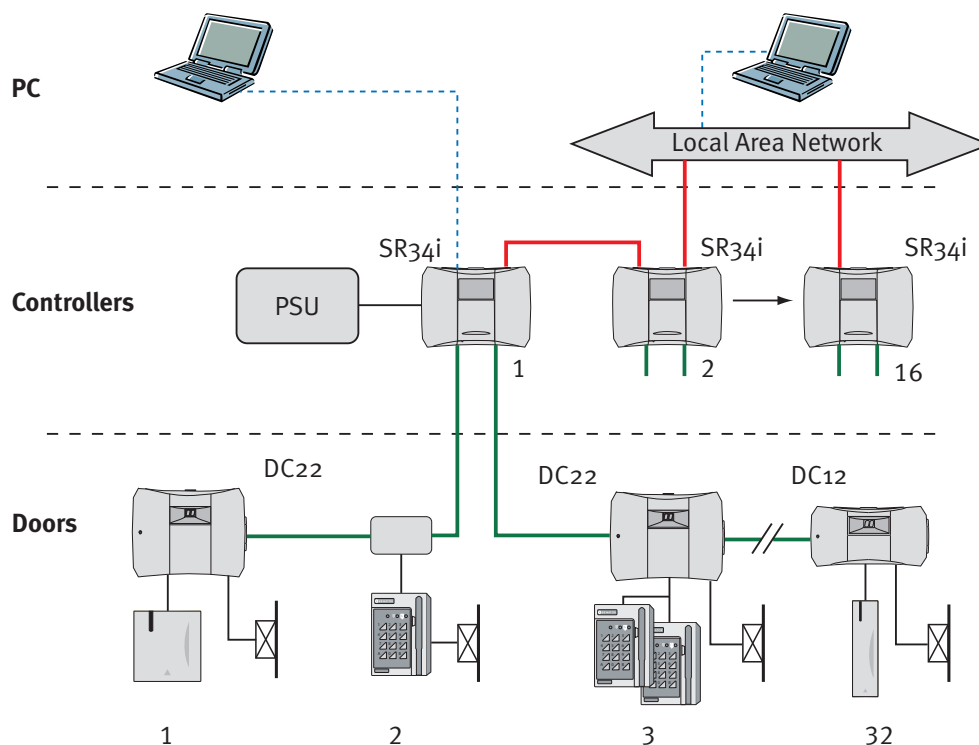


Figure 1 - Different levels in Bewator Entro

A site could exist using up to 16 different SR34i with 32 door environments each.

Small applications – without LAN

Bewator Entro is designed for use in smaller applications with only a few doors. The figure above shows a site with local area networks (LAN) and several controllers – but might also be used with only one SR34i without LAN. It is still very easy to configure a complete system.

Other than correct planning it is often necessary to take use of some dedicated cabling. You do not have to consider LAN, IP-addresses etc.

You just need some metres of cable, an SR34i, a Power supply and readers! It's as simple as that!

Larger applications – with/without LAN

Bewator Entro has the capacity of handling up to 512 doors and 20 000 people in the same system (database).

In addition one PC can manage up to 1000 similar systems – via modem and/or LAN. These systems consist of separate, unique databases. They can however, be controlled and stored on the same PC.

The access control system should include one or several properties placed in different localities.

- When one premises has many doors you can still use dedicated cabling. The system is split into separate sections managed by its own SR34i Segment Controller. This handles a couple of doors (local bus). All sub-systems are then linked into a higher level of communication (global bus). See Figure 2 - *Facility with RS485 cable*.
- When several properties exist in the same system, a LAN may be considered. Note that the numbers of doors cannot exceed 512.
In this case the **global bus** will be connected **via LAN** (TCP/IP) but each SR34i controls “its own” doors locally.
A combination of the two communication methods can also be possible as **only one SR34i** in the facility uses LAN whilst the others connect via traditional cable. See Figure 3 – *Both TCP/IP and RS485 use global communication*.
- In some cases only a central PC can manage different, unique systems in different facilities. This can be obtained via modem or LAN. See Figure 4 – *Network connected PC for two separate Bewator Entro*.

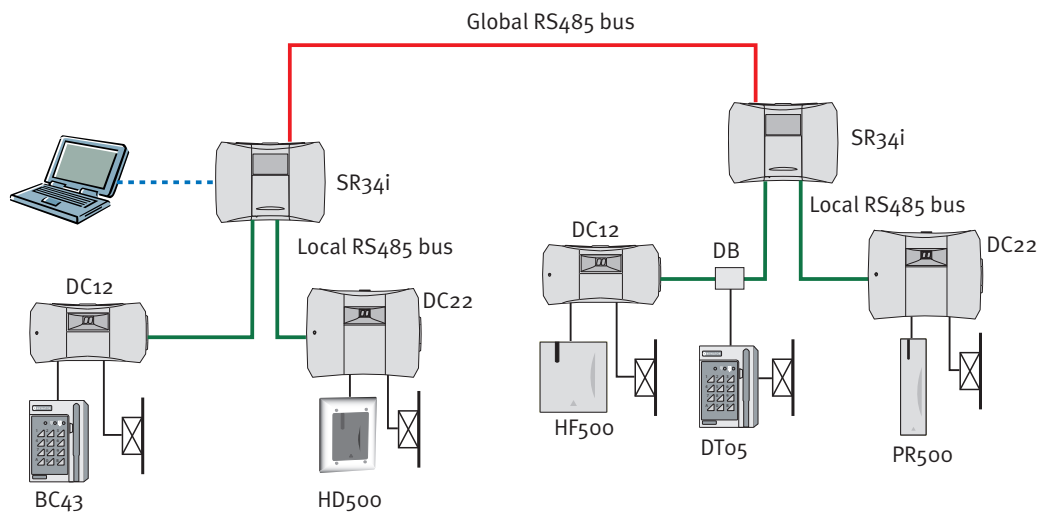


Figure 2 - Facility with RS485 cable

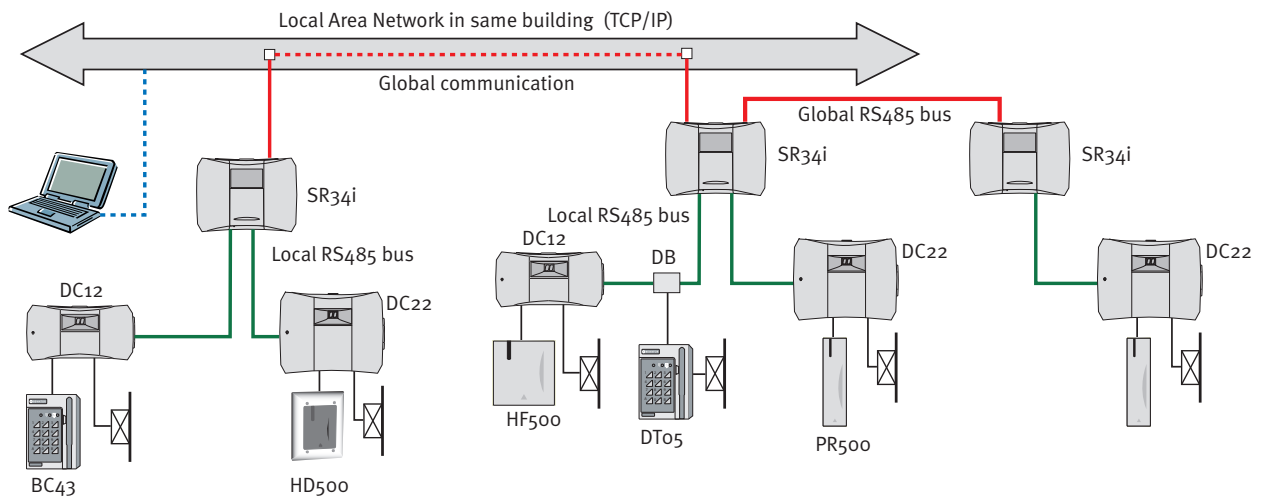


Figure 3 – Both TCP/IP and RS485 in global communication

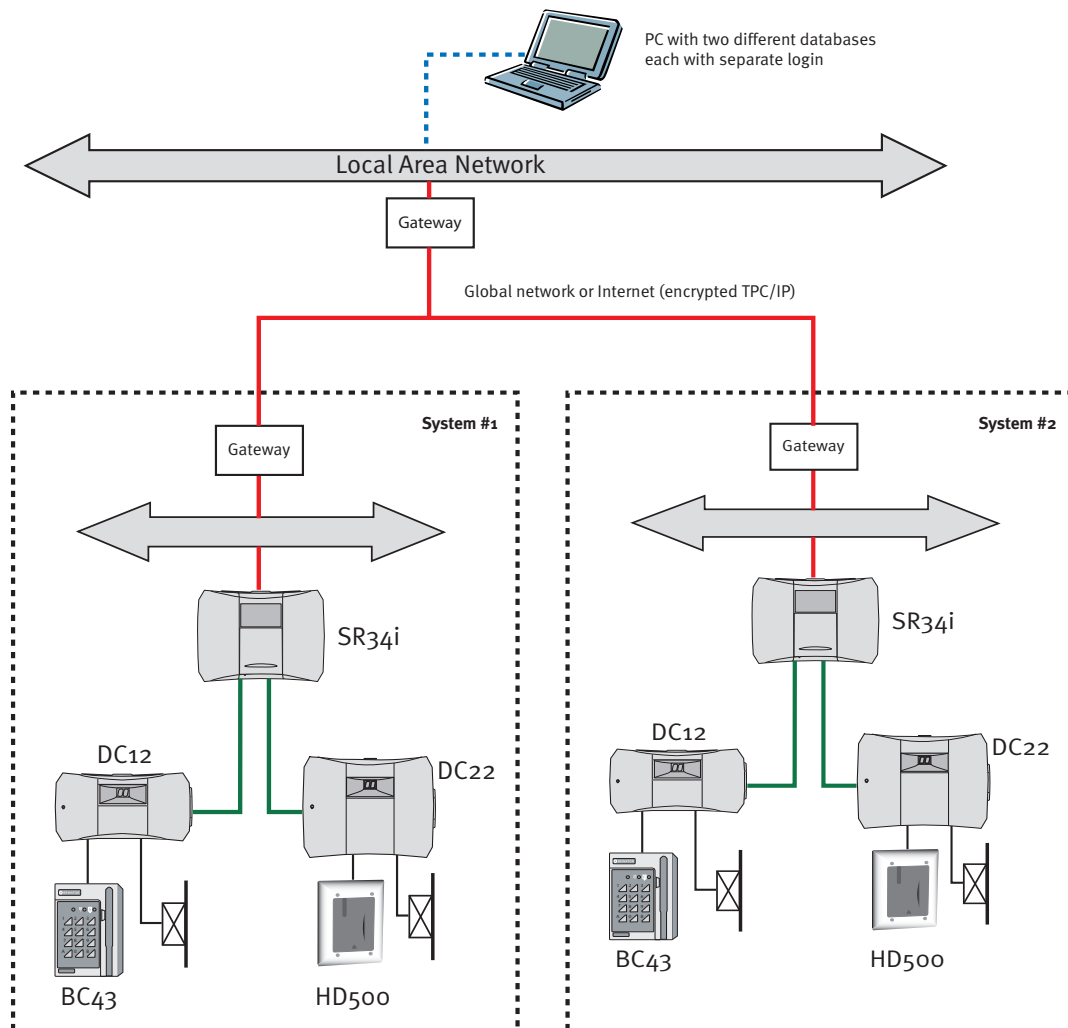


Figure 4 – Network connected PC for two separate Bewator Entro

How to communicate between units?

Bewator Entro version 5 onwards communicates on three levels:

- 1 Between the site and one (or more) PCs.
 - RS232 direct serial (< 25 metres).
 - Local Area Network TCP/IP (10/100 Mbit).
- 2 Between SR34i Segment Controllers.
 - Global RS485 bus (<1 200 metres).
 - Local Area Network TCP/IP (10/100 Mbit).
- 3 Between SR34i and its door environments (door controllers/readers).
 - Local RS485 bus (<1 200 metres).

Different combinations of the above are possible. See chapter on: Cables for choice at different methods.

Advantages and disadvantages

Level and method	Advantage	Disadvantage
RS232 (to PC)	Auto detection between PC and hardware. Electrical contact with only one PC.	Short distance. Normally max 25 metres.
TCP/IP (to PC)	Only the network itself restricts the distance. (Around the globe!). Isolation between PC and hardware. Faster data transfer. Existing cables in the facility often work.	Slightly more parameters to set in PC and SR34i. E.g. the IP-address. Networks may have scheduled or accidental communication failures.
Global RS485 (between SR34i)	Dedicated communication between segment controllers – higher security. Easier to set up.	Expensive to install new cable. Restricted geographical area (max 1200 metres).
TCP/IP (between SR34i)	No theoretical limit of the distance. Isolation between different sections of the site. Internet (e.g. Reservation system). Network cables are often already installed in the facility.	IP-address has to be programmed. Networks can have planned or accidental communication failures.
RS485 (to door controllers)	All installation is done locally in the door environment. Power supply is available in same cable.	

Designed housings

The new Entro components have a new, designed housing offering an even easier and nicer installation. The different components have several nice features but the most important details are:

- Special corner elements are designed to be removed but then again hiding and sealing the cable entry when re-fixed again. Also ideal when mounting via trunking-list. See figure 5.
- Secured cable entry can easily be achieved by entering the cable over edge (before the corner elements are re-fixed). See figure 6.
- The cable entry can be solved in many ways. There are knockouts in both the base and the corner elements. See figure 7.
- Integrated fixing details for securing the cables with cable ties.

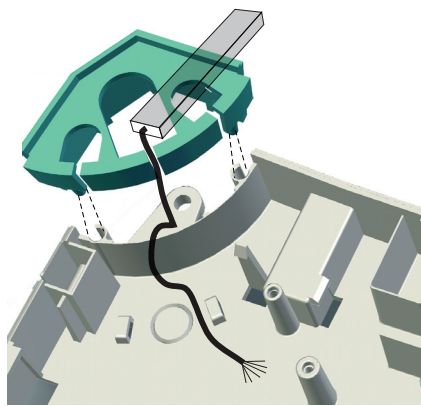


Figure 5 - With trunking-list

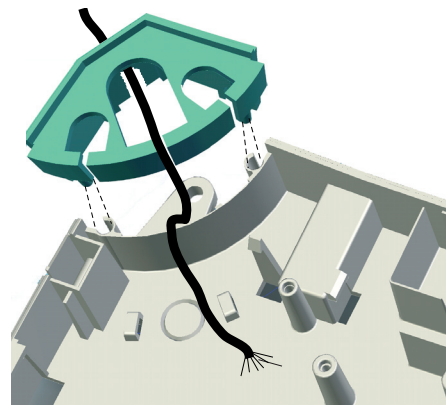


Figure 6 – Secured cable entry over edge

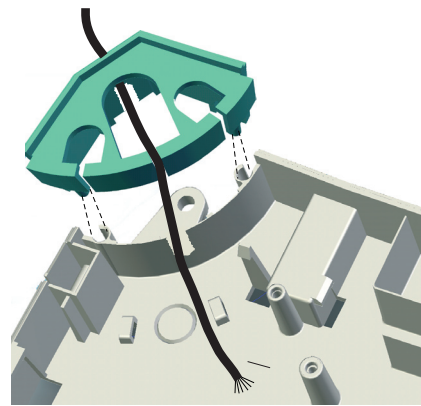


Figure 7 – Cable entry via knockouts

Cables

Bewator Entro can be operated using different cable types for the communication levels, as well as for the power supply.

Cable for power supply

In both large and small systems it is important to use the dimensioned cable correctly. The most important factor to consider is that the cable is linked to the door environment. In most cases it will be the electrical locks that will consume the most current and could cause a drop in voltage. This is why it is necessary to know the types of locks; (lock strikes, motor locks etc.) when dimensioning the cables.

In most access control systems there are some kind of centralised power supplies such as battery-backup. When using these methods it is very important that there is a large enough area of cable. We recommend an area of at least 1,0 mm².

This will exclude data cables such as ELAKY, Belden etc. as they have areas around 0,1 – 0,2 mm² and will not fit the purpose of a power supply. A popular cable is Bewator "combi-cable", which is a PAARFLEX with 2 x 1,5 mm² (also with a pair 2 x 0,5 mm² aimed for data communication).

See more in section Power supply for advice on how to plan the cable network.

Cable for RS485

Between SR34i's and door environments, cable should be specified for RS485. It is important that the cable is screened and twisted. In both cases the maximum length is 1200 metres.

If each SR34i is powered by its own power supply, only a simple data communication cable between them is sufficient. E.g. the Bewator-cable, ELAKY, Belden - or similar.

However - if two SR34i's are to be powered from the same supply another pair of cables are needed. The Bewator combi-cable is sufficient. It is also available with two pairs of communication wires.

Cable for network (TCP/IP)

If LAN is used as a communication between a PC and a SR34i – or between SR34i's – some existing LAN cable will suffice. **Cat-5 cable** (specified for 10/100 Mbit) is mandatory.

Note that the **SR34i have an integrated network switch** with two external connections and one internal for SR34i. This means that you can use a standard network cable – without any hub – direct to PC and/or local area network.

Whether new or old cables are used the customer's IT-manager must be consulted when specifying the system. This is also advised when starting up the system.

Cable to PC

Between the SR34i and the COM-port on the PC a straight RS232 cable is used. For LAN use a common, standard LAN cable (Cat-5 Ethernet).

Earthing & screening for RS485

The cable screens on each circuit must be connected to the protective earth, but **only in one place in the system** (see picture). Also remember that metal parts in doors or vehicle barriers can be in contact with earth. For readers installed on these surfaces, the screen must not be connected to the metalwork.

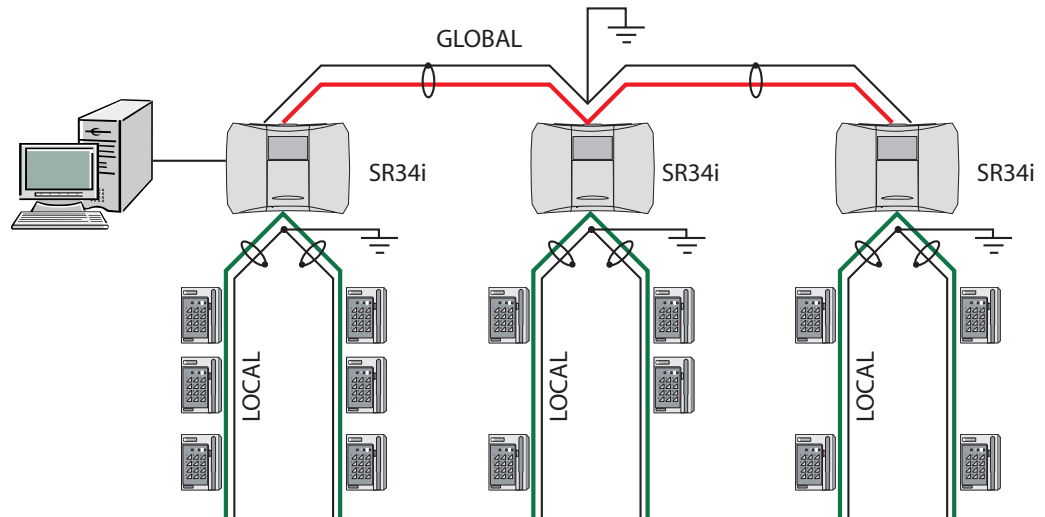


Figure 8 - Connection of screen

Power Supply

Powering Bewator Entro is covered in a separate section. Embedded power supplies etc. are not to be considered.

Overall standardised power supplies (usually 24V DC or 12V) and cable can be used to fulfil the requirements.

Local Power Supply

By using separate Power Supplies for Bewator Entro it is very important to wire all minus (0V) cables together. This is because the **RS485 communication interface uses the minus potential** as a reference. If there are voltage differences between the units there might be unwanted disturbance of the communication.

Be sure that the PSUs have a stable voltage output. Even if the Bewator Entro system components are tolerant to voltage fluctuations, the locks may be more sensitive.

Also remember to use enough area of the power cables – especially if there are long distances involved. Please refer to further chapters to get an idea of what happens when poor dimensioning occurs.

Below is an example of a 12V application where the SR34i is powered with a local supply.

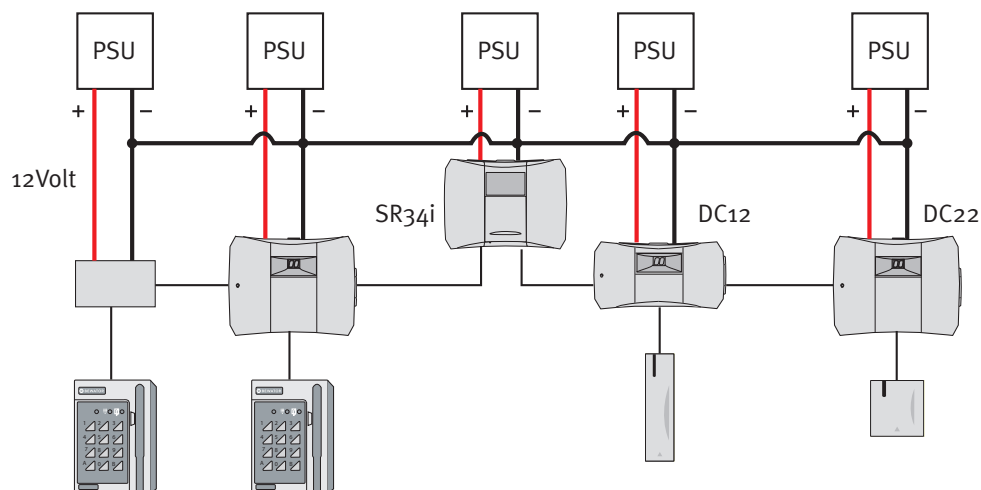


Figure 9 – Local Power Supply

Central Power Supply

As stated previously, central power supplies are often used to power an access control system. Bewator Entro is no exception. Here are some advantages:

- Stable 24 (or 12) Volt to electrical lock (which normally only accept +/- 15 %).
- Backup power for locks when main voltage falls.
- An alarm can be generated if main voltage falls and battery powering starts.
- Fewer units to install.
- Easier to expand the system (if enough margin from the start).

NOTE! SR34i has a lithium battery that keeps data when power disappears.

The main idea is to form a system such as that illustrated in figure below, where every segment is powered separately. If this is achieved the risk of earth current is minimised because the only existing link between the segment controller is a galvanic, isolated RS485. Note that also TCP/IP LAN means isolation between SR34i.

The following chapter describes more about specifying a correct and secure power supply. The examples are calculated for 24V but this can be applied to any power supply.

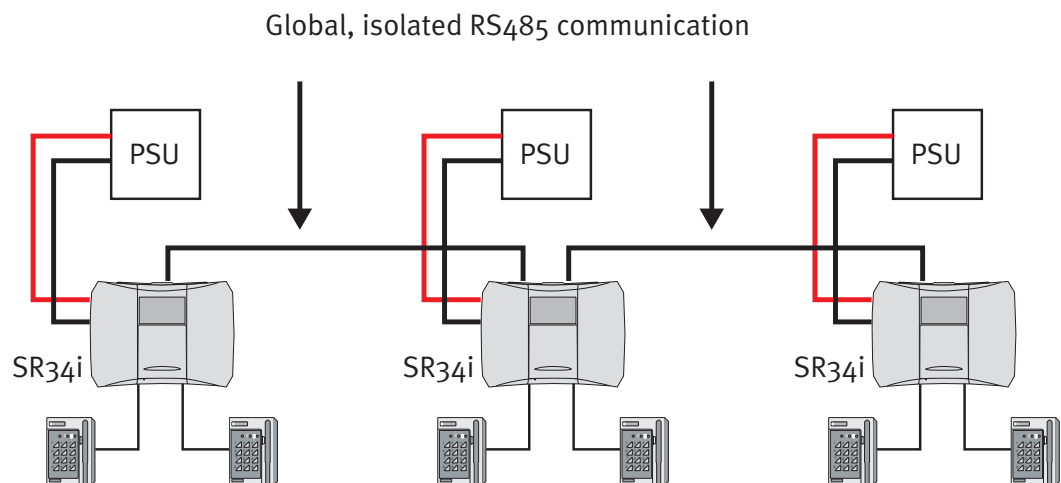


Figure 10 - Main principal for central Power Supplies

Voltage drop

Bewator Entro tolerates voltage levels down to approx. 10V DC for working whilst a 24V electrical lock might have a tolerance of maximum +-15 % which means that the voltage cannot drop below 20,4 V DC.

The calculation of voltage drop in cables is achieved by using Ohms law, which states:

$$\text{Resistance (Ohm)} \times \text{Current (A)} = \text{Voltage (V)}$$

The parameters affecting the voltage drop are as follows:

- Current consumption at each unit (Ampere)
- Cable area (mm²)
- Length (metre)
- Resistance factor for chosen cable (ohm/m)

It may be easier to understand voltage drop by using a simple example.

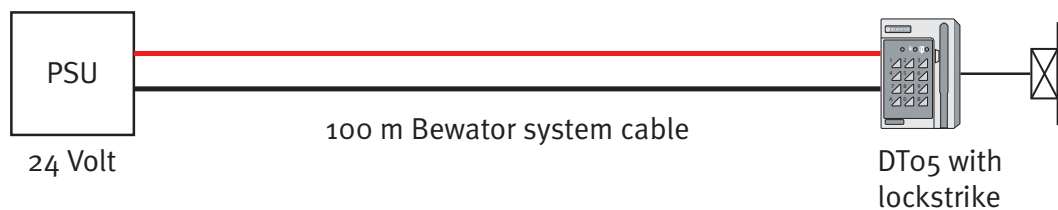


Figure 11 – Example of cable

Method of calculation

Current consumption at reader + lock (Ampere) = 0.075 A + 0.1 A = **0.175 A**

Cable area (mm²) = 1.5 mm²

Length (metre) = 100 meter x 2 (both directions) = **200 metres.**

Resistance factor for Bewator cable (ohm/m) = **0.0112 ohm/m**

Resistance: 0.0112 ohm/m x 200 m = 2.24 ohm

Current: 0.075 A + 0.100 A = 0.175 A

Result: 2.24 ohm x 0.175 A = 0.39 V voltage drop. I.e. 24.0 V – 0.39 V = **23.61V** at lock. This is sufficient for a 24 Volt electrical lock.

Result with 12V power

In many cases a 12V application consumes more current than in the case of 24V. With this in mind we assume that these units need 0.35 A.

Result: 2.24 ohm x 0.35 A = 0.78 V voltage drop. I.e. 12.0 V – 0.78 V = **11.22V** at the lock which still is sufficient.

Example of an insufficient dimensioning

To see the effects of insufficient dimensioning, we can assume that the same cable, readers and locks are used as before, but more readers are involved.

NOTE! Always calculate with nominal battery voltage 24V (or 12V) despite the battery back-up, output voltage may be higher – and maximal load at the units.

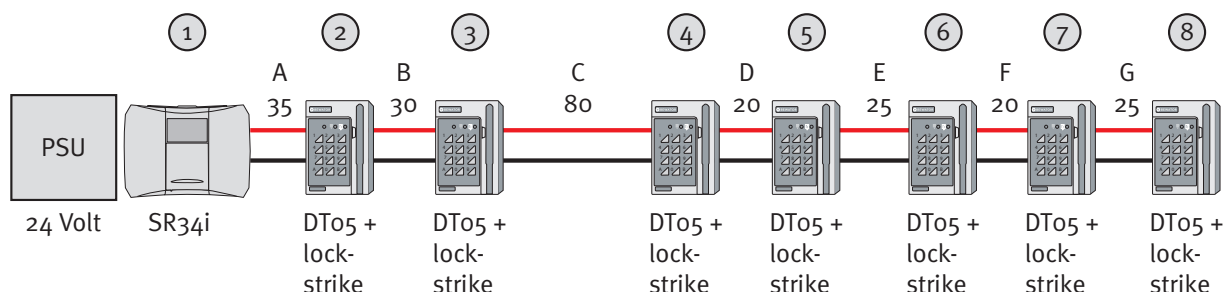


Figure 12 - Insufficient dimensioning

Method of calculation

1. Calculate the total maximal **current** (I) at each unit.
2. Calculate the **resistance** (R) for cable. E.g. 1.5 mm² Bewator-cable (11.2 ohm/km * length * 2).
3. Calculate the **voltage drop** (V) in each cable section (A, B etc.).
4. Reduce the voltage from battery backup at each unit.

Result with 24V system:

Unit:	1	2	3	4	5	6	7	8
Current (approx.)	0.250A	1.225A	1.050A	0.875A	0.700A	0.525A	0.350A	0.175A
Voltage drop	0	- 0.96V	-0.71V	-1.57V	-0.31V	-0.29V	-0.16V	-0.10V
Voltage	24.00V	23.04V	22.33V	20.77V	20.45V	20.16V	20.00V	19.90V

The example clearly shows that the electrical locks at 6 to 8 could malfunction because the voltage is outside the set tolerance +/- 15 % - I.e. under 20.4V.

Result with 12V system and the same area of cable:

Unit:	1	2	3	4	5	6	7	8
Current (approx.)	0.5A	2.45A	2.10A	1.75A	1.4A	1.05A	0.70A	0.35A
Voltage drop	0	-1.92V	-1.41V	-3.14V	-0.63V	-0.59V	-0.31V	-0.20V
Voltage	12.00V	10.08V	8.16V	5.53V	4.90V	4.32V	4.00V	3.81V

With 12V the locks will not work properly because they normally only tolerate a +/- 10 % voltage difference (approx. min. 10.8V)

See next section on how to compensate for this.

Example of correct cable sizing

By moving the power supply, (such as a 24V), you gain a better balance in the load and a better margin can be achieved.

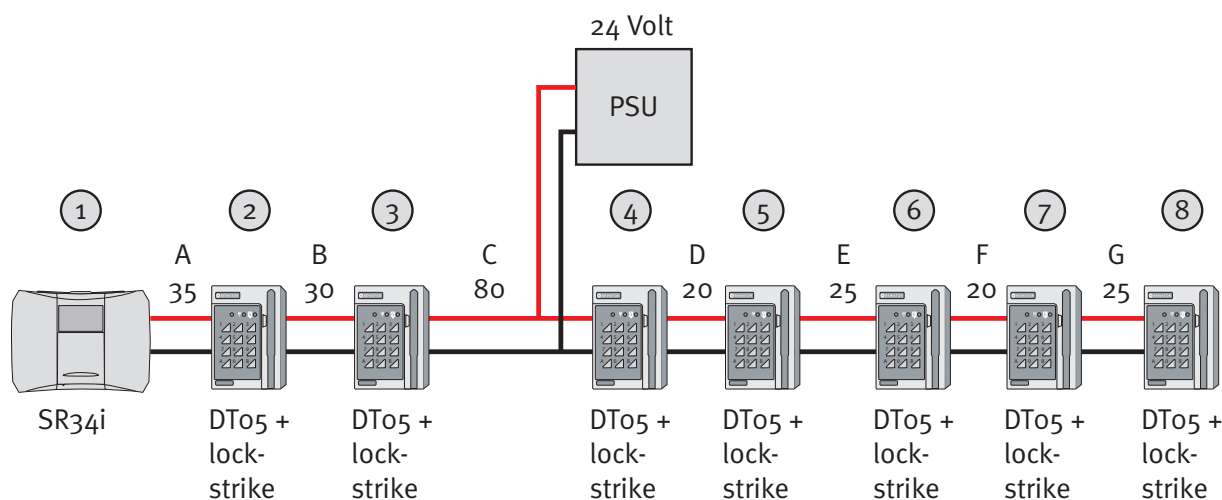


Figure 13 - Correct cable sizing

Result in a 24V system:

Unit:	1	2	3	4	5	6	7	8
Current	0.250A	0.425A	0.600A	0.175A	0.700A	0.525A	0.350A	0.175A
Voltage drop	-0.20V	-0.29V	-1.08V		-0.31V	-0.29V	-0.16V	-0.10V
Voltage	22.44V	22.64V	22.92V	24.00V	23.69V	23.39V	23.24V	23.14V

The SR34i could be moved at the same time to facilitate the connection of the alarm output from the battery backup.

If each section of the access control system is specified according to these rules a secure power supply is achieved.

Result in a 12V system (with the same area of cable):

Unit:	1	2	3	4	5	6	7	8
Current	0.50A	0.85A	1.20A	0.35A	1.70A	1.05A	0.70A	0.35A
Voltage drop	-0.39V	-0.57V	-2.15V		-0.63V	-0.59V	-0.31V	-0.20V
Voltage	8.89V	9.28V	9.85V	12.00V	11.37V	10.78V	10.47V	10.28V

This calculation uses the same cable (1.5 mm²) as with 24V.

NOTE: it is not sufficient to move the Power Supply. **We have to increase the area of cable.**

Several power supplies in the same cable section

Sometimes one power supply is not enough for securing power to all units in the same system section that a SR34i controls. If several power supplies are to be installed the minus (negative) wire must be tied between them. (This is similar to using local power supplies described in earlier chapters).

If this is ignored, the data communication (RS485) to/from door environments may be risked because the minus is used as a reference.

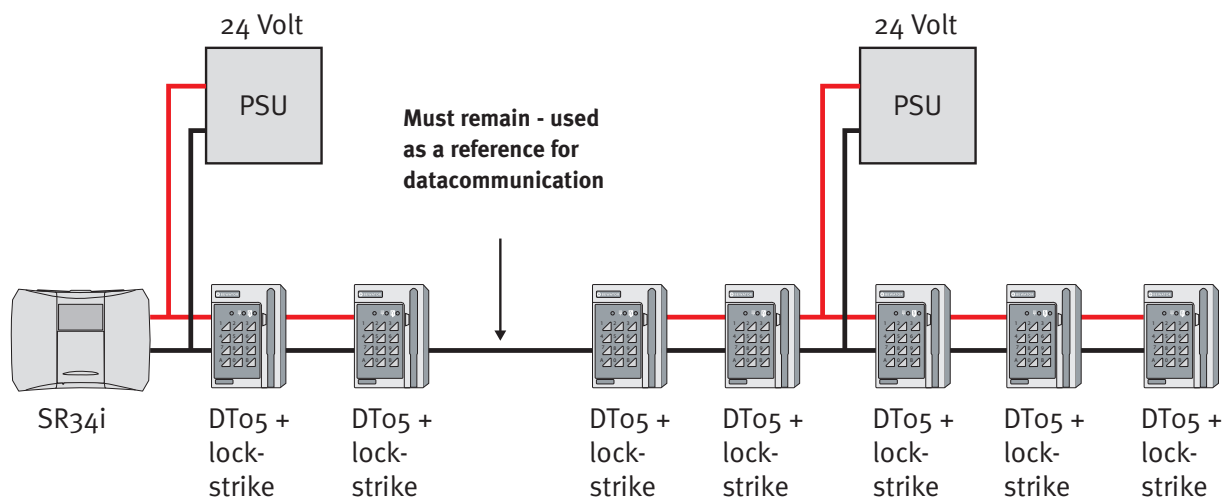


Figure 14 - Several power supplies in same cable section

Alarm Control

In Bewator Entro there are functions for controlling and bypassing external intruder alarm systems by using a relay. Two different methods are available:

- Monostable alarm by-pass (at each door).
- Bistable alarm control (of complete area).

Both methods can coexist in the system. Below we describe differences and how to use them.

Monostable alarm by-pass

In general this function applies for each individual door. The principle is that the intruder alarm has an alarm circuit often through a magnetic door contact mounted in the door. The alarm by-pass relay in the access control system is shunted with this. The intruder alarm is normally then activated all the time.

When access is granted, a timed alarm by-pass takes place at the same time as the door unlocks. When the door held warning time ends and the door still does not close, the relay will go off and the alarm circuit breaks. An alert alarm is activated, both in Bewator Entro and the intruder alarm.

All granted access (with authorised card or code) results in alarm by-pass. This method requires a door controller type **DC22** to control the actual door, because it is the only unit equipped with an alarm by-pass relay.

The door contact dedicated to the access control system will be used for ending the sequence when the door is closed. I.e. the lock relay and the alarm by-pass relay falls and the buzzer become silent. This will prevent the door from unlocking although the people have passed and left the door.

In the example given below the door contact of the intruder alarm is mounted near to the hinges on the door.

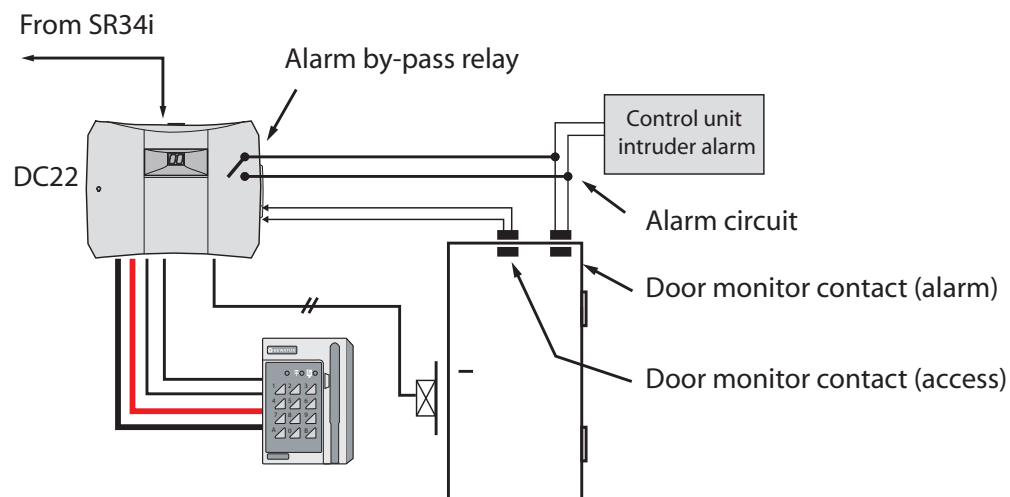


Figure 15 - Monostable alarm by-pass

Bistable alarm control (level or pulse)

Bistable alarm control is used when a certain space is to be supervised by an intruder alarm and must be deactivated when anyone enters

Bistable level means that the alarm by-pass relay is activated all the time whilst bistable pulse means that the relay is activated for approximately one second and then falls back. I.e. every other pulse means activation.

In Bewator Entro there are several methods by which to activate a bistable intruder alarm.

- By using a valid card at the door.
- By using an alarm button connected to the alarm input.
- By using an external timer connected to the alarm input.
- By using a time schedule in Bewator Entro for automatic triggering.
- By using the Door Monitor program and right-click
- By using the control panel of the intruder alarm. Then its output status signal can be connected to the ASF input (in DC22) to “follow” the intruder alarms status (feedback). See section *Intelligent Alarm status feedback (ASF)*.

To deactivate a bistable intruder alarm following methods apply:

- By using a valid card at the door.
- By using the Door Monitor program and right-click
- By using the control panel of the intruder alarm (the status signal connects to ASF input (in DC22). See section *Intelligent Alarm status feedback (ASF)*.

Alarm zones

The starting point is that one or more card reader forms an alarm zone, which is coordinated with a section/area in the intruder alarms control unit. Every alarm zone must include **at least one DC22** door controller, which will act as a master for every other card reader in the same alarm zone. Only the alarm by-pass relay in that DC22 will connect *electrically* to the control input the in central unit of the intruder alarm.

Bewator Entro allows a maximum of 240 zones and it is free to programme card readers which are included in each alarm zone. However – no overlapping is allowed.

NOTE! Remember that readers aimed for bistable alarm control must include a keypad and use ”B” + card +PIN-code when deactivating.

Example

The example shows a basic configuration of two separate alarm zones each with a DC22. (The intruder alarm assumes its own cabling and alarm units).

Readers A, B and C will all allow for activating and deactivating alarm zone 1 (assuming the card is valid). I.e. all readers "remote control" the actual alarm by-pass relay in the DC22.

Readers D, E and F will all allow for activating and deactivating alarm zone 2 (assuming the card is valid). I.e. all readers "remote control" the actual alarm by-pass relay in the other DC22.

When the alarm is activated the doors in the zone are "disabled" and any passing will be prevented.

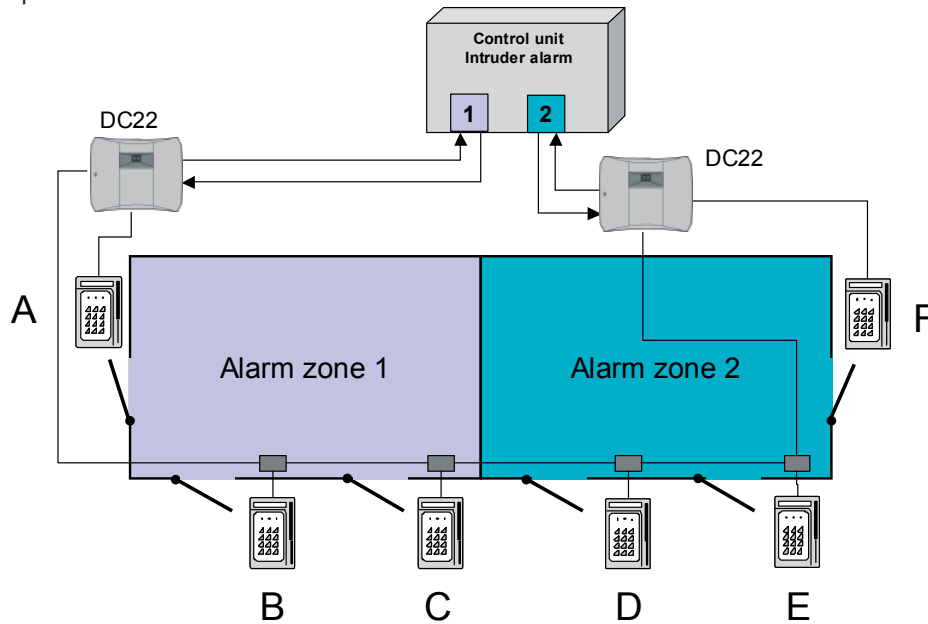


Figure 16 – Alarm zones

Alarm indications

Normally a second signal is connected to the DC22 and it is possible to light the red LED on all readers in the same zone when the alarm is activated.

Readers with a keypad have a red LED, which can indicate if the alarm is on. Depending on which signal is connected, the LED can be lit all the time, go off after some time – or flash. It depends on the character of the output signal from the intruder alarms' control units.

For example, it is possible to have the ASF signal to control the LED in the way that it is initially ON - but goes OFF after a software controlled time.

Intelligent Alarm status feedback (ASF)

There is a feature in the Bewator Entro, which is called ASF (Alarm Status Feedback) it is a way of controlling the status of the alarm zone (ON or OFF). It also allows for the intruder alarm to completely control and disable the doors in the access control system.

E.g. a timer function automatically triggers an activation of the alarm while it is free to deactivate through a card reader – or a control panel in the intruder alarm.

There is an option in the software for how to light the red LED. Either it is controlled in parallel with the status signal - or a separate signal.

If the DC22 is used, there is a separate rely output (pre-warning) for optionally connecting any sirens, or similar, to “copy & amplify” the buzzer sound in the reader. During this time an Exit Button request can still be used to unlock the door

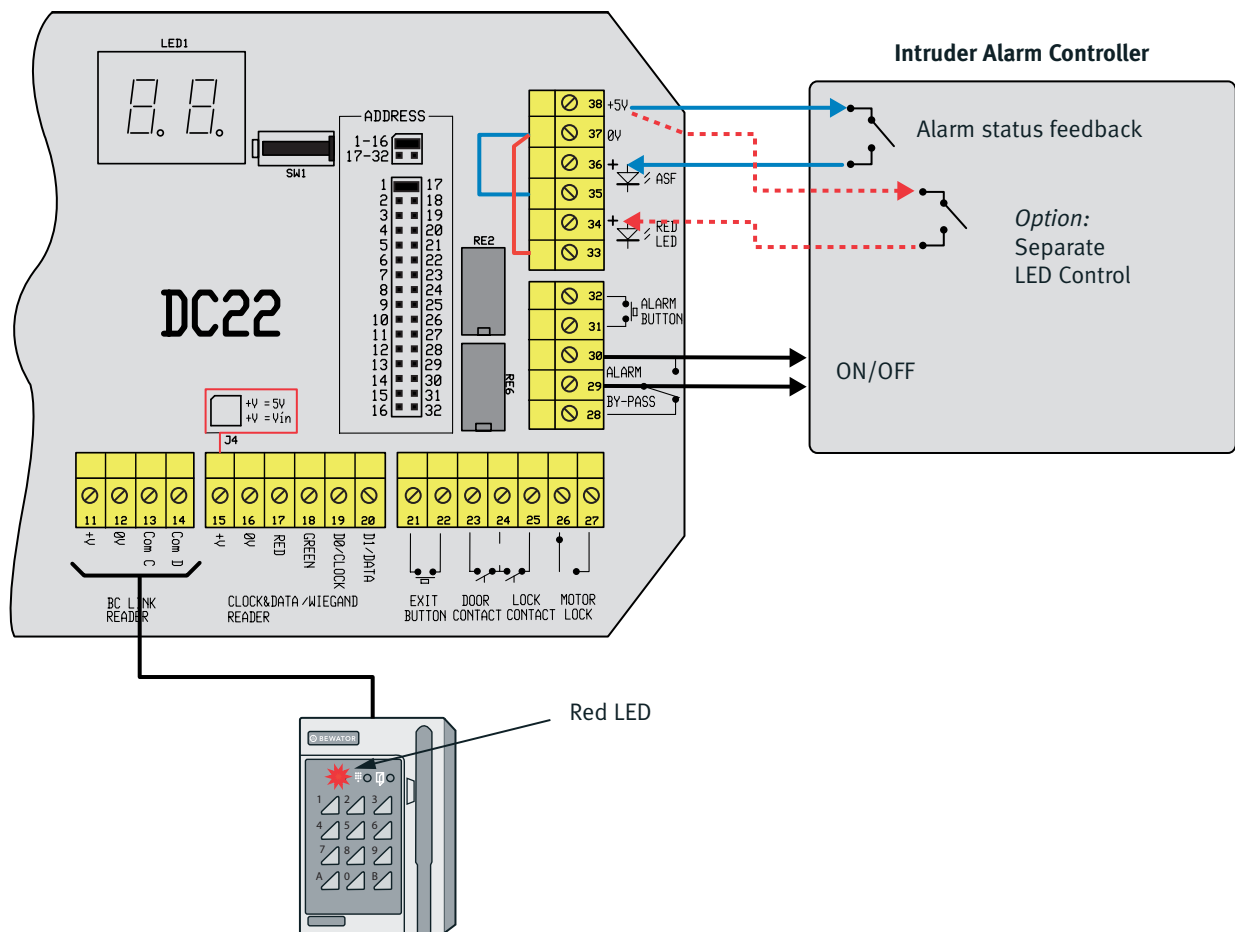


Figure 17 - Alarm Status Feedback

SR34i Segment Controller

In earlier sections we have described different kind of controllers. The most important is the SR34i Segment which contains all data about the site. Even the User name and password for the PC software package is included.

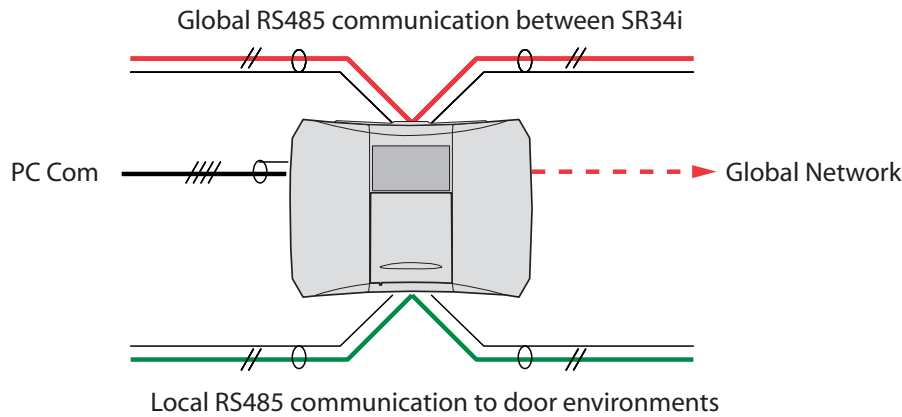


Figure 18 - SR34i Segment Controller

RS485 – in two levels

If LAN is not used the RS485 protocol is effective, both a global bus and a local bus are used. Both have a maximum distance of 1200 metre.

Global is only installed when one or SR34i(s) are used. Den global bus is also isolated between controllers, but must be terminated at both ends.

The local bus is installed between door controllers via a SR34i and beyond the next door controller. This bus must also be terminated with termination resistors.

Ethernet and LAN

SR34i has a complete, integrated **network switch with two RJ45** connectors. This is embedded and admits connection directly on the LAN. In many cases there is often an existing cable, which can be used.

SR34i – different capacity

The Segment Controller is available in four different capacities which indicates how many doors it can manage:

- SR34i/4 Controls max four doors
- SR34i/8 Controls max eight doors
- SR34i/16 Controls max 16 doors
- SR34i/32 Controls max 32 doors

It is possible to upgrade and extend the capacity gradually. This eases future expansion. The SR34i communicates on two levels (global and local bus). It gives many choices of how to specify Bewator Entro. Properties with several floors can include a SR34i on each floor which can handle a couple of doors each.

SR32, SR32i or SR34i?

Historically there are different generations of segment controller.

In Entro version 5 is required that only SR34i are used as segment controllers (which we also recommend when upgrading an older site to take advantage of all new functions). In cases where an existing Bewator Entro site is expanded a system generation check must be carried out on the system generation.

If the existing version is 4.1 to 4.5, both SR32i and SR34i can be used if the intermediate version 4.7 is installed. Note that the SR34i will still lack some of the functionality. The SR34i is shipped with firmware suitable both for version 4.7 and 5 and can be activated directly via the keypad.

Generations before 4.0 use SR32 controllers (without an "i") – whilst version 4.0 – 4.5 and later require SR32i.

Following table describes which software available for the different Segment Controllers.

	Version 2.x	Version 3.x	Version 4.x	Version 4.7	Version 5.0/5.1
SR34i	No	No	No	Yes *)	Yes
SR32i	No	No	Yes	Yes	No
SR32	Yes	Yes	No	No	No

*) Some restrictions in functionality.

Door environments

Door environments are the part of the system that has the most flexible solutions regarding products. E.g. magnetic card readers, proximity readers, hands-free or Wiegand readers can be mounted.

The door environment also has an electrical lock, exit button and door monitor contacts to be installed.

As mentioned earlier the type of “media” (card/tags) will affect the choice of reader technology. In the table below the combinations of door controllers and readers are shown.

We referred to the actual Installers manual in each case .for every product you find complete, detailed information about components, terminal blocks etc. Remember that the product range may be changed gradually and products may be obsolete.

Door-controller	Alarm-control	Door monitor input	Lock monitor input	Reader type
DC22 Split mounting	Yes, relay available	Yes	Yes	BC43 (magnetic card) BC43Prox BC16/BC18 (card only) HF500 (hands-free) HD500-2, PR500, SP500, PM500 (prox) BC5515 (prox, split mount) BC5511 (Hands-free, split mount) BC5516 (loop antenna) M43 (keypad) Wiegand
DC12 Split mounting	In alarm zone where DC22 exists.	Yes	-	As above (requires minimum version 4 of PC software)
DC01	Cannot control alarm but can be included in alarm zone and locks door when alarm is activated	Yes	-	-
Dropbox	In alarm zone where DC22 exists.	Yes	-	DT05 (magnetic card) DT05Prox
Dropbox	No	No	No	PD30EM

Figure 16 - Door controllers and readers

Proximity or magnetic card reader – or both?

The difference between the two, is that magnetic type of reader accepts banking cards, credit cards etc. that have a magnetic trace without a card number recorded and the reader is equipped with a magnetic reading head.

Proximity readers use a card or tag, which has embedded antennas and a microchip with a unique code. Bewator uses eight digits but the chip has more unique digits. The readers have corresponding antennas that read the code.

Magnetic cards will not work with proximity readers - and vice versa. However – there is a combination, proximity card passive type (without battery) that also has a magnetic trace. The card will then be accepted by both types of readers.

The table below gives an overview of readers and keypads.

Reader model	Type	Interface (to Entro)	Comments
BC43	Magnetic	BCLink	Embedded keypad
BC43Prox/EM	Proximity	BCLink	Embedded keypad
HD500-2/EM	Proximity	BCLink	Robust metal housing
PR500/EM	Proximity	BCLink	Small profile
SP500/EM	Proximity	BCLink	Switch-plate model (mounted in wall-socket)
PM500/EM	Proximity	BCLink	Panel mount (for integration in panels)
HF500	Hands-free	Clock/Data	Reading distance 1 metre. Indoor mounting
BC5515	Proximity	Clock/Data	Split mounting BC5311 (indoor) PR100 (outdoor)
BC5511	Hands-free	Clock/Data	Split mounting BC5311 (indoor) HF100 (outdoor)
BC5516	Antenna	Clock/Data	Split mounting BC5311 and loop coupler (indoor). Customised antenna.
M43	Keypad	BCLink	Keypad. Can complete proximity readers without keypads.
BC18	Magnetic	Clock/Data	Card-only reader
BC16	Magnetic	Clock/Data	Card-only reader (UK Market)
Wiegand	Different	Wiegand	26- or 32 bit protocol.
DT05	Magnetic	RS485 bus	Compact reader with dropbox
DT05Prox/EM	Proximity	RS485 bus	Compact reader with dropbox
PD30EM	Proximity	RS485 bus	Electromechanical (Codoor type)

Figure 17 - Readers for Bewator Entro

BCLINK or CLOCK&DATA interface

There are two different interfaces used by Bewator to communicate with reader units. Each data sheet shows which type the unit requires.

- **BCLINK** enables several units to exist on the same cable and they are addressed on another level. BCLINK can control LEDs and buzzers. The interface can send information in both directions (Tx and Rx).

The most common case is a DC22, which has a main address in Bewator Entro. Two BC43 readers are mounted on each side of the door with cables in parallel. The readers are then addressed as ENTRY and EXIT – they have a sub-addresses.

- **CLOCK&DATA** means every unit has its own cables and cannot be addressed. This is addressed by using the door controller. This is a more “open” interface consisting of a clock signal and a data signal (Clock and Data).
- **WIEGAND** connects to the same interface as CLOCK&DATA but uses another protocol.

A door controller has the ability to communicate on both interfaces simultaneously. E.g. could a hands-free reader HF500 with Clock/data be mounted indoors and read through the wall and at the same time use a M43 keypad with BCLINK mounted outdoors for typing PIN-code.

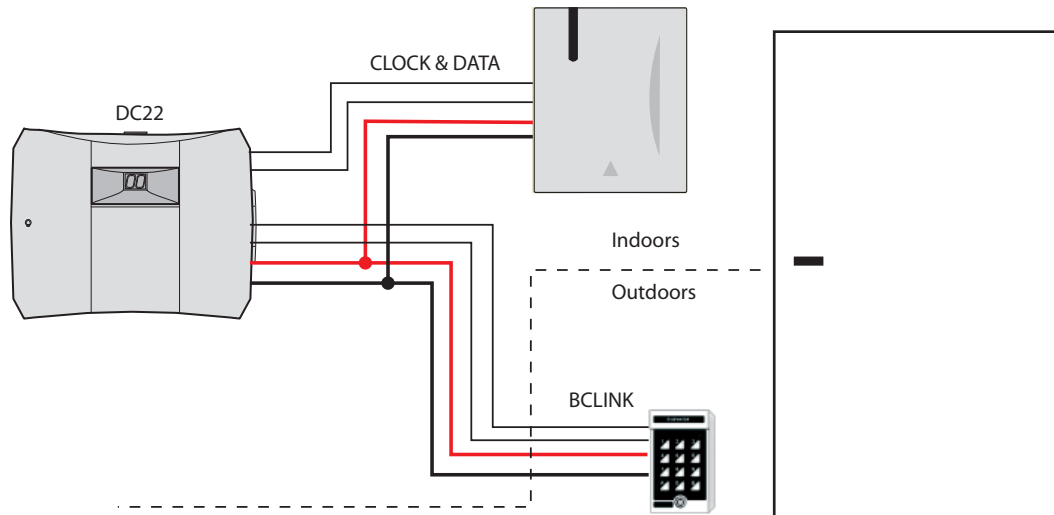


Figure 19 – Door environment with both BCLINK and Clock/data

Compact or split mount?

The main difference between compact and split mount, is that the connection of wires to a lock in a split mount are made indoors.

In a compact mount the lock relay (and other connections) are done in the unit outdoors.

This is potentially risky and therefore not recommended to be installed outdoors

In Bewator Entro there are only two compact mount products - DT05, DT05Prox and DT05EM. All other products are split mount.

Door Monitoring

In Bewator Entro there are functions for door monitoring. First in the door environment but also in combination with the PC software. Different events and alarms can be generated depending on what is happening on the site. The most common examples will be:

- **Door open too long.** A door has been open correctly but has not been closed during the set time + door held warning time (maximum 99 + 99 seconds).
- **Door forced.** An illegal opening of a door has occurred (e.g. if a door handle has accidentally been used).
- **Mechanically unlocked.** A door equipped with both door contact and lock contact has been unlocked with a key. I.e. the contacts have not been activated in correct sequence. This function is only available in the DC22.
- **Door locked.** The lock is in a locked position.
- **Door closed.** The door is closed.

A door monitor contact and/or lock monitor contact should be connected to the door controller. Next set up the relevant software.

If no contact exists you do not mark anything in the software and the system ignores this input of the door controller.

In the Table 1 - *Door controllers and readers* you can see the available inputs in different products.

Motor lock and lock strike plate

The door controller DC22 can be set up to control both an ordinary lock strike plate and a motor lock. The lock strike connects to the opening relay and the motor lock to the separate relay for motor lock.

If the lock monitor output of the motor lock is connected to the lock monitor input of the DC22, the wear of the motor lock is reduced. The DC22 will not activate the lock strike until the motor lock is completely unlocked. This means that you prevent the motor lock from mechanical damage.

The User will also see the normally lit, green LED of a reader flashing, while the motor lock is working. During this time (a few seconds) the door cannot be opened.

Functions in the IOR6

The relay controller IOR6 can be used for different functions (aside from lift control applications described in the next chapter).

Common alarm

In the same way as events can be retrieved, filtered and stored on a PC, the events can be used for other purposes. Particularly if events are specified as an **alarm event**, a relay in the IOR6 can be activated. This we call a *common alarm*, because several, different events can be summarised to one alarm.

On the other hand, every relay can invoke its own event filter and generate many types of common alarms.

Emergency exit

In addition to the function in the Door Monitor program to open all doors, inputs in the IOR6 can also be set to monitor a signal from e.g. a **fire alarm system**. That is the system allows for external sources to set doors unlocked.

Power failure warning

Inputs of the IOR6 can be set to monitor power failure warnings from the power supply. Especially units equipped with batteries.

Sometimes the alarm output of the power supply can be set to different actions (e.g. main falls or battery level). However Entro have one type of message ("Power failure") in the event log.

Many times an Entro site have several PSUs installed (= many warning signals) and we can connect and monitor each of them.

Timer controlled

Each relay in the IOR6 have the capability to control external functions by using separate, standard time schedules in Entro. Because each time schedule in Entro have two time zones + other time, we can arrange for **six different on/off for each relay**.

Machine & door control in Reservation

If an IOR6 is included in a Reservation object, there are possibilities to fine tune how the reservation object is used. In many cases you may want to spread the wear of a group of machines. (E.g. that a machine is not used more than any else). The relay in the IOR6 is activated the *whole* reserved time interval.

At the same time another relay (in the same object) can be activated by the same user but only a *specified time*. E.g. opening time for a door.

Lift Control

In Bewator Entro there is an easy way of controlling the access to different floors in a building. You can install readers on each lift door (on every flat) preventing access to the lift itself. However – this is a round about way of solving the problem.

By placing card readers *inside* the lift – and forcing the users to use their card, Bewator Entro and Lift control system will decide which button(s) the user will press.

Bewator Entro allows 32 IOR6 in a system with a total of 192 relays. It is possible to split these into several lifts (equipped with their own master reader) – or just one for 192 floors! This function is true global which means that the IOR6 and the Master reader can be placed anywhere on the system.

It is advisable to use the Relay controller Bewator Entro IOR6 to interface the Lift Control and then use one reader on the system as a Master for this IOR6. This is to get the identity of the user. Depending on the authority (access group) of the user – different access can be granted.

It is also possible to time control each relay and/or remote control (similar to an exit button).

Example

The example below shows an application where the Master reader controls two IOR6-units with 2 x 6 relays which offers the possibility of controlling twelve floors.

In the software you will see each relay the same way as a door, where you decide in which time zone the access group access. Every time the card is presented to the reader – the system checks for authorities – and activates the appropriate relays.

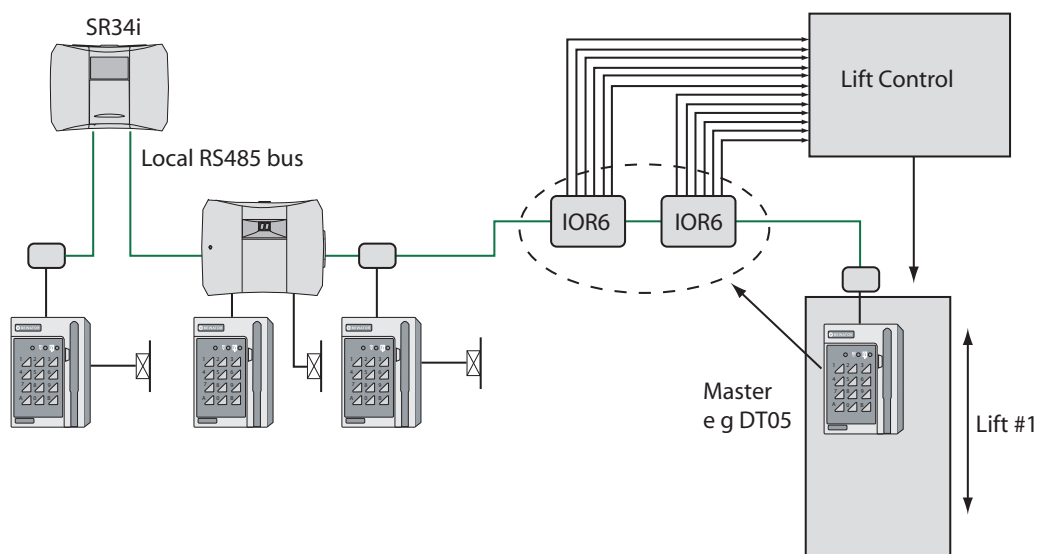


Figure 20- Lift Control in Bewator Entro

Software

Bewator Entro software package (available on CD) includes all necessary software modules and no extra modules need to be ordered. Instead the System administrator has the opportunity to disable menus/functions not needed in the final application. This makes it user-friendly.

The modules are as follows:

- **Installer** – a module which automatically finds units and their addresses. Also used for creating zones consisting of readers as well as creating database and connections
- **Entro** – Main module to manage time schedules, zone settings, authorities, cards and some system settings like auto-logoff.
- **Door Monitor** – displays the events and can also unlock door.

The main point to consider is the power of the PC used. A modern PC has more than enough capacity to manage a Bewator Entro system. See also Technical data

Several PC's on the same site

Different kinds of solutions are available to gain more Users (PCs) on the system. In these cases often a local area network is available. Entro version 5 allows for several System users and/or PC are on-line at the same time.

Some important points to consider:

- Every PC (used in network applications) should be linked (connected) to the same SR34i.
- Every PC must have a valid Bewator Entro software license.
- Dedicated PCs names must be known (and noted). Read more in the User manual.
- All editing of the database should be performed on-line. Otherwise the data may be overwritten.

Reservation system

In a Bewator Entro site, the readers are installed– but the chosen doors are "transferred" to the reservation system.

When using Bewator Entro you have to choose between one of two possible User interfaces when booking functions:

- Using the embedded reservation functions in Bewator Entro where a LAN is connected to a PC or where a touch-screen terminal is used. Both **time schedules** and **reservation objects** are created (by the System administrator) inside Bewator Entro software.
- An external reservation software package sends reservation information times and authorities to Bewator Entro. Reservation objects must be created in Bewator Entro. Technically a special protocol called "BAPSI" is used. Please contact Bewator if you want to know more.

In both cases the reservation objects in Bewator Entro are based on actual sites for example sports arenas, conference rooms etc.

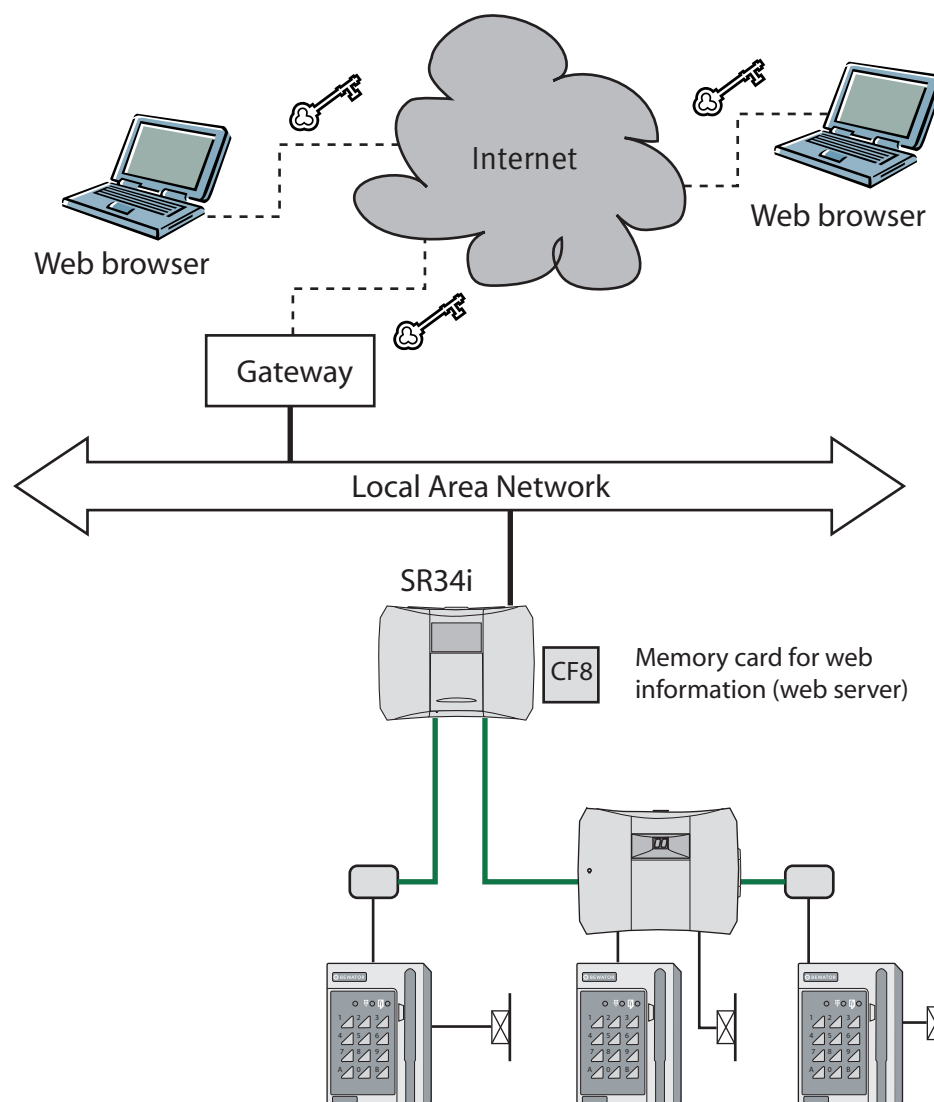


Figure 21 – Example of standard solution for Reservation in Bewator Entro.

Necessary components

The Reservation system always requires a TCP/IP LAN to be used because the web server function on the SR34i is reached by using IP-addressing technique.

The SR34i acting as the web server must be equipped with a flash memory card CF8. This will store the HTML-pages, which will be sent to the Users web browser (such as Internet Explorer) when a booking is to take place.

Web browser or touch-screen terminal

When booking times it is essential that a **web browser** browses the IP-address of the SR34i. This can be done either from a home computer or an office computer. Also the System Administrators' PC (used for setting common parameters in Bewator Entro) can be used for bookings. The identification process will require the Users' card number and PIN-code.

An alternative method is to use a touch-screen terminal placed nearby the reservation object in conjunction with a card reader. Identification is done by presentation the Users' card.

InfoPoint IP811/IP810 Reservation terminal

The InfoPoint IP810 unit is a general-purpose terminal based on TCP/IP technology. With Bewator Entro systems it forms a compact, easy-to-use platform for making reservations close to the Reservation object.

It has an integrated web browser function that connects via local area network e.g. to the SR34i Segment Controller running as a web server.

The colour display and keys as well as the intuitive software ensure this system is user friendly for the End-User.

The InfoPoint IP810 also have an integrated numeric keypad.

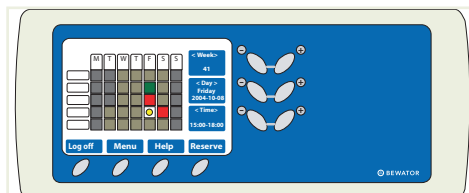


Figure 22 - IP811

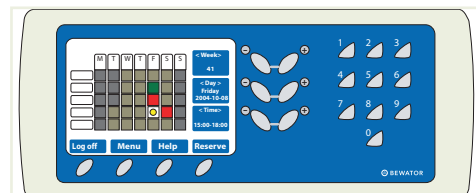


Figure 23 - IP810

Machine and door control

The reservation object consists of a traditional card reader at a door – and up to 10 IOR6 relays.

For example, a relay can control a washing machine in the way that when a person uses his card, not only will the door be unlocked, also the machine starts and can be used during the reserved time.

At the same time other relays in the IOR6 may be used to control other reserved doors (like a drying room), which can be open for access (with a defined opening time) and then lock again.

Other relays can be controlled with a time schedule (e.g. lights on at a certain time).

Example 1 – three doors without LAN

A company, situated on one floor of a building, has three doors that require the following:

Door name	Prerequisites in the door environments
Main Entrance	Magnetic card reader and exit button from inside. Security level: Code at working time 8 AM – 5 PM and Card + PIN rest of day. Visitors use a simple doorbell. Lock #1: Lockstrike 24V DC, 120 mA. Lock #2: Motor lock 24V DC, 700 mA
Computer room	Magnetic card reader and exit button from inside. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lockstrike 24V DC, 120 mA
Employee's' entrance	Magnetic card reader and exit button from inside Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lock #1: Lockstrike 24V DC, 120 mA. Lock #2: Motor lock 24V DC, 700 mA Controlling an intruder alarm with one alarmed area (whole company)

Figure 21 – Example 1 (three doors)

Suggestion

Because there is an intruder alarm installed, at least one door controller **DC22** must be included. In addition there is a need for magnetic cards + PIN-code used at night to deactivate the alarm. The obvious choice would be the **BC43** for both the main entrance and the employee's' entrance. There are two locks installed in both entrances, which require DC22 to control the motor locks. At the same time it will be possible to monitor the state of the motor lock.

In the computer room a **DT05** compact reader will be sufficient because it is placed indoors. Higher security could be achieved by using an alternative DC12 + BC43 in split mount.

The Segment controller **SR34i/4** with a four door capacity will be enough in this case and the PC is connected with serial RS232 cable within 25 metres from the SR34i. Maximum current in the system is approx. 2.7A at 24 V DC and a 24V battery-backup BA24/5 with 5A supply and 7Ah battery capacity is of sufficient.

The local bus communication between SR34i and door environments is necessary and we use the **Bewator cable** for both power and communication.

A bistable **alarm zone** is configured in Bewator Entro including the *main entrance* and the *employees entrance* where the intruder alarm is controlled from either door. The signal wire has to connect from one DC22. The available signals are connected from the intruder alarm to acknowledge any activation/deactivation (ASF) and light the red LED's on the readers.

The security levels in the doors are configured in the software. However – when the alarm is ON the security level is normally is card + PIN.

Example 2 – three floors with three SR34i (without LAN)

A large company uses three floors with entrances from internal stairs and a main entrance at the first floor. The company uses proximity cards to gain access.

Floor	Door	Prerequisites in the door environments
1st floor	Main entrance	Hands-free reader indoors (reads through wall) and keypad outdoors. Security level: Unlocked at working time 8 AM – 5 PM and Card + PIN rest of day. Visitors use the Bewacom BM31 door phone. Lock #1: Lockstrike 24V DC, 120 mA. Lock #2: Motor lock 24V DC, 700 mA Controls the intruder alarm with alarm zone First floor.
	Warehouse	Hands-free reader indoors (reads through wall) and keypad outdoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lock #1: Lockstrike 24V DC, 120 mA. Lock #2: Motor lock 24V DC, 700 mA Controls the intruder alarm with alarm zone First floor.
	Store	Proximity reader with keypad. Security level: Card at working time 8 AM – 5 PM and Card rest of day. Lockstrike 24V DC, 120 mA.
2nd floor	Entrance	Hands-free reader indoors (reads through wall) and keypad outdoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lockstrike 24V DC, 120 mA. Controls the intruder alarm with alarm zone 2nd floor
	Computer room	Proximity reader with keypad and exit button indoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Solenoid Handle Locks 24VDC, 250 mA
	Accounts	Proximity reader with keypad and exit button indoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lockstrike 24V DC, 120 mA.
	Conference room 1	Proximity reader with security level Card all week. Lockstrike 24V DC, 120 mA.
3rd floor	Entrance	Hands-free reader indoors (reads through wall) and keypad outdoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lockstrike 24V DC, 120 mA. Controls the intruder alarm with alarm zone 3rd floor
	Conference room 2	Proximity reader with Security level Card all week. Lockstrike 24V DC, 120 mA.
	Store	Proximity reader with keypad and exit button indoors. Security level: Card at working time 8 AM – 5 PM and Card + PIN rest of day. Lockstrike 24V DC, 120 mA.
	MD room	Proximity reader with Security level Card all week. Lockstrike 24V DC, 120 mA.

Figure 22 - Example 2 (three floors)

Suggestion

Due to the use of proximity cards we have a choice of proximity and hands-free readers. **Three SR34i** controllers are installed on each floor and we tie these together with a global RS485 connection. Every SR34i controls doors on each floor.

In the Entrances and Warehouses we install **DC22** door controllers and **HF500** hands-free readers (used for passing in both directions) with **M43** keypad outdoors for PIN-code use. Power supplies **BA24/5** 24V DC, 5A are also installed on each floor.

Three separate alarm zones (on each floor) are controlled from a DC22 connected to input in the intruder alarms control unit.

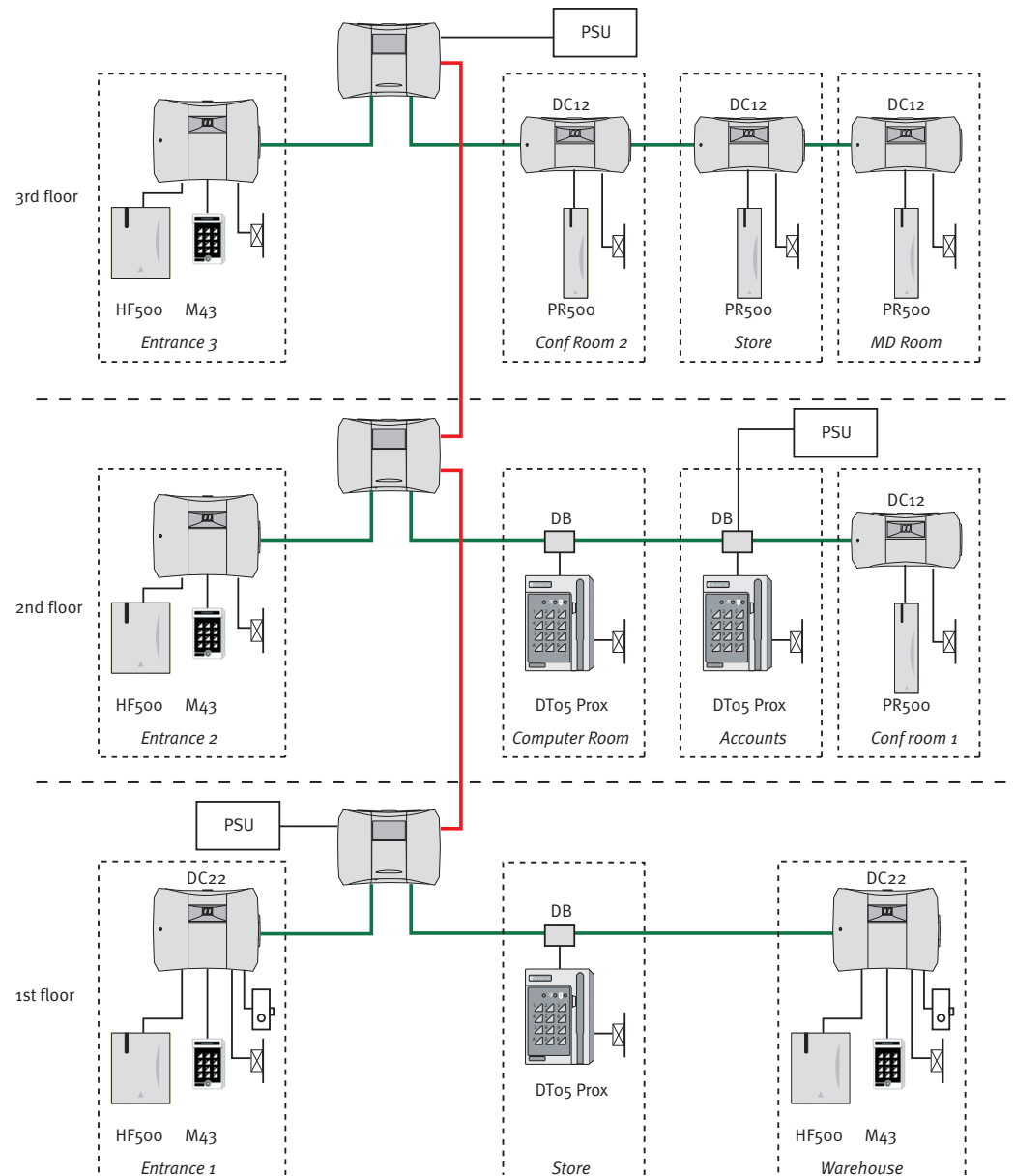


Figure 24 - Example 2 (three floors)

Example 3 – LAN in same property

This example is based on the earlier example 2, but will use local area network for communication between SR34i and PC. The door environments do not have to be changed. Suggestion

It is very important that the IT-manager of the company is involved (at an early stage) to define which IP-addresses to use as well as the overall structure of the LAN (routers, firewalls etc.). In addition the LAN must be able to use 10/100 Mbit/s Ethernet. SR34i controllers have to be be set up with the **correct IP-address**. The Installer program will supply this if the PC is inside the same *logical subnet* as the SR34is.

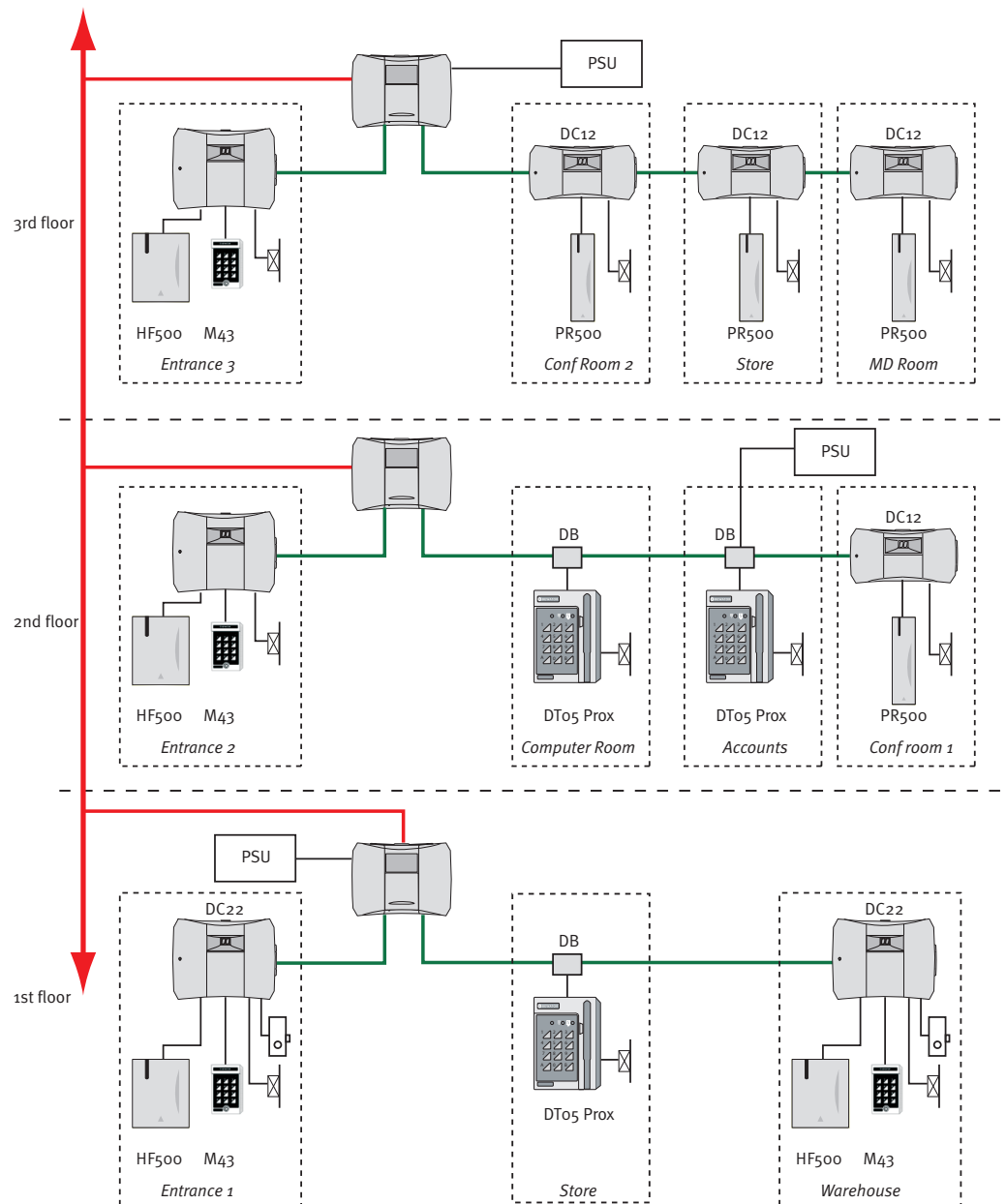


Figure 25 - Example 3 Local Area Network

Example 4 – a LAN system located both inside outside the property

For this example we have two sites, a *Head office* and a *Branch office* (which is located in another town). The company's intranet (Wide Area Network) will be used to tie the two systems together onto one database. This will make it possible for users to gain access to both offices.

As with an earlier example, it will only be the SR34i and PC that will communicate through the Ethernet network. The door environments on the sites are not affected at all.

Remember that the two sites always try to update each other through the internal network (or Internet). Any delays (or breaks) in the network will affect the systems ability to maintain database integrity. However – synchronisation is done automatically, as soon as the link is up and running again.

Security aspects

In cases where Bewator Entro is to be connected to a LAN, the customers **IT-manager** must be consulted when specifying the systems. This is even more important when a public network (like the Internet) is used. In order to guarantee a high degree of security and integrity in the access control system, the IT- manager must define any routers and firewalls that will be used.

In Bewator Entro there are a number of security functions:

- Encrypted **TCP/IP** communication (128 bit level).
- Unique **system name** for each database.
- Defined **connection** (with computer name).
- **Login** for PC software (five different levels).
- **Auto-logoff** in PC software (time can be chosen).

Suggestion

As mentioned earlier in example 2, Head office can be a complete system. A similar system should be added at the branch office remote site and a **gateway** at both sites.

The basic database on the PC (created more or less automatically) for the head office must be completed manually with parameters and data for the branch office. E.g. information about the IP-addresses, Netmask and Gateway of the branch office etc. At the same time the SR34i must be be programmed with the corresponding parameters, to allow for communication when the sites are connected together.

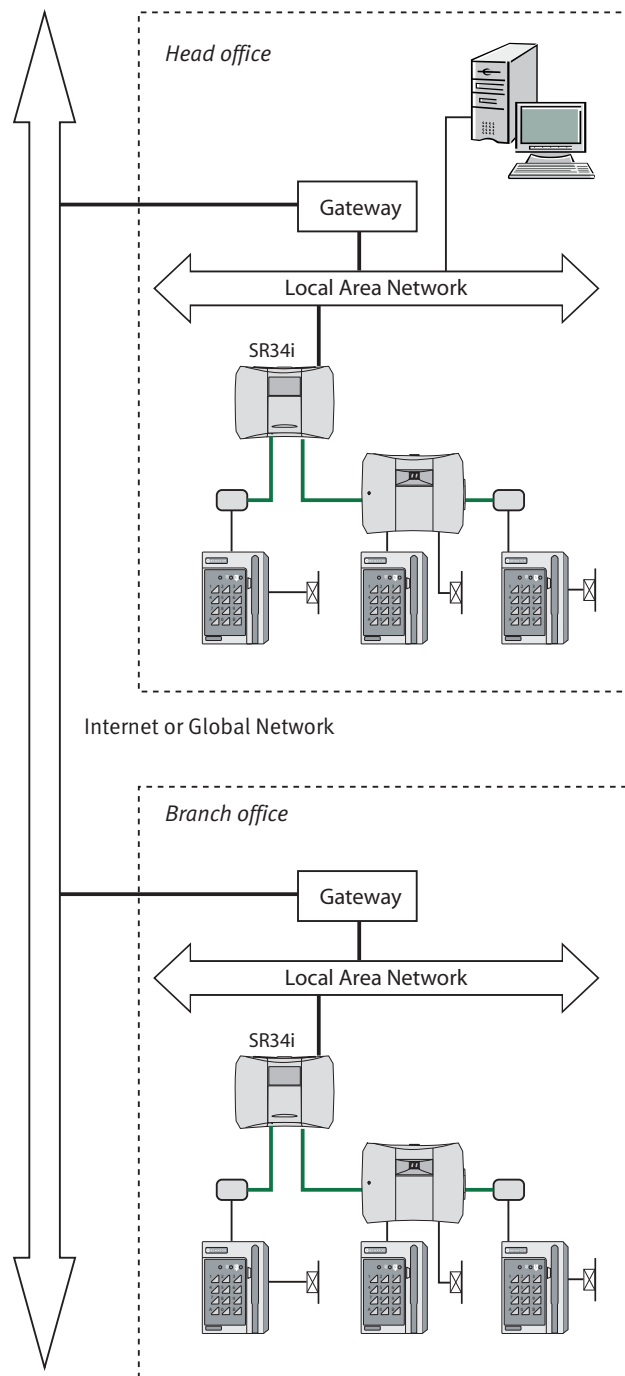


Figure 26 - Example 4 – (global network)

Example 5 – Reservation system

We have a facility with an entrance door and a garage door. In addition there is a laundry room with two machine groups where reservations can be made. To reduce the wear of machines, we want to randomly allot them to users.

Each machine group reservation should allow for the use of a drying room during the reserved time. This door will only be unlocked during a specified opening time when the card is presented.

The End-User should be able to reserve time intervals via the Internet – or by using InfoPoint IP810 terminal.

Suggestion

We make arrangements for the local area network (LAN). This includes an Internet connection. The InfoPoint is mounted near to the laundry room and connected to the LAN. The IOR6 relay controller is used in two ways:

- **Machine control** – the relay is active during the whole interval, which means that the machine is turned on and can be used. When the interval ends – the machine stops and can not be reused.
- **Door control** – the relay is active only the specified opening time (like an ordinary access door). The main reader of the reservation object freely can be used to unlock the door during the reserved interval.

The End-user reserves time intervals by using the PCs web browser or via the InfoPoint IP810. In both cases a login must be entered. One of the machine groups is the allotted User (based on the parameters set by the System Administrator).

The system automatically activates the necessary equipment to be used. Access to the Entrance door and the Garage door will be fully controlled by the “ordinary” Time schedules and Access groups in Bewator Entro – not by the Reservation system.

Please see next page for the solution.

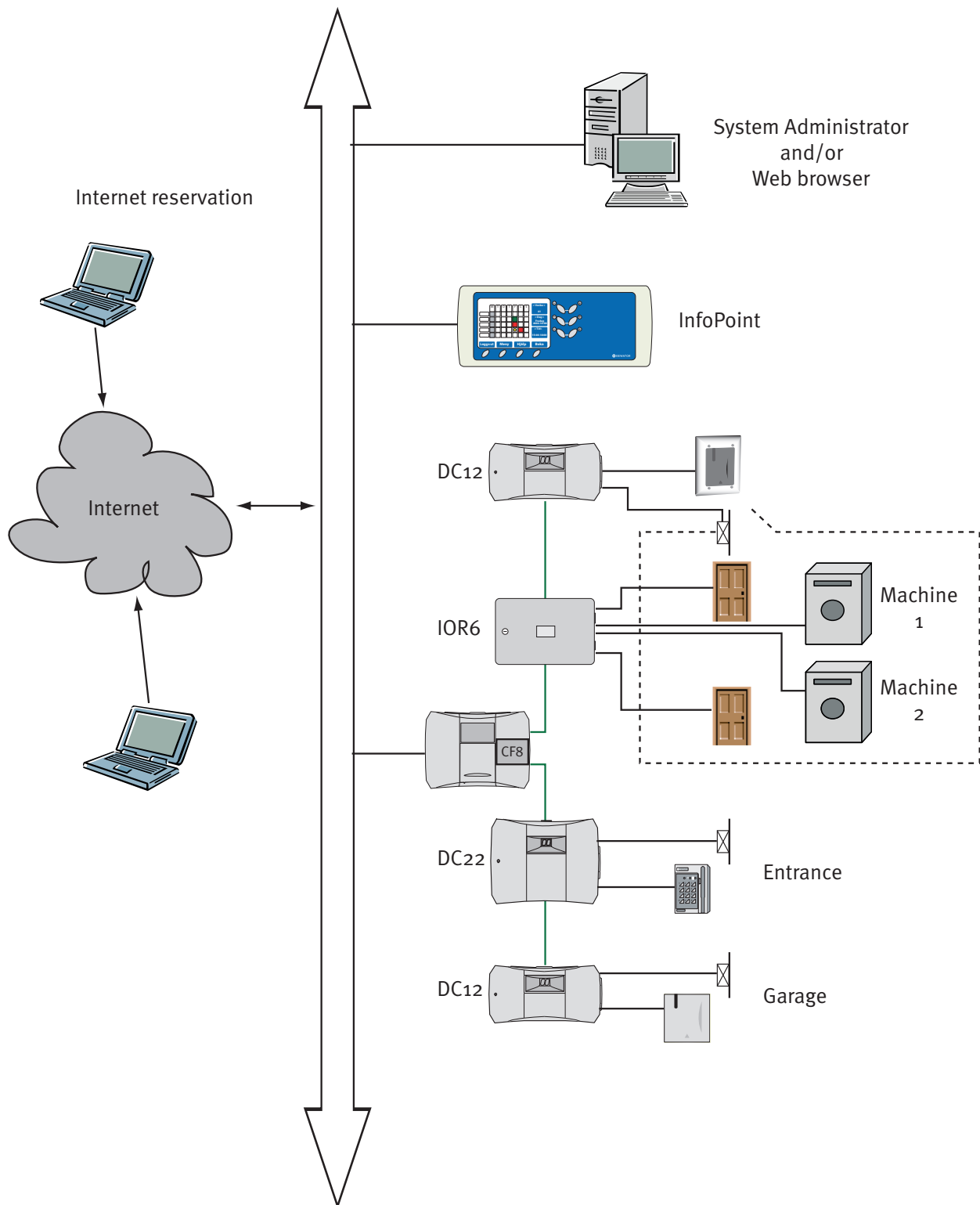


Figure 27 - Reservation system with machine control.

Example 6 – two PC in the same network

In a larger Entro application there may be a need for allowing more system users to programme the system. Different to earlier versions of Entro several users can be on-line at the same time. The prerequisites for this are that we know the names of the PCs to connect.

Every System user must specify which PC, which event filter and where to store events on the PC. When a system user logs on the system knows if events can be retrieved from the actual user.

The illustration below shows how two System users connect to Entro.

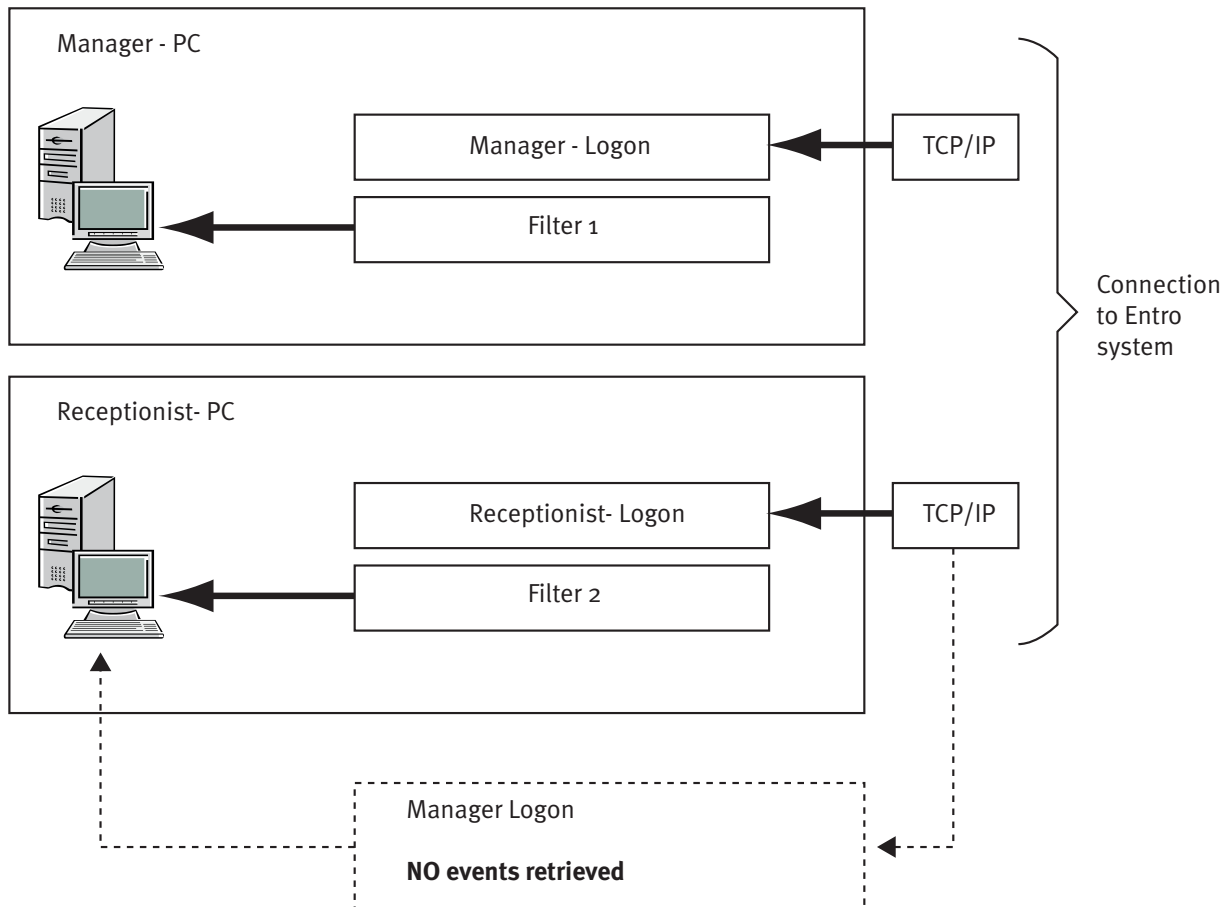


Figure 28 - Several System Users

Advanced information about LAN

The following chapter contains questions and answers regarding Bewator Entro when used in local area networks and is primarily aimed at IT-managers.

What does the traffic load look like when it is using Entro in TCP/IP LAN?

As Entro/TCP is evolved with RS485, the traffic is relatively moderate providing that the database is hard packed. The traffic SR34i will have a socket open to every other SR34i. This socket is alive and is tested for failures with a special ping-message every eight second (in version 4). This is not an ICMP-ping, rather a common TCP/IP package with some information (only a few bytes in size).

Beside this, in an idling system, there is a comparing-of-databases message to the node nearby approx. every ninth second. The time depends of the configuration. In a small system this could be every sixth second. Also this message is short - approx. 40 bytes plus the length of header (see item 2).

How does the messages look like e g for events and creating cardholders? What is size of packages is sent?

The packet size is currently 407 bytes (plus TCP header and IP header together with a MD5 hashing of the message). Totally it is less than 500 bytes. The information sent in case of an event (e g granted access) is approx. 40 bytes. Creating a new cardholder results in a database update with a frame of 80 bytes and a 10-byte frame.

How often does the SR34i communicate with each other?

At least every 6-8 second.

How often does the SR34i requests a timeserver?

It does it every 23rd hour continuously

What happens if the SR34i loses the database and uploads from another SR34i – does the LAN become slow?

No, because we only use a fraction of the total capacity. Entro uses 10Mbit LAN and just a few percent of that. The reason is that the Entro primary should handle the access issues rapid. The communication has a lower task priority. In addition the communication is encrypted with 128-bit RC4, which together with the MD5 authentication takes CPU power and reduces the speed. However – in modern LANs switches are often used which do not affect the speed negative.

Is it possible to change the IP port used by the system – e g if 4001 and 4002 are occupied by another application?

Only port 4002 is used in communication to the PC (and may be in conflict with other application is the same PC). In version 4 you cannot change the port. The risk for a conflict is seen as minimal. If this should be a problem we will of course solve it. There are no applications known so far that uses this port.

How is the traffic affected? Use of “sniffers”?

We have (during the development phase) off course have been using “sniffers” (three commercial and one of our own). We have also bursted 100% bandwidth to the SR34i to see the effects of the information quantity. Both UDP and TCP. This is however not quite so dramatic relative to a 100 Mbit LAN.

Why not use VLAN?

VLAN is a good alternative to create a more secure network. It is however difficult for Bewator to state general recommendations how to build the users own LAN.

There is no reason for using VLAN, due to network load, in an Entro TCP/IP environment. In general we recommend IT-managers to use LAN switches rather than an Entro recommendation.

Is it possible to run Entro via Citrix VTS Mainframe v 1.8?

We do not really support a configuration with Citrix and/or PC Anywhere, VNC etc. However we cannot see why it should not work.

Remote programming can also beside modems be done via TCP/IP.

Can database files be placed on a LAN-server to make it possible making backups in night-time?

To store the files on a server is not a problem itself; just install the software on the server. You then must of course be sure that the server is running all the time.

The way Entro is designed there is also redundancy integrated in the database, because all data is stored in every SR34i (except events handshaked from the PC).

Is the communication secure in Bewator Entro?

All communication in Bewator Entro version 4 is heavily encrypted. At the moment RSA RC4 128-bit is used. This is the same level as most banks are using. The encryption key can easily be changed. In Internet applications the IT-manager can raise the security by increasing the encryption set up in the LAN itself. In addition the User name and Password is checked at login as well as the correct System name.

What is RSA RC4?

RC4 is a symmetric encryption method, developed by RSA Security, which has been used for many years and is seen to be very reliable. Bewator Entro uses 128-bit strong encryption.

128-bit encryption does not sound enough! I use 1024 on my e-mail!

When comparing encryption algorithms, it is not correct to compare only the amount of bits because different encryption methods have different strength. Bewator Entro uses a *symmetric* method not to compare with e-mail software (usually using PGP or similar), which is an *asymmetric* method (with public keys). These methods normally require a higher size of key to fulfil the security need.

What is MD5?

MD5 is a method to confirm messages and logins. This is used in Bewator Entro to ensure that all messages are correct when they arrive. In addition also as an extra security when logging on via an web browser on to the Reservation system

What redundancy is there in the system?

The system is seen as very reliable. A breakdown often appears in the installation and set-up phase (or because of poor planning).

If there however is an accident, the Bewator Entro has a range of technical solutions that eases a fast trouble-shooting and repair. E.g. removable, straight-through terminal blocks support even a change of parts when the system is still running (somewhat like plug-and-play).

Under normal, preventive efforts we think that Bewator Entro (with its integrated monitoring functions and distributed intelligence) is very good alternative with good redundancy to reasonable price level.

Why use battery-backup (UPS)?

One of the best insurances against breakdowns etc. is to install the necessary amount of battery-backed power supplies. A correct planning regarding number of doors, type of locks, distances, cable type etc. is then of course a prerequisite.

We recommend every SR34i (together with its doors) to have its own power supply, if it is possible. First because of it gives a “cleaner” installation. Secondly it is possible to connect a power fail signal from the power supply to the SR34i. Every segment of the system can then separately be monitored for main voltage breakdowns. An alarm event can be sent to the PC and/or an external alarm system (via IOR6).

What happens if an SR34i gets a short interruption?

Every SR34i as well as the PC have a complete copy of the database (mirroring). As long as the hardware is intact but an interruption occur (e.g. the data memory is corrupt) the data is recovered automatically through an up- or download. The stop of communication will generate an internal alarm to connected PC and/or an external alarm (via IOR6).

What happens if an SR34i fails?

Due to the SR34i's isolation capabilities the superior (global) communication will probably still work. If the door environment still has power and includes a DC22 (with memory) these will pass to an autonomic mode where decisions of access are taken locally. Other doors (without DC22) can be locked or unlocked. When the faulty SR34i is replaced it will automatically recover itself via a download from another SR34i (or PC). The event alarm functions still apply.

What happens if a reader fails?

In most cases other doors controlled by the same SR34i will still work. An alarm event will be sent from the actual SR34i because the actual door “disappears”.

What happens during a cable failure?

A stop in the global communication (between SR34i Segment Controllers) will be discovered and an alarm event is sent from every SR34i respectively. The doors can work as normal.

A stop in the local communication (between a SR34i and door) will be discovered by the actual SR34i and an alarm event is sent from actual SR34i. The doors can work as usual.

A stop in the communication with the PC has the same effect as if the PC is turned off. I.e. all data is still stored in the system (together with an amount of events). Then the communication is established again and the PC goes on-line – all events are transferred automatically.

Technical data

Bewator Entro software

- Software for control of up to 1000 systems, each capable of managing up to
 - 512 doors
 - 20 000 cards
 - 240 time schedules
 - 480 access groups
 - 128 zones (alarm, anti pass back, roll call and entrance limitation zones)
 - 16 system users in 4 levels + installer level
 - 14 holidays, 7 half days and 4 holiday periods in each time schedule
- 64 reservation objects (machine groups).
- Maximum of 10 IOR6 relays in each machine group.
- 32 time schedules with 24 intervals in each.
- Flexible interval reservation.
- Maximum number of reservations is 4000.
- Supplied on CD with accompanying manuals

Basic requirements for PC:

- Pentium processor 266 MHz
- 64 Mb RAM
- At least 20 MB free hard disk space
- CD-ROM drive
- VGA colour monitor
- Serial port for connection of segment controller/modem
- Local Area Network connection
- Windows 98/2000/XP or Windows NT version 4.0 or later
- MS Internet Explorer 5.0 or Netscape 4.7 (or above) is recommended as Web browser.

Basic requirements for network:

- Twisted pair Ethernet 10/100 Mbit/s connection.
- Communication between SR34i is done through TCP/IP.
- We recommend static/permanent IP-address for every SR34i (In some cases also Netmask and Gateway is needed).
- We recommend permanent, active Internet connection of SR34i (when Internet is used).

Note - when Internet connection is used, the following ports have to be open (in fire-walls or similar) and configured as follows:

- 1002 if communication is used between PC and the chosen SR34i.
- HTTP (port 80) when using reservation via Internet.
- 4011 for TCP when several SR34i communicates through LAN.
- SNTP (port 123) for fetching correct time, if SR34i uses TCP protocol between each other. SR34i Segment controller

InfoPoint IP810

- Reservation terminal for Bewator Entro.
- Colour screen with 400 x 200 resolution in 256 colours.
- Integrated proximity reader.
- Numeric keypad (0-9) and 10 function keys.
- Temperature range: +5° to +40°C
- Power supply: 10 – 35 V DC/AC.
- Power consumption: 350 mA (24V DC).
- Dimensions:
 - InfoPoint: 154 x 350 x 52 mm (HxWxD).
 - Flush mount box: 211 x 388 x 43 mm (HxWxD).
 - Cut out hole: 140 x 354 x 40 mm (HxWxD).

Segment controller for 4, 8, 16 or 32 doors

- Four built-in communication interfaces:
 - RS232 – for connection of PC, printer or modem. Max 25 m
 - RS485 global – for interconnection of up to 16 segment controllers
 - **Two** TCP/IP network connections 10/100 Mbit for communication via WAN/LAN
 - RS485 local – for connection of door readers
- Integrated network switch with one 'internal' and two external ports.
- Display and keypad for programming.
- Memory for 10 000 events.
- Lockable housing for wall mounting
- For installation inside in a dry environment only
- Temperature range: 0° to +50 °C
- Housing fitted with tamper switch
- Dimensions: 182 x 248 x 66 mm (HxWxD)
- Power supply: 8–40V DC or 8–30V AC
- Power consumption: 100 mA, 24V DC.
- RS232 interface:
 - 9600 baud
 - No parity
 - 8 bits
 - 1 start bit
 - 1 stop bit
 - Printer output with hardware handshaking (character table ISO 8859-1)

DC22 Door controller

- Door controller for 1 door and connection of up to two Bewator readers.
- 6 voltage free relay contacts.
 - Change over contact for control of electrical locking devices or similar.
 - Closing contact for control of a motor lock.
 - Change over contact for alarm by-pass, (Monostable, Bistable or Bistable pulse).
 - Closing contact for pre-warning during alarm activation cycle.
 - Closing contact for door held warning i.e. if a door remains open beyond the set time.
 - Alert relay for door alarm (e.g. when doors are forced open) or for motor lock control.
- Maximum load over the relay contacts: 2A, 30V DC.
- Opening time: 1–99 second.
- Exit request input with delay.
- Input for indication of intruder alarm status (red LED).
- Input for alarm by-pass activation e.g. from a time clock or the Alarm status feedback signal (ASF).
- Separate inputs for door & lock monitoring for closed/open door and locked/unlocked lock.
- Maximum reader load: 500 mA.
- Rectified DC output for door locks (input voltage less 1.5 volts at 500 mA maximum).
- Lockable housing for wall mounting.
- For installation inside in a dry environment only.
- Housing fitted with tamper switch.
- Temperature range: –35° to +50°C.
- Dimensions: 182 x 248 x 55 mm (HxWxD).
- Power supply: 8–40 V DC or 8–30 V AC.
- Power consumption: Max 60 mA, 24 V DC (excl reader).

DC12 Door controller

- Door controller for 1 door and connection of up to two Bewator readers.
- Opening relay for control of electric locking device or similar.
- Maximum load over the relay contacts: 2 A, 30 V DC.
- Opening time: 1–99 seconds.
- Exit request input with delay.
- Input for door monitoring. Indicates closed/open door.
- Maximum reader load: 500 mA.
- Lockable housing for wall mounting.
- For installation inside in a dry environment only.
- Housing fitted with tamper switch.
- Temperature range: –35° to +50°C.
- Dimensions: 128 x 250 x 54 mm (HxWxD).
- Power supply: 8–40 V DC or 8–30 V AC.
- Power consumption: Max 60 mA, 24 V DC (excl reader).

DCo1 Door controller

- Door controller for 1 door and control of door without reader.
- Opening relay for control of electric locking device or similar.
- Maximum load over the relay contacts: 2 A, 30 V DC.
- Opening time: 1–99 seconds.
- Exit request input with delay.
- Input for door monitoring. Indicates closed/open door.
- Lockable housing for wall mounting.
- For installation inside in a dry environment only.
- Housing fitted with tamper switch.
- Temperature range: –35° to +50°C.
- Dimensions: 80 x 120 x 40 mm (HxWxD).
- Power supply: 10–40 V DC or 8–30V AC.
- Power consumption: 100 mA.

DTo5 / DTo5Prox Door reader

- Door reader controlling 1 lock/door.
- Keypad with background illumination.
- Exit request input with delay.
- Opening relay for control of electric locking device or similar.
- Max load on relay contacts: 2A, 30V DC.
- Input for door monitoring. Indicates closed/open door.
- Cast metal housing with stainless steel keys.
- Housing fitted with tamper switch.
- Lockable housing in weatherproof design to IP54.
- Temperature range: DTo5: –35° to +50°C, DTo5Prox: –30° to +50°C.
- For flush mounting, use BB4 flush mounting box.
- In very exposed locations, use SH4 or SH1 protective cover.
- Dimensions: 160 x 110 x 47 mm (HxWxD).
- Supplied with drop box.
- Drop box dimensions: 80 x 120 x 40 mm (HxWxD).
- Power supply: 10–40V DC or 8–30 V AC.
- Power consumption: DTo5: 100 mA and DTo5Prox: 150mA.

BC43 / BC43Prox Card reader

- Remote card reader for DC22 or DC12 door controllers.
- Cast metal housing with stainless steel keys.
- Housing fitted with tamper switch.
- Keypad with background illumination.
- Lockable housing in weatherproof design according to IP54.
- Temperature range: BC43: –35° to +50°C, BC43Prox: –30° to +50°C.
- For flush mounting, use BB4 flush mounting box.
- In very exposed locations, use SH4 or SH1 protective cover.
- Dimensions: 160 x 110 x 47 mm (HxWxD).
- Power consumption: BC43: 50 mA and BC43Prox: 100mA.

BC16 Card only reader (UK Market)

- Card only reader to DC22/DC12 door controllers.
- Metal housing, surface mounted
- Temperature range: -20° to $+55^{\circ}\text{C}$.
- Dimensions: 89 x 34 x 24 mm (HxWxD).
- Power supply: + 5 V DC $\pm$ 10%.
- Power consumption: 60 mA.

BC18 Card reader

- Card reader only to DC22/DC12 door controllers.
- Metal housing.
- Temperature range: -10° to $+55^{\circ}\text{C}$.
With heater plate VS18 connected: -20° till $+55^{\circ}\text{C}$.
- Dimensions: 124 x 29 x 28 mm (HxWxD).
- Power supply: + 5 V DC $\pm$ 10%.
- Power consumption: 40 mA.

M43 Keypad

- Keypad to DC22/DC12 door controllers.
- Cast metal housing with stainless steel keys.
- Housing fitted with tamper switch.
- Keypad with background illumination.
- Lockable housing in weatherproof design according to IP54.
- Temperature range: -35° to $+50^{\circ}\text{C}$.
- Dimensions: 140 x 80 x 40 mm (HxWxD).
- Power consumption: 50 mA.

IOR6 Relay controller

- Relay controller for:
 - Lift control
 - Reservation function or
 - Timer control
 - Common alarm
 - Emergency opening
 - Power failure warning
- 6 voltage free relay outputs.
- Maximum load over the relay contacts: 60V, 0,9A (30V, 2A).
- 4 inputs.
- In Lift Control applications, up to 32 IOR6 can be connected in a system.
- Lockable housing for wall mounting.
- For installation inside in a dry environment only.
- Housing fitted with tamper switch.
- Temperature range: -35° to $+50^{\circ}\text{C}$.
- Dimensions: 140 x 200 x 60 mm (HxWxD).
- Power supply: 8–40 V DC or 8–30 V AC.
- Power consumption: 50 mA in standby mode, 200 mA with all relays activated.

Notes

This image shows a full page of blank, lined paper. It features approximately 28 horizontal blue or grey lines spaced evenly apart, typical of notebook paper. The lines extend across the entire width of the page, leaving small margins at the top and bottom. There are no vertical lines, text, or other markings on the page.

[illegible]

