

Manual 3060 System

Version: September 2006

If the contents of the foreign language version of the documentation differ from the contents of the original German version, the original German version shall apply in case of doubt. We reserve the right to make technical changes.

SimonsVoss Technologies AG • Feringastrasse 4 • 85774 Unterföhring • Germany
Hotline 01805-SV3060 • FAQs www.simons-voss.de
Telefon +49-89-99 228-0 • Fax +49-89-99 228-222

Simons  Voss
technologies

Table of Contents

Version: June 2006

Table of Contents

Seite 2

P

People to Contact

Sales
Technical
Address in Munich



D

Digital Locking System 3060

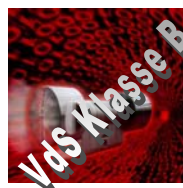
General method of operation
The components
Access control, time zone administration



V

Digital Locking Cylinder 3061 VdS

Method of operation
Installation instructions
Battery warning, battery replacement



H

Digital Half Cylinder 3061

Method of operation
Installation instructions
Battery warning, battery replacement



R

Digital Smart Relay 3063

Installation
Connections
Programming



Smart Output Module

Installation
Connections
Programming



T

Transponder 3064

Method of operation
Loss of a transponder
Password transponder



Table of Contents

Seite 3

Q

Biometric Transponder Q 3007

Method of operation
Learn state
Recognize state
Delete state



PinCode Keypad 3068

Method of operation
Installation
Programming



N

Network 3065

Network structure
Components
Installation



B

Shunt lock function 3066

Activation unit
Deactivation unit
Installation and connecting plan



E

Shunt lock function 3066 VdS

Master activation unit
Slave activation Unit
Deactivation Unit
VdS-compliant Installation



M

Programming Transponder 3067

Backup card
Error messages
Programming



P

PalmCD

Commissioning
Export and import
programming



Table of Contents

Seite 4

K

Key
Explanation of technical terms
Special Symbols



People to contact

Version: September 2006

People to contact

Page 2

SALES

If you have any questions please contact our specialist dealers, or the sales representative responsible for your region. You can obtain information concerning the responsible contact at the following telephone number.

+49 89-9 92 28-180

United Kingdom

SimonsVoss Technologies Ltd.
Mr. Oliver Quaisser
44 Newton Court, Old Windsor
Berkshire SL4 2SN
Great Britain
Tel. +44 / (0)1753 / 85 98 44
Fax +44 / (0)1753 / 83 17 03
Email: oliver.quaisser@simons-voss.co.uk

Singapore and Asia

SimonsVoss Security Technologies (Asia) Pte. Ltd.
Mr. Jason P. Kurek
72 B Pagoda Street
Republic of Singapore 059231
Tel. (65) 6227 7318
Fax (65) 6227 7018
Email: jpk@simonsvossasia.com

Middle East

SimonsVoss Technologies (Middle East) FZ-LCC
Dubai Internet City
P.O. Box 500188
Dubai, UAE
Tel. +9714 3629761
E-Mail: uae@simons-voss.com

Headquarters Munich

SimonsVoss Technologies AG
Feringastrasse 4
85774 Unterföhring
Germany

Tel: +49 89-9 92 28-180
Fax +49 89-9 92 28-222

www.simons-voss.com

Digital Locking System 3060

State of: June 2006

Digital Locking System 3060

Register



1.0	General Method of Operation	3
2.0	The Components of the Digital Locking and Organization System 3060	3
2.1	Software LDB	3
2.2	Programming	4
2.3	Digital Locking Cylinder 3061	4
2.4	Digital Smart Relay 3063	4
2.5	Transponder 3064	4
2.6	Network 3065	5
2.7	Block Lock Function 3066	5
3.0	Digital Components With Access Logging and Time Zone Control	5
3.1	Access Logging	5
3.2	Time Zone Control	6

1.0 General Method of Operation

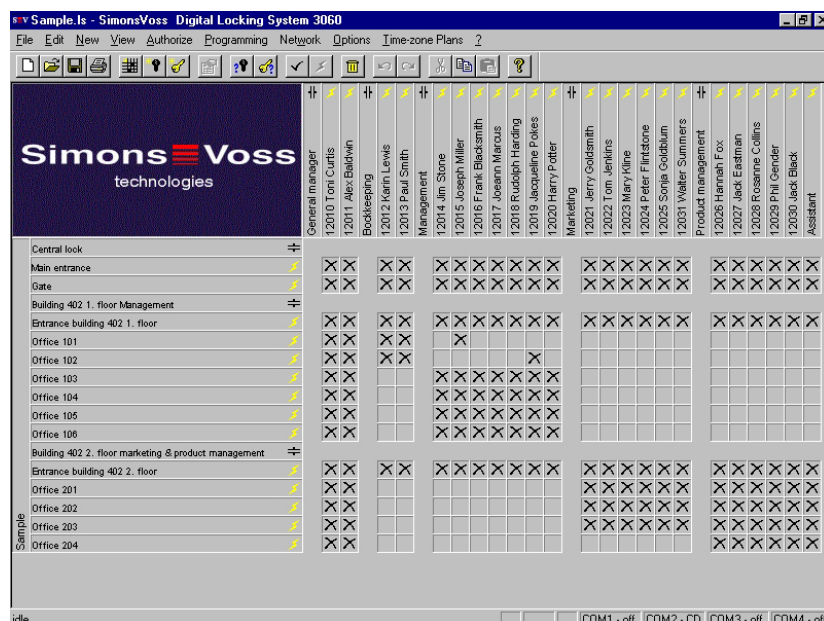
The Digital Locking and Organization System 3060 is modularly constructed and is suitable for uses ranging from a simple locking system for individual doors all the way to a complex PC-controlled access control system. Conventional mechanical keys are replaced by the programmable transponder, which controls doors, gates, barriers, furniture and elevators, for example, over radio transmission. Each transponder is programmed individually for the locking system. The access authorisations are assigned by means of the locking plan. This makes it possible to provide each employee with an individual locking plan with access control and time zone control. The identification in the system and the radio transmission are done by sending and receiving constantly changing crypto codes, thus making the misuse of the system technically practically impossible. Modifications or expansions of the system at a later date are always possible.

2.0 The Components of the Digital Locking and Organization System 3060

2.1 Software LDB

The locking plan software runs under Windows 98, Windows ME, Windows NT/2000 and Windows XP. All components can be programmed as required using the locking plan software. One locking plan can contain a maximum of 16,386 lockings and 8000 transponders. For even larger locking systems, the lockings and transponders are distributed among several locking plans. The locking authorisations are assigned by simply clicking with the mouse. As a result, later modifications are possible with no trouble.

☺ A detailed description is to be found in our Software Operating Instructions!



Digital Locking System 3060

Page 4

2.2 Programming



You will need the SmartCD and a PDA for programming the digital components. The data is encoded and then transmitted to the digital components via radio signal.



Another possibility for programming a Digital Locking Cylinder 3061 and Transponder 3064 is with the Programming Transponder 3067. For example, you can issue or change access authorizations in small systems by simply pressing a button when you lose a key or change the locking plan. No PC or special system software is needed.

2.3 Digital Locking Cylinder 3061



The Digital Locking Cylinder 3061 is a compact, powerful access control system that can be installed in any door in only minutes. Its dimensions correspond to those of an ordinary mechanical cylinder that meets the norms. Because the Digital Locking Cylinder 3061 has batteries (master and backup batteries), it can be installed without wires in all Euro Profile doors and can replace already

existing mechanical cylinders. A drop in the battery voltage is indicated by a multilevel warning system (service life approximately 60,000 operations).

2.4 Digital Smart Relay 3063



The SimonsVoss Smart Relay is an electronic switch that can be switched with a SimonsVoss transponder. You can use the SimonsVoss software to configure the authorisation for transponders that are permitted to operate the Smart Relay. In this way, the Smart Relay offers the full function of an access control reader.

2.5 Transponder 3064



The Transponder 3064 is a digital key that can be programmed using SimonsVoss software and that works by radio transmission, without contact. It not only replaces mechanical keys, but also takes over the function of identity cards. Simply pressing a button triggers the encoded communication between the transponder and locking

cylinder, Smart Relay or activation unit.

2.6 Network 3065

The cable-free Network 3065 is an online access control system that administers, visualises and archives all System 3060 information in one central location, and all without manipulations at the door, door frame or the door hardware.

It is especially recommended for medium-sized and large locking systems in order to be able to configure and administer the locking system from a central PC. The LON standard data transmission is done from the PC over the network wiring (twisted pair) and out to the network nodes (LockNodes), which are installed near a digital component. From the LockNode, the data is directed without wires over radio transmission to the digital unit.

- ☺ While it is true that access to the network software is no longer possible if there is a power failure (unless the network has been protected by a no-break power supply), however, all of the locking system's components that are equipped with a battery still function.

2.7 Block Lock Function 3066

SimonsVoss has the Block Lock Function 3066 in its product line as an option of the Digital Locking and Organization System. This function offers the possibility of activating your alarm system from a central point while at the same time preventing the monitored doors from being accidentally opened during this time. This rules out annoying and expensive false alarms right from the start.

The Block Lock Function 3066 is also available as a VdS version.

3.0 Digital Components With Access Logging and Time Zone Control

3.1 Access Logging

The Plus versions of the digital locking cylinder, SmartRelay and activation unit record the access attempts of authorised transponders. The read-out of the access list from the lockings is done using the SmartCD or, in the case of a networked locking system, over the LockNodes.

A total till 128 accesses (with Smart Relay 1.024), with date, time of day and transponder designation can be stored in the access lists of the separate components. After that, the complete file isn't deleted, but instead the oldest access is always overwritten with the new one.

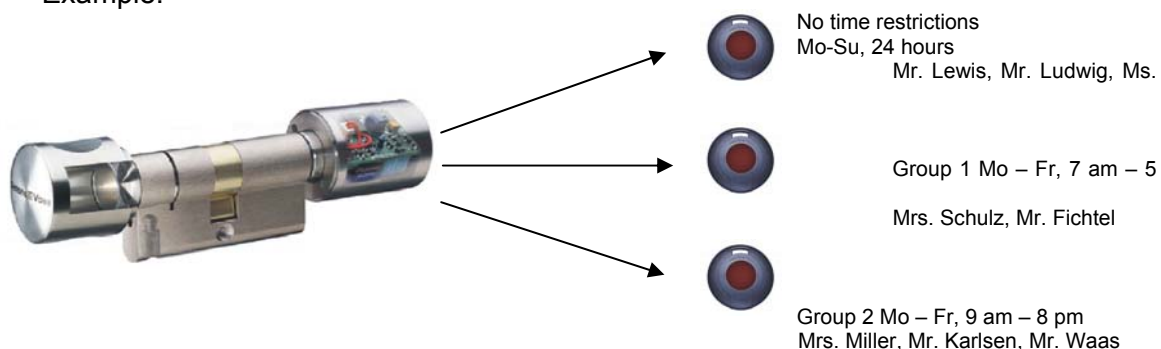
After the access list has been read out with the programming device or network nodes, it is imported into the PC and administered there by the locking plan software. A total of 10,000 accesses can be stored in the PC file. When the data is accepted from the programming device, a comparison is done so that it is always only the current, new accesses that are accepted into the PC file.

3.2 Time Zone Control

You can program lockings in such a way that authorised transponders are authorised for access only at certain times.

Transponders normally have no time restrictions, i.e., that are always authorised for locking 7 days a week, 24 hours a day. However, you can assign transponders to time groups so that they can open or lock at times that can be freely defined. There are five different time groups available (for a more precise description, see the Software Operating Instructions).

Example:



You can draw up an individual time zone plan for each locking.



It is **not** possible to equip a standard version with the access logging and time zone control functions of the TZC-version at some later time.

Digital Locking Cylinder 3061 VdS

State of: September 2006

Digital Locking Cylinder 3061 VdS

Page 2

1.0	Method of Operation	3
1.1	General Information	3
1.2	Opening and Locking From Outside	3
1.3	Opening and Locking From Inside	3
2.0	Special Models	4
2.1	FH Version	4
2.2	Overview	4
3.0	Additional Functions	4
3.1	OMRON	4
3.2	Extending the Coupling Time	4
3.3	Logging Unauthorized Access Attempts	5
3.4	No Acoustic Programmer Acknowledge	5
4.0	Battery Warnings	5
4.1	Locking Cylinder	5
4.2	Transponder	6
5.0	Battery Replacement	6
6.0	Installation Instructions	7
6.1	General Information	7
6.2	Programming the Locking Cylinder	7
6.3	Removing the Outer Knob	7
6.4	Inserting the Digital Cylinder Into the Lock	8
6.5	Screw On the Outer Knob	8
6.6	Perform Function Test	8
7.0	Potential Applications	8
7.1	General Information	8
7.2	Fire Protection Doors	8
7.3	SLP Locks	8
8.0	Data Sheet	9

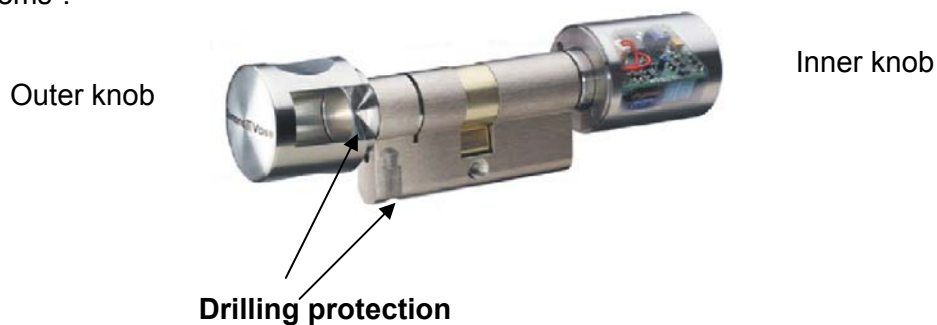
Digital Locking Cylinder 3061 VdS

Page 3

1.0 Method of Operation

1.1 General Information

The Digital Locking Cylinder 3061 VdS meets the requirements of VdS (Association of German Property Insurers) Class B and its outer dimensions exactly match those of a standard mechanical cylinder. In comparison to mechanical systems, it excels because it is very easy to install, provides greater security, is more flexible and costs less to operate. It can quickly and easily replace existing mechanical cylinders in "old systems".



1.2 Opening and Locking From Outside

When not activated, the outer knob turns freely. It is not possible to open the door or to lock it. Hold the transponder at a distance of approximately 10 to 40 cm (4 to 16 inches) from the digital locking cylinder and briefly press the transponder button once. If this is an authorised transponder, a double signal tone sounds and the cylinder couples. Now turn the outer knob in the locking or opening direction. You have approximately five seconds for this process. You can use the software to adjust the coupling time. The longer the coupling time, however, the shorter the service life of the battery. Then a single signal tone sounds and the outer knob turns freely again. Make sure that the outer knob of the locking cylinder turns freely again after the coupling process.

👉 If this transponder is not authorised at this time because of the time zone plan, a single signal tone sounds. The cylinder does not couple, however, and you cannot open the door.

1.3 Opening and Locking From Inside

It is always possible to open doors with Digital Locking Cylinder 3061 VdS devices from the inside without operating the transponder

2.0 Special Models

The standard Digital Locking Cylinder 3061 VdS is equipped as a TZC version, which means that the following functions are always included:

- | | |
|-------------------|---|
| Access logging | The locking cylinder stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the PalmCD2 or over the network. |
| Time zone control | You can program locking cylinders in such a way that authorised transponders are authorised for access only at certain times. |

The Digital Locking Cylinder 3061 VdS is also available in the following optional versions:

2.1 FH Version

For doors with thick metal inserts (such as fire protection doors) or with a large screening effect. This version is also used in areas with strong interference fields, such as in server rooms.

2.2 Overview

Locking Cylinder (TZC)

- Entrance doors
- Residential doors
- Office doors
- Interconnecting doors

Locking Cylinder FH (TZC)

- Fire protection doors
- Aluminium doors

3.0 Additional Functions

You can activate the following functions with the software settings:

3.1 OMRON

All product versions can be operated in OMRON mode. You will find a detailed description in the Smart Relay manual.

3.2 Extending the Coupling Time

The default time for the coupling of the cylinder is approximately 5 seconds. You can use the software to extend this time to approximately 10 seconds. This shortens the lifetime of the battery, however.

3.3 Logging Unauthorised Access Attempts

For cylinder version 10.2 and later and in combination with the LDG Version 1.40, it is possible to log unauthorised access attempts, as well as authorised accesses. This includes both access attempts without authorisation and access attempts outside the specified time zone. In this connection, however, only transponders from the locking system are logged, which means that the transponder must have the same locking system ID (SID).

3.4 No Acoustic Programmer Acknowledge

When programming over the network, it can be advantageous to deactivate the acoustic programmer acknowledge. You can do that with this function.

4.0 Battery Warnings

4.1 Locking Cylinder

Warning level 1 for main battery

If the main battery of the locking cylinder goes empty, eight short signal tones, coming quickly one after another, sound after you operate the transponder and before the cylinder couples. You must replace both batteries now.

Warning level 2 for backup battery (SW Version 10.0 & SW Version 10.1)

In addition to the main battery warning, an additional eight short signal tones, coming quickly one after another, now sound for the backup battery warning. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 2 for backup battery (SW Version 10.2 and later)

Now the signal tones of the backup battery warning sound for only approximately 30 seconds (without the main battery warning). The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 3 (SW Version 10.2 and later)

If you continue to ignore this backup battery warning, either the door can be used 50 more times or the cylinder switches off after 4-5 weeks if there is no further operation. In both cases, the cylinder switches into the so-called storage mode. After this, you can only open the cylinder with the programming device.

4.2 Transponder

If the transponder battery voltage is coming to an end, eight short signal tones, coming quickly one after another, sound each time the transponder is operated on the locking cylinder after the uncoupling.

- ⚠ Attention: Do not take out the transponder battery because this will probably result in the loss of data. See the "Transponder 3064" manual for more information.

5.0 Battery Replacement

Only authorised personnel are permitted to replace the battery. Use only batteries that are supplied by SimonsVoss.

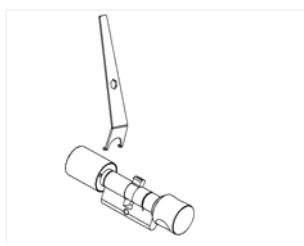


Fig. 1

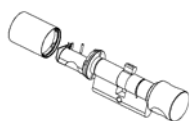


Fig. 2

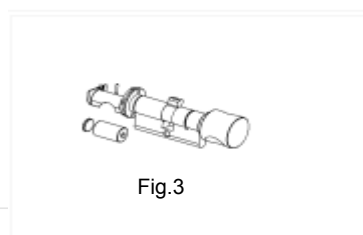


Fig. 3

Use the special tool to loosen the locknut (Fig. 1) on the inner knob (long knob) approximately one rotation (only loosen slightly, do not unscrew completely). Carefully push the inner knob back and forth so that the sealing cone loosens and then unscrew the inner knob completely (Fig. 2).

Note: Only push the inner knob to the side very lightly because otherwise you may damage the electronics.

- ⚠ When changing batteries, always change both batteries.

Insert the main battery into the holding device with the positive pole toward the door and the backup battery in the opposite direction (Fig. 3).

- ⚠ Reversing the polarity can result in damage to the locking cylinder. Incorrect handling of the batteries used in this device can result in the risk of fire or burns. Do not charge, open, heat to more than 100 °C (212 °F) or burn. Replace the batteries only with original batteries supplied by SimonsVoss.
- ⚠ Please dispose of lithium batteries immediately when discharged. Store away from children, do not open and do not throw into fire.
- ⚠ Never operate the cylinder without a main battery because otherwise the entire power consumption of the cylinder runs over the backup battery.

Fix the lock nut in position with the special tool and press it against the flange. Now turn the inner knob onto the screw thread until the stop and tighten the locknut firmly. Now operate an authorised transponder and test the function.

- 👉 Please dispose of discharged lithium batteries immediately. Store away from children, do not open and do not throw into fire.
- 👉 You must reset the time of day after the battery change because the clock does not work without current (Software Operating Instructions: Programming → Setting the Clock on the Locking).

6.0 Installation Instructions

6.1 General Information

When installing the Digital Locking Cylinder, make sure that there are no sources of interference in the vicinity. You should install locking cylinders at least 0.5 m (approximately 1.5 feet) from one another and control units or Smart Relays at a distance of at least 1.5 m (approximately 5 feet). The PC housing of the half cylinder is not allowed to stick out into the exterior area more than 3 mm. If necessary, attach a profile cylinder rosette. Furthermore, you must ensure that no water can penetrate the cylinder in the area of the catch

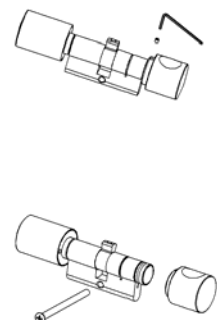
6.2 Programming the Locking Cylinder

You must program the Digital Locking Cylinder and accompanying transponders in the locking plan before you install them. Please refer to the Software Operating Instructions for more detailed information.

- 👉 The locking cylinders are delivered in so-called storage mode, which means that no communication is possible with the transponder (exception: programming transponder). You can also use software and the programming device to remove the storage mode. Please refer to the Software Operating Instructions for more detailed information.

6.3 Removing the Outer Knob

Loosen the setscrew on the outer knob (short knob) with a 1.5 mm Allen key (do not screw the whole way off). Operate an authorised transponder and hold the inner knob still. The locking cylinder couples and you can unscrew the outer knob by turning it counterclockwise.



6.4 Inserting the Digital Cylinder Into the Lock

First turn the lock pin until it is pointing straight down. Then insert the Digital Locking Cylinder through the lock so that the inner knob (long knob) points toward the inside of the door. Fasten the cylinder with the lock screw included in the delivery

Never hit against the knobs during installation. Do not bring the cylinder into contact with oil, paint or acid.

6.5 Screw On the Outer Knob

Screw the outer knob on the screw thread, fixing it in position with your fingers if necessary. Then operate the transponder. Hold the inner knob still and tighten the outer knob solidly. Finally, tightly screw the setscrew with the Allan key.

6.6 Perform Function Test

1. With the door open, turn the inner knob in the locking and opening directions. The knob must turn easily.
2. Close the door and repeat the process. If the locking cylinder is stiff, you must align the door or correct the edge plate.
3. Then perform the same test on the outer knob. To do this, operate an authorised transponder near the cylinder.

7.0 Potential Applications

7.1 General Information

The Digital Locking Cylinder fits locks for Euro Profile Cylinders that meet DIN 18254 specifications.

7.2 Fire Protection Doors

It is possible to install the locking cylinder in fire protection doors. In this case, use the Locking Cylinder Version FH. The approval for a fire protection door is always unaffected by the locking cylinder.

7.3 SLP Locks

The Digital Locking Cylinder 3061 FD is used for applications of this type. The Digital Locking Cylinder 3061 VdS does not have approval for SLP doors at this time. See the "Digital Locking Cylinder 3061" manual → "Possible Applications."

Digital Locking Cylinder 3061 VdS

Page 9

8.0 Data Sheet

Knobs	Material	Stainless steel
	Colours	Brushed stainless steel
	Diameter	Brass 30 mm
FH cylinder knobs	Material	Outer knob stainless steel, inner knob plastic
	Colour	Black
	Diameter	30 mm
Profile cylinders	Standard length	Outside 30 mm, inside 30 mm
	Construction length	In 5 mm increments (no kit) up to a total length of 140 mm, where one side of the cylinder can have a max. length of 90 mm. Other lengths upon request.
Battery	Type	Lithium 3.6 V, 1/2 AA Lithium 3 V, CR1220 Use only original replacement batteries from SimonsVoss
	Service life	Approx. 60,000 operations, or 4 years Standby or approx. 4 years
Environmental Conditions	Operating temperature	-20°C to +50°C (-4° F to +122° F)
	Storage temperature	-35°C to +50°C (-31°F to +122°F)
	Degree of protection	IP54 (when installed)

Digital Half Cylinder 3061

State of: September 2006

Digital Half Cylinder 3061

Content



1.0	Method of Operation	4
1.1	General Information	4
1.2	Opening and Locking	4
2.0	Special Models	4
2.1	PLUS Version	4
3.0	Additional Functions	5
3.1	OMRON	5
3.2	Extending the Coupling Time	5
3.3	Logging Unauthorized Access Attempts	5
3.4	No Acoustic Programmer Acknowledge	5
4.0	Battery Warnings	6
4.1	Half Cylinder	6
4.2	Transponder	6
5.0	Battery Replacement	7

Digital Half Cylinder 3061

Content

6.0	Installation Instructions	8
6.1	General Information	8
6.2	Programming a Half Cylinder	8
6.3	Installing in Doors	8
6.4	Installation Behind Blanks for Half Cylinders With 3 <u>Setscrews</u>	9
	(New Flange Mounting)	9
6.4.1	Removal of the Knob and Flange of the Half Cylinder	9
6.4.2	Installing the Knob and Flange of the Half Cylinder	10
6.5	Installation Behind Blanks for Half Cylinders With 2 <u>Setscrews</u>	11
	(Old Flange Mounting)	11
6.5.1	Removal of the Knob and Flange of the Half Cylinder	11
6.5.2	Installing the Knob and Flange of the Half Cylinder	11
6.6	Perform Function Test	12
7.0	Data Sheet	13

1.0 Method of Operation

1.0 General Information

The outer dimensions of the Digital Half Cylinder exactly match those of a mechanical cylinder complying with DIN 18252. Please ask for approved self-locking and anti-panic locks at the manufacturer.

1.1 Opening and Locking

When not activated, the outer knob turns freely. It is not possible to open the door or to lock it. Hold the transponder at a distance of approximately 10 to 40 cm (4 to 16 inches) from the digital half cylinder and briefly press the transponder button once. If this is an authorised transponder, a double signal tone sounds and the cylinder couples. Now turn the outer knob in the locking or opening direction. You have approximately five seconds for this process. Then a single signal tone sounds and the outer knob turns freely again. Make sure that the outer knob of the half cylinder turns freely again after the coupling process.



If this is a transponder that is not authorised at this time because of the time zone plan, a single signal tone sounds. The cylinder does not couple, however, and you cannot open the door.

2.0 Special Models

The Digital Half Cylinder 3061 is also available in the following optional versions:

2.0 PLUS Version

Design is similar to the standard version but with access logging and time zone control.

Access logging	The locking cylinder stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the SmartCD or over the network.
Time zone control	You can program locking cylinders in such a way that authorised transponders are authorised for access only at certain times.
Weatherproof	This version is also approved for outdoor use. The knob is certified to IP 65.
Multi-ratchet	A spring mechanism (with 8 ratchet-points) prevents the key tab from turning with the knob when not coupled (e.g. for use in key-switches).

3.0 Additional Functions

3.1 OMRON

All product versions can be operated in OMRON mode. You will find a detailed description in the Smart Relay manual.

3.2 Extending the Coupling Time

The default time for the coupling of the cylinder is approximately 5 seconds. You can use the software to extend this time to approximately 10 seconds. This shortens the lifetime of the battery, however.

3.3 Logging Unauthorised Access Attempts

For cylinder version 10.2 and later and in combination with the LDB Version 1.40 and later, it is possible to log unauthorised access attempts, as well as authorised accesses. This includes both access attempts without authorisation and access attempts outside the specified time zone. In this connection, however, only transponders from the locking system are logged, which means that the transponder must have the same locking system ID (SID).

3.4 No Acoustic Programmer Acknowledge

When programming over the network, it can be advantageous to deactivate the acoustic programmer acknowledge. You can do that with this function.

4.0 Battery Warnings

4.1 Half Cylinder

Warning level 1 for main battery

If the main battery of the half cylinder goes empty, eight short signal tones, coming quickly one after another, sound after you operate the transponder and before the cylinder couples. You must replace both batteries now.

Warning level 2 for backup battery (SW Version 10.0 & SW Version 10.1)

In addition to the main battery warning, an additional sixteen short signal tones, coming quickly one after another, sound for the backup battery warning. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 2 for backup battery (SW Version 10.2 and later)

In addition to the main battery warning, the signal tones of the backup battery warning now sound for approximately 30 seconds. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning Level 3 (SW version 10.3 and later)

If you continue to ignore the backup battery warning, either the door can be used 50 more times or the cylinder switches off after ca. 4 weeks if there is no further operation. In both cases, the cylinder switches into the so-called storage mode. After this, you can only open the cylinder with the programming device.

4.2 Transponder

If the transponder battery voltage is coming to an end, eight short signal tones, coming quickly one after another, sound each time the transponder is operated and after the uncoupling. (look at manual digital-locking-cylinder 3061)






Attention: Do not take out the transponder battery because this will probably result in the loss of data. See the "Transponder 3064" manual for more information.

5.0 Battery Replacement

Only authorised personnel are permitted to replace the battery. Use only batteries that are supplied by SimonsVoss.

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders.
2. Use an authorised transponder to couple the cylinder and unscrew the knob by turning it counter-clockwise. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
3. Replace the main and emergency batteries. Make sure that the polarity is correct.
4. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. Make sure that the knob is screwed on up to the stop (important for the function). While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
5. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.
6. Now operate an authorised transponder and test the function.

Dispose of used batteries immediately, keep out of reach of children, do not open and do not throw into a fire!

-  Reversing the polarity can result in damage to the locking cylinder. Incorrect handling of the batteries used in this device can result in the risk of fire or burns. Do not charge, open, heat to more than 100° C (212° F) or burn.
-  Never operate the cylinder without a main battery because otherwise the entire power consumption of the cylinder runs over the backup battery.
-  For PLUS versions, you must reset the time of day after the battery change because the clock does not work without current (Software Operating Instructions: Programming → Setting the clock on the locking).

6.0 Installation Instructions

6.1 General Information

Only trained and authorised personnel are permitted to perform the installation. The battery used in the cylinder can present a risk of fire and burns if not handled correctly! Do not charge, open, heat to more than 100° C (212° F) or burn! Do not short-circuit! When installing the digital half cylinder, make sure that there are no sources of interference in the vicinity. You should install half cylinders at least 0.5 m (approximately 1.5 feet) from one another and Smart Relays or activation units at a distance of at least 1.5 m (approximately 5 feet). The PC housing of the half cylinder is not allowed to stick out into the exterior area more than 3 mm. If necessary, attach a profile cylinder rosette. Furthermore, you must ensure that no water can penetrate into the cylinder in the area of the catch.

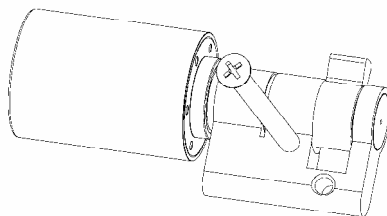
6.2 Programming a Half Cylinder

You must program the digital locking cylinder and accompanying transponders in the locking plan before you install them. Please refer to the Software Operating Instructions for more detailed information.

- 👉 The locking cylinders are delivered in so-called storage mode, which means that no communication is possible with the transponder (exception: programming transponder). You can also use software and the programming device to remove the storage mode. Please refer to the Software Operating Instructions for more detailed information.

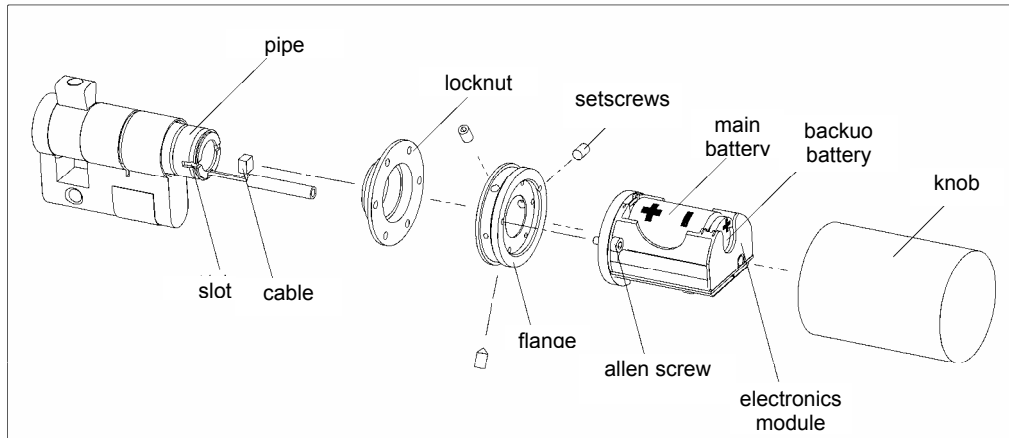
6.3 Installing in Doors

Insert the cylinder through the lock from the outside of the door towards the inside and secure it with the lock screw.



- 👉 Never hit against the knobs during installation. Do not bring the cylinder into contact with oil, paint or acid.

6.4 Installation Behind Blanks for Half Cylinders With 3 Setscrews (New Flange Mounting)



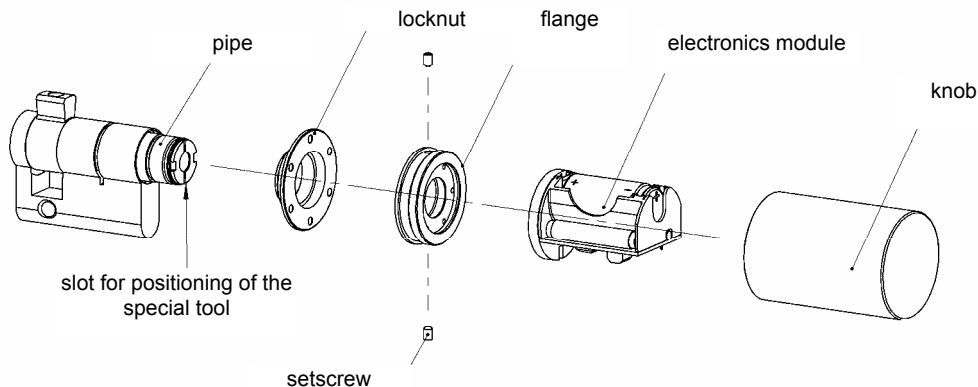
6.4.1 Removal of the Knob and Flange of the Half Cylinder

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders. (If the locknut is already bumping into the profile, then start to unscrew the knob as described in the following point (approximately one rotation) and continue).
2. Use an authorised transponder to couple the cylinder and then unscrew the knob. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
3. Carefully pull the cable out of the socket-contact in the electronics but do not remove the insulation sleeving. The electronic covering is thermally welded on and also remains on the unit.
4. Remove the two Allen screws that are parallel to the battery from the flange with an Allen key (1.5 mm). Remove the electronics module.
5. Remove the three setscrews on the outer circumference of the flange (same Allen key).
Note: If you can see two setscrews here, this cylinder has an old flange mounting (in this case, refer to Point 6.5).
6. Remove the flange and locknut.
7. Now you can install the blank.

6.4.2 Installing the Knob and Flange of the Half Cylinder

1. Put on the locknut. The flat surface with the bore holes faces away from the cylinder.
Note: If you cannot see any screw thread on the end of the pipe, this cylinder has a new flange mounting (in this case, refer to Point 6.4).
2. Put the flange onto the end of the pipe; the side of the flange with the screw thread faces away from the cylinder. The flange contains a crosspin that sticks out of the interior diameter. This crosspin must catch in the longitudinal slot of the pipe. Push the flange up against the stop on the pipe.
3. Holding it in this position, fix the three setscrews very tightly with the Allen key (1.5 mm). Check whether the setscrews are really tightly screwed, because this is important for correct functioning.
4. Fix the electronics module to the flange with the Allen screws that are parallel to the battery (same Allen key as above). Guide the cable through the recess next to the connector. Make sure that the cable is not pinched.
5. Connect the cable to the electronics socket and lay it so that it is flat on the electronics covering and not in the way when screwing on the knob (danger of pinching).
6. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. Make sure that the knob is screwed on up to the stop (important for the function). While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
7. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.

6.5 Installation Behind Blanks for Half Cylinders With 2 Setscrews (Old Flange Mounting)



6.5.1 Removal of the Knob and Flange of the Half Cylinder

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders.
2. Use an authorised transponder to couple the cylinder and then unscrew the knob. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
3. Carefully pull the cable out of the socket-contact in the electronics but do not remove the insulation sleeving. The electronic covering is thermally welded on and also remains on the unit.
4. Remove the two Allen screws that are parallel to the battery from the flange with an Allen key (1.5 mm). Remove the electronics module.
5. Remove the setscrew on the outer circumference of the flange (same Allen key). Note: If you can see 3 setscrews here, this cylinder has a new flange mounting (in this case, refer to Point 6.4)
6. The fore-part of the pipe, which sticks out of the profile, contains two slots on which you can position the special tool (offset 90° to the lengthwise slot which guides the cable). The narrow end of the installation tool can move into this slot. This ensures that the pipe cannot twist.
7. Now you can unscrew the flange without the pipe also turning.
8. Remove the locknut.
9. Now you can install the blank.

6.5.2 Installing the Knob and Flange of the Half Cylinder

1. Put on the locknut. The flat surface with the bore holes faces away from the door.
Note: If you cannot see any screw thread on the end of the pipe, this cylinder has a new flange mounting (refer to Point 6.4).
2. Please note the two lateral impressions on opposite sides of the pipe. The lateral setscrews of the flange must fit into this later in order to guarantee that

the flange holds securely. To find the exact position quickly, the flat surfaces of the pipe and flange have black markings that must line up.

3. Put the flange on the end of the pipe without screwing it in. The side with the small outside diameter points towards the door. The fore-part of the pipe, which sticks out of the profile, contains two slots in which you can position the special tool (offset 90° to the lengthwise slot which guides the cable). The narrow end of the installation tool can move into this slot. This ensures that the pipe cannot twist.
4. The pipe should not turn during the following steps (see Point 3). Lightly screw on the flange until it reaches the stop and the markings line up. In this position, tighten the two setscrews with the Allen key (1.5 mm) so that they center in the indentations of the pipe. Then tighten both setscrews securely. Please check whether the setscrews are really tightly screwed, because this is important for correct functioning!
5. Fix the electronics module to the flange with the Allen screws that are parallel to the battery (same Allen key). Make sure that the cable is not pinched.
6. Connect the cable to the electronics socket and lay it so that it is flat on the electronics covering and not in the way when screwing on the knob (danger of pinching).
7. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
8. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.

6.6 Perform Function Test

1. Operate an authorised transponder and turn the knob in the lock and open directions when the door is open. The knob must turn easily.
2. Close the door and repeat the process. If the locking cylinder is stiff, you must align the door or correct the edge plate.

7.0 Data Sheet

Dimensions	Standard length	30/10 mm
	Standard length Multirast (MR)	30/15 mm
	Max. profile length	100 mm (in 5mm intervals)
	Knob diameter	33,5 x 30 mm
	Knob length	51.5 mm (distance from knob end to profile fore-part)
	Standard for profile dimensions	DIN 18252
Battery	Batteries	Lithium, 3.6V, ½ AA, 900mAh Lithium 3V, CR1220 Use only original replacement batteries from SimonsVoss
	Service life	Max. 50,000 operations or roughly 4 years
Environmental Conditions	Operating temperature range	-20°C to +50°C (-4°F to +122°F)
	Storage temperature range	-35°C to +50°C (-31°F to +122°F)
	Degree of protection	IP 54 (when installed)
		IP 65 knop VW Option (when installed)

**Smart Relay:
SREL, SREL.ZK, SREL.AKV**

State of: September 2006

Smart Relay: SREL, SREL.ZK, SREL.ADV

Content

1.0	Important Information	4
2.0	Product Description	4
3.0	Before Ordering	5
3.1	Determine Which Version of the Smart Relay you need	5
3.2	Determine Which Accessories you need	5
3.3	Dimension and Procure Power Supplies	5
3.4	Determine the Installation Position	6
3.5	Additional Information:	6
4.0	Before Installation	6
4.1	Installation of the Backup battery	7
5.0	Installation	8
6.0	Connection Assignments	9
6.1	SREL and SREL.ZK	9
6.2	SREL.ADV	10
6.3	Description of the SREL, SREL.ZK and SREL.ADV Connection	10
7.0	Programming and Configuration	11
7.1	Access control	12
7.2	Time zone control	12
7.3	Overlay	12
7.4	Flip Flop	12
7.5	Repeater	12
7.6	Time switching	12
7.7	OMRON	13
7.7.1	The Smart Relay in OMRON Mode	14
7.8	No acoustic programmer acknowledge	15
7.9	External beeper/ External LED	15
7.10	Internal/ external antenna	15

Smart Relay: SREL, SREL.ZK, SREL.ADV

Content

7.11	Number of expansion modules _____	15
7.12	Pulse length _____	15
7.13	Interface _____	16
7.14	Restricted range _____	16
7.15	External Beeper/ External LED _____	16
7.16	Log unauthorised accesses _____	17
8.0	Serial Interface _____	18
8.1	Functional Description _____	18
8.2	Wiegand Interface (32 bit and 26 bit) _____	18
8.3	Kaba Benzing, Siemens, Gantner Legic, Primion, Isgus Interface	19
9.0	Maintenance _____	19
9.1	Battery Warning and Battery Replacement if you are using the SREL.BAT battery _____	19
9.2	Backup Battery _____	20
10.0	Data sheet _____	21

1.0 Important Information

Safety remark:

Caution! – Incorrect handling of the batteries and storage batteries used in this product can result in the risk of fire or burns. Do not charge, open or burn these batteries or heat them to more than 100 °C (212 °F).

Installation of a SimonsVoss Smart Relay requires knowledge in the areas of door mechanics, door certifications, installation of electronics and the use of the SimonsVoss software. For this reason, only trained and authorised personnel should install the unit.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect installation.

Incorrectly installed Smart Relays may block the access through a door. SimonsVoss AG is not liable for the consequences of incorrect installation, such as blocked access to injured or endangered persons, property damage or other damages.

If you will be storing the Smart Relay for more than one week, remove the backup battery.

The Smart Relay must be installed in compliance with ESD (electrostatic discharge) guidelines. In particular, contact with the printed circuit boards and the switching circuits integrated on them must be avoided.

2.0 Product Description

The SimonsVoss Smart Relay is an electronic switch that you can switch with a SimonsVoss transponder. You can use the SimonsVoss software to configure the authorisation for transponders that are permitted to operate the Smart Relay. As a result, the Smart Relay offers the full function of an access control reader.

3.0 Before Ordering

3.1 Determine Which Version of the Smart Relay you need

1. Smart Relay basic version: ordering code SREL

This relay allows simple yes/no authorisation for up to 8184 different transponders.

2. Smart Relay TZC version with access logging and time zones: ordering code SREL.ZK.

Like the basic version, but with the capability of separately switching on access logging for the last 1024 accesses (for firmware version 4.0.01.15 and later), with date and time, or day-time zones for up to five groups of people, and automatic locking and unlocking.

3. Smart Relay Advanced version, ordering code SREL.ADV

Like the TZC version, but with the following additional functions:

- Connection for external modules using a three-wire bus
- Connection of an extended antenna
- Connections for serial interfaces to external time recording terminals or access control readers
- Connection for external LED or buzzer

3.2 Determine Which Accessories you need

Extended antenna for unfavourable reception conditions ordering code: SREL.AV

Battery only for SREL, SREL.ZK and SREL.ADV in case you will be operating these products without an additional supply voltage: ordering code SREL.BAT

3.3 Dimension and Procure Power Supplies

These power supplies are necessary for all Smart Relays that will not be battery operated. The power supply should have an output of no more than 15 watts and should be capable of delivering voltage of 12 VAC or 5 to 24 VDC when the current is 100 mA.

Attention! Do not use any switched-mode power supplies near the Smart Relays.

The customer must provide all power supplies; they are not available from SimonsVoss.

3.4 Determine the Installation Position

The range from the transponder to the Smart Relay (reader range) is a maximum of 1.5 m (5 feet), but can be dampened by a metal environment (particularly by strong magnetic fields or aluminium).

Ideally, you should conduct a range test with an authorised transponder and a battery-operated Smart Relay.

3.5 Additional Information:

- All cables for connecting to the Smart Relay should be type IY(ST)Yx0.6 (Twisted-Pair shielded cable). The maximum cable length should not exceed 100 m (approximately 330 feet). At the same time, you must take into account the power losses when you dimension the supply voltage.
- You must take into consideration the technical specifications for the inputs and outputs (see Technical Data)
- You must lay and connect all cables according to VDE standards.

4.0 Before Installation

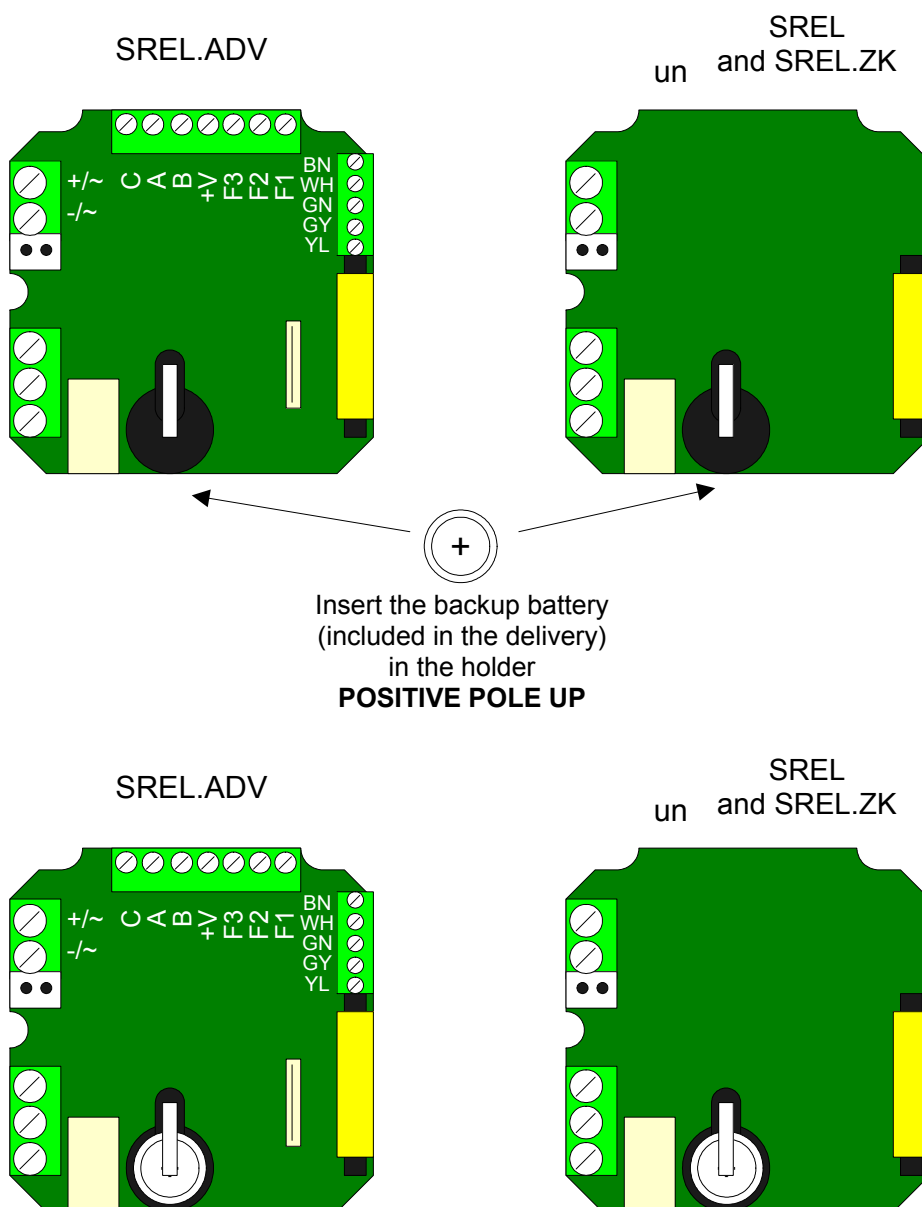
- Unpack the Smart Relay and check for any damages.
- Connect the Smart Relay to a supply voltage or battery.
- If you are operating the Smart Relay with a power supply, insert the backup battery included in the delivery into the holder provided for it (see Installation of the Backup Battery).
- Verify the function of the Smart Relay with a transponder in the condition as received from the factory.
- If you are installing the Smart Relay in a flush socket device, remove the housing.
- If you are installing the Smart Relay on the wall, you can use the bottom plate as a template for the bore holes (6 mm).

Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 7

4.1 Installation of the Backup battery

Insert the battery only if you will be operating the Smart Relay with the power supply. Do not insert this battery if you will be operating with the SREL.BAT!



5.0 Installation

- Switch off the supply voltage (if necessary, pull out the plug or disconnect the battery).
- Connect all cables to the terminals provided on the Smart Relay (see Connection Assignments on the following page)

If you are connecting a direct current power supply, make sure that you get the polarity right.

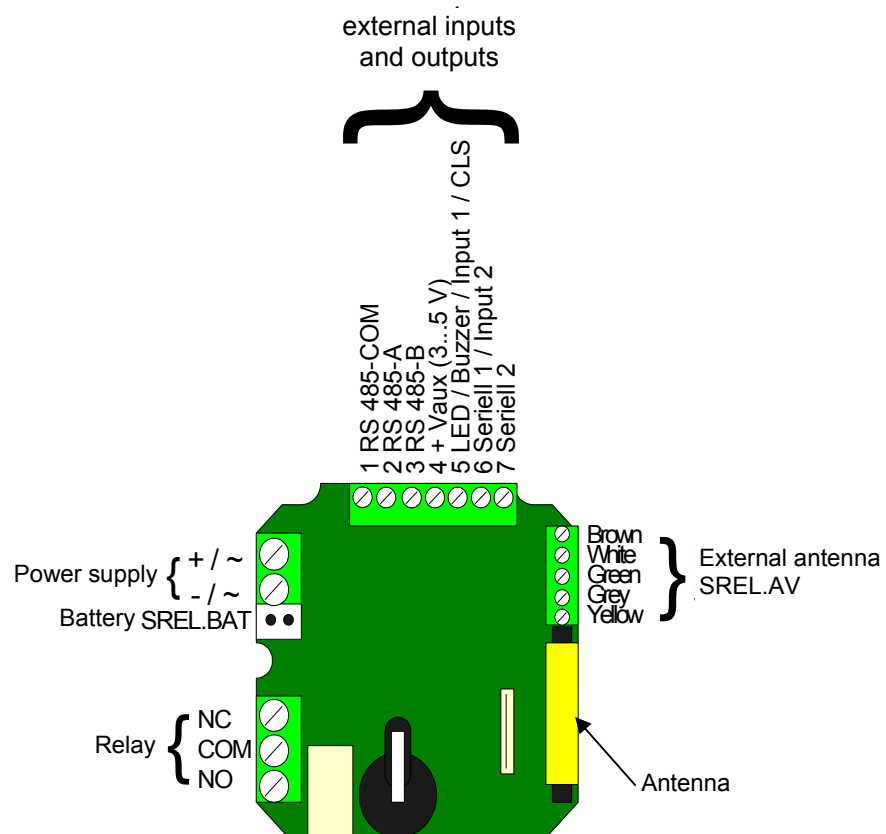
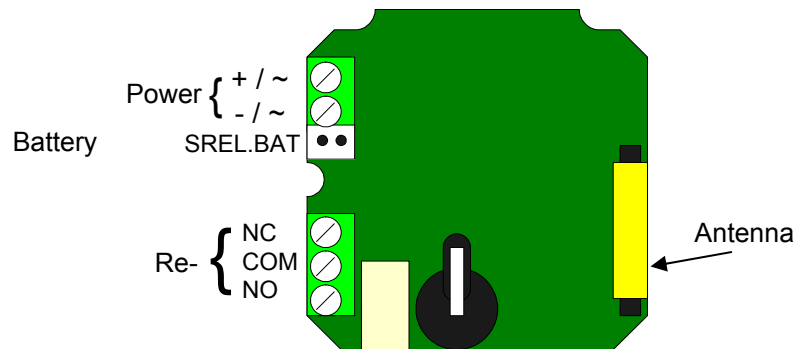
- You can attain the largest reader range if you align the Smart Relay antennas so that they are parallel to that on the transponder during the installation.
- Switch on the supply voltage (if necessary, insert the plug or connect the battery).
- Verify the function of the Smart Relay with a transponder in the condition as received from the factory.
- Program the Smart Relay with the SimonsVoss software (we recommend software version LDB.EXE 1.40 or later).
- Use a transponder that is now authorised in order to test the functioning of the Smart Relay again.

Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 9

6.0 Connection Assignments

6.1 SREL and SREL.ZK

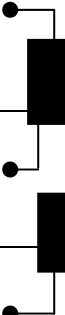


Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 10

6.2 SREL.ADV

6.3 Description of the SREL, SREL.ZK and SREL.ADV Connection

Name	Symbol	Description
Power supply	+ / ~	If connecting a direct current (5 to 24 VDC) source, use the positive pole, otherwise use one of the two alternating current connections (12 VAC)
Power supply	- / ~	If connecting a direct current (5 to 24 VDC) source, use the negative pole, otherwise use the second alternating current connection (12 VAC)
Battery		Plug connection for a battery (when operating without a power supply) Battery ordering code, incl. connector: SREL.BAT
NC relay		Normally closed contact for the change-over relay. When not acted on, this contact is closed to the COM relay
COM relay		Common contact on the change-over relay. This contact is either wired to the NC relay (normally closed contact) or to the NO relay (normally open contact)
NO relay		Normally open contact on the change-over relay. When acted on, this contact is closed to the COM relay
External antenna Brown White Green Grey Yellow	BN WH GN GY YL	Connection for the coloured cables of an extended antenna (ordering code SREL.AV)
RS-485COM RS-485A RS-485B	C A B	Bus connection for external modules
+ Vaux	+V	Typically 3.0 - 5.0V +/- 0.5V for external LED's or buzzer, max. 10mA
LED/ Buzzer/ Input 1/ CLS	F3	Multifunction connection
Serial 1/ input 2	F2	Multifunction connection
Serial 2	F1	Multifunction connection

7.0 Programming and Configuration

When you choose Smart Relay as the locking type in the SimonsVoss software (Version 1.40 and later), you have the following configuration option's:

Schließung Eigenschaften

Name | Generalebenen | Transponder | Daten | **Konfiguration** | Transpondergruppen

☒ Zugangskontrolle ☒ Zeitumschaltung
☒ Zeitonensteuerung ☐ OMRON
☐ Overlay
☐ Flip Flop
☐ Repeater

Erweiterte Eigenschaften

Pulslänge: Sek.

Zeitgesteuerte Relaisumschaltung

☐ Manuelle Verriegelung ☒ Automatische Verriegelung
☒ Manuelle Entriegelung ☐ Automatische Entriegelung

Transponder aktiv:

☐ immer ☒ nur, wenn verriegelt

☐ Begrenzte Reichweite (nur bei interner Antenne)
☐ Unberechtigte Zutritte protokollieren

Advanced Funktionen

Anzahl der Erweiterungmodule:

Schnittstelle

☐ Zusatzsignal CLS

☐ Keine akustischen Programmier-Quittungen

☒ Externe LED ☐ Externer Piepser

Interne/externe Antenne:

☒ Autodetektion ☐ beide aktiv

OK Abbrechen Übernehmen Hilfe

7.1 Access control

Only possible for SREL.ZK and SREL.ADV

The last 1024 transponder activation's are saved with the date and time.

7.2 Time zone control

Only possible for SREL.ZK and SREL.ADV

You can load a time zone plan and the transponders are then approved or blocked, according to their time zone group.

7.3 Overlay

Replacement transponders can overwrite the transponders that they replace. After the first operation with a replacement transponder, the system blocks the original transponder.

7.4 Flip Flop

Pulse mode (default setting) is switched off, and the pulse width does not matter any more. When flip flop mode is switched on, the Smart Relay changes its state from ON to OFF or back again, each time the transponder is activated. We recommend this mode for switching lights or machines, etc.

With an installation of this kind, it may be necessary to make sure that the power supplies and door openers are suitable for continuous current operation.

7.5 Repeater

The Smart Relay receives a transponder signal and then sends it again, amplified. You can use the Smart Relay in this function in order to link a way through larger radio paths. The distance to another Smart Relay can be up to 2.0 m (6.5 ft).

7.6 Time switching

Only for SREL.ZK and SREL.ADV

If time switching is activated, you must load a time zone plan, which allows a general release of the Smart Relay during the marked times (in Group 5). This means that a door can be freely accessible during the day but only opened by transponder at night.

With an installation of this kind, you must make sure that the power supplies and door openers are suitable for continuous current operation.

If you select time switching, the "Time-controlled relay switching" field has the following option's (you may select more than one):

1. Manual locking:
The door is not locked automatically according to the selected time of day, but instead only after an authorised transponder is operated after this time.
2. Automatic locking (default setting):
The door is locked at exactly the time stored in the time zone plan.
3. Manual unlocking (default setting):
The door is not unlocked automatically according to the selected time of day, but instead only after an authorised transponder is operated after this time.
4. Automatic unlocking:
Normally, the door is not opened at the selected time of day, but instead only after operation with the first transponder. If it is required that the door always open automatically at the selected time of time, then select this option.
5. Transponder active:
 - Always:
Normally, a transponder cannot be used during the released periods. If it is necessary, however, to be able to lock the door during this time (for example, if everyone leaves the building), then select this option.
 - Only when locked:
In this operating mode, the transponder has no effect during the released time.

7.7 OMRON

Only for SREL.ADV

Many access control and time recording systems have serial interfaces for connection to card readers. It is also possible to connect a Smart Relay over these interfaces. This means that you can also use the SimonsVoss transponder in systems from other companies.

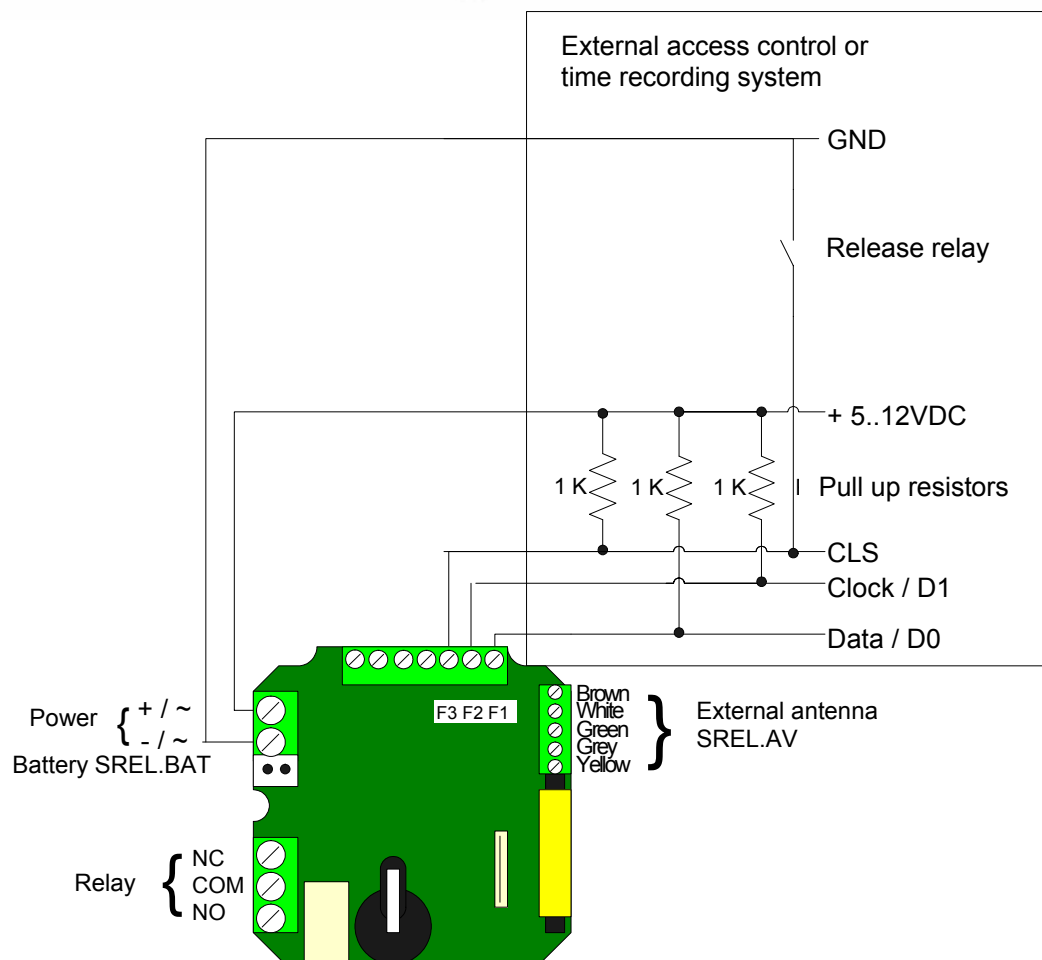
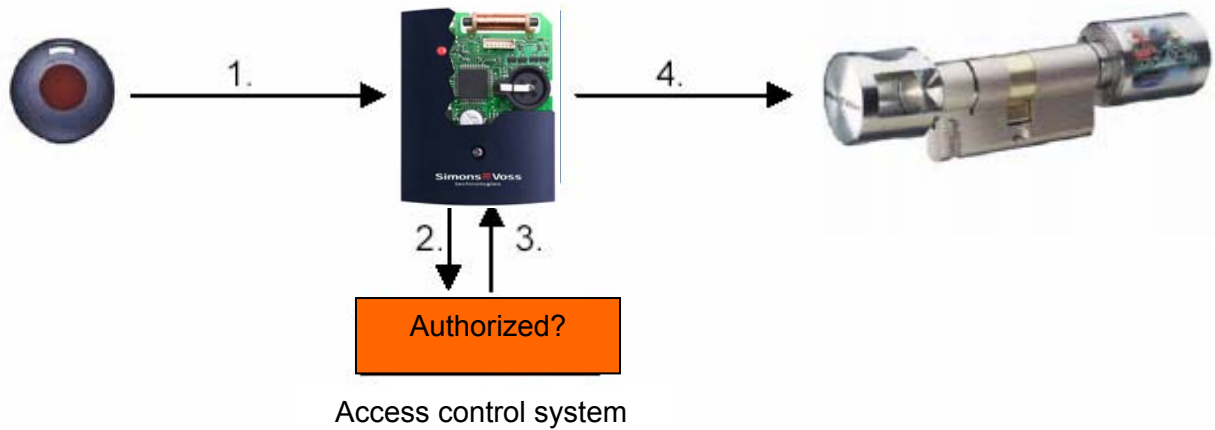
If you would like the Smart Relay to transmit the transponder data to such an external system, and for the Smart Relay to send a remote opening command to a cylinder when released by this external system, then select this option, both on the Smart Relay and on the cylinder.

Select the type of external system under "Interface" (7.13). The following types are available:

Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 14

7.7.1 The Smart Relay in OMRON Mode



7.8 No acoustic programmer acknowledge

Only SREL.ADV

Mark this field if you want no programmer acknowledge to be given via a connected buzzer/beeper when the Smart Relay is programmed.

7.9 External beeper/ External LED

Only SREL.ADV

This is where you specify which external unit is connected. In Flip Flop mode, the Smart Relay generates a continuous signal when switched if there is an external LED connected; if a beeper is connected, it briefly acknowledges each change of state with a sound signal.

7.10 Internal/ external antenna

Only SREL.ADV

- Autodetection:

If an external antenna is connected, only this antenna is used. The Smart Relay then switches the internal antenna off. If no external antenna is connected (default case), the Smart Relay works with the internal antenna.

- Both active:

The Smart Relay can assess entries from transponders at both antennas.

7.11 Number of expansion modules

Only for SREL.ADV

This is where you indicate the number of external modules that are connected to the Smart Relay. These modules are connected to terminals RS-485 **COM**, RS-485 **A** and RS-485 **B**. For more information, refer to the documentation for the separate modules.

7.12 Pulse length

This is where you specify the value, in seconds, for the pulse width of the switching pulse. The value has a range from 0.1 to 25.5 seconds. For example, if you enter 3 seconds here, then a door opener will be released for 3 seconds before it is then blocked again.

7.13 Interface

Only for SREL.ADV

For operation as a serial interface, you can select the type of card reader here that the Smart Relay should simulate. You have the following options:

- Wiegand 32 bit
- Wiegand 26 bit
- Primion
- Siemens
- Kaba Benzing
- Gantner Legic
- Isgus

You will find the corresponding cabling information in the chapter "The Smart Relay as a Serial Interface".

7.14 Restricted range

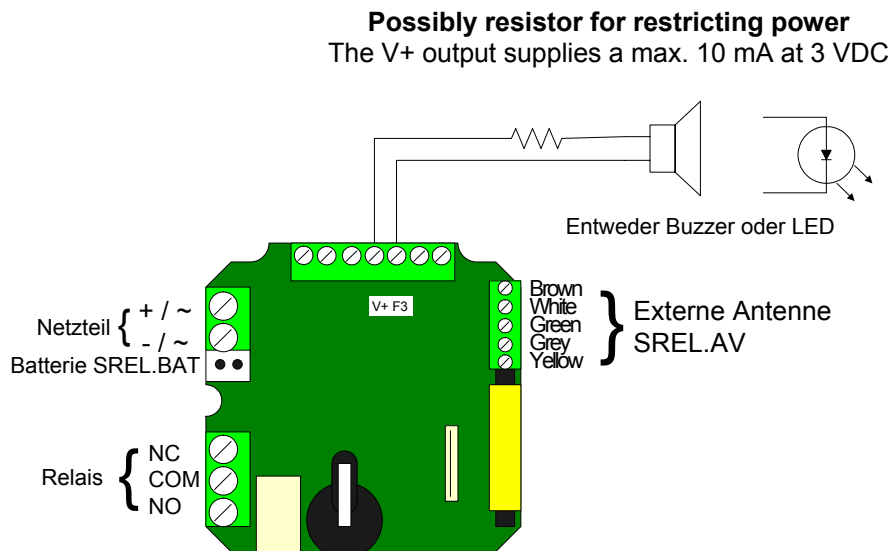
If you select this option, the reader range from the transponder → Smart Relay is restricted from approximately 1.5 m (4.9 ft) down to 0.4 m (1.3 ft). For example, you can use this option if there are several Smart Relays close to one another and individual transponders are authorised for several Smart Relays.

7.15 External Beeper/ External LED

Only for SREL.ADV

Normally, the Smart Relay is configured for connection to an LED. If you want to connect a beeper or buzzer as the external signaller, mark this option. In this way, the beeper/buzzer can be used for an acoustic acknowledgement, instead of the LED.

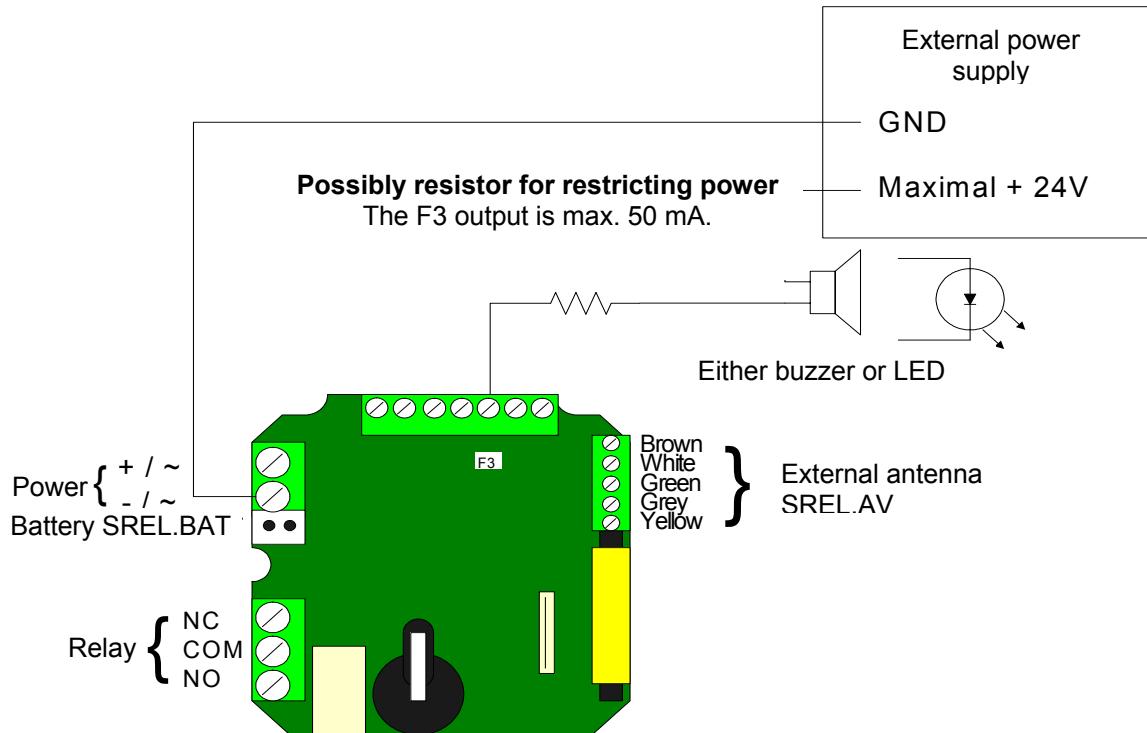
Should the connected component need less than 10 mA maximum current at 3 VDC, the connecting plan can look as follows:



Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 17

If the current for the external component is larger than 10 mA, then this component must be fed by an external power supply. In this case, the connection should be made as follows:



7.16 Log unauthorised accesses

Only for SREL.ZK and SREL.ADV

Normally, only authorised transponder operations are logged. If you also want to record attempts to open the door with an unauthorised transponder, you must select this option.

8.0 Serial Interface

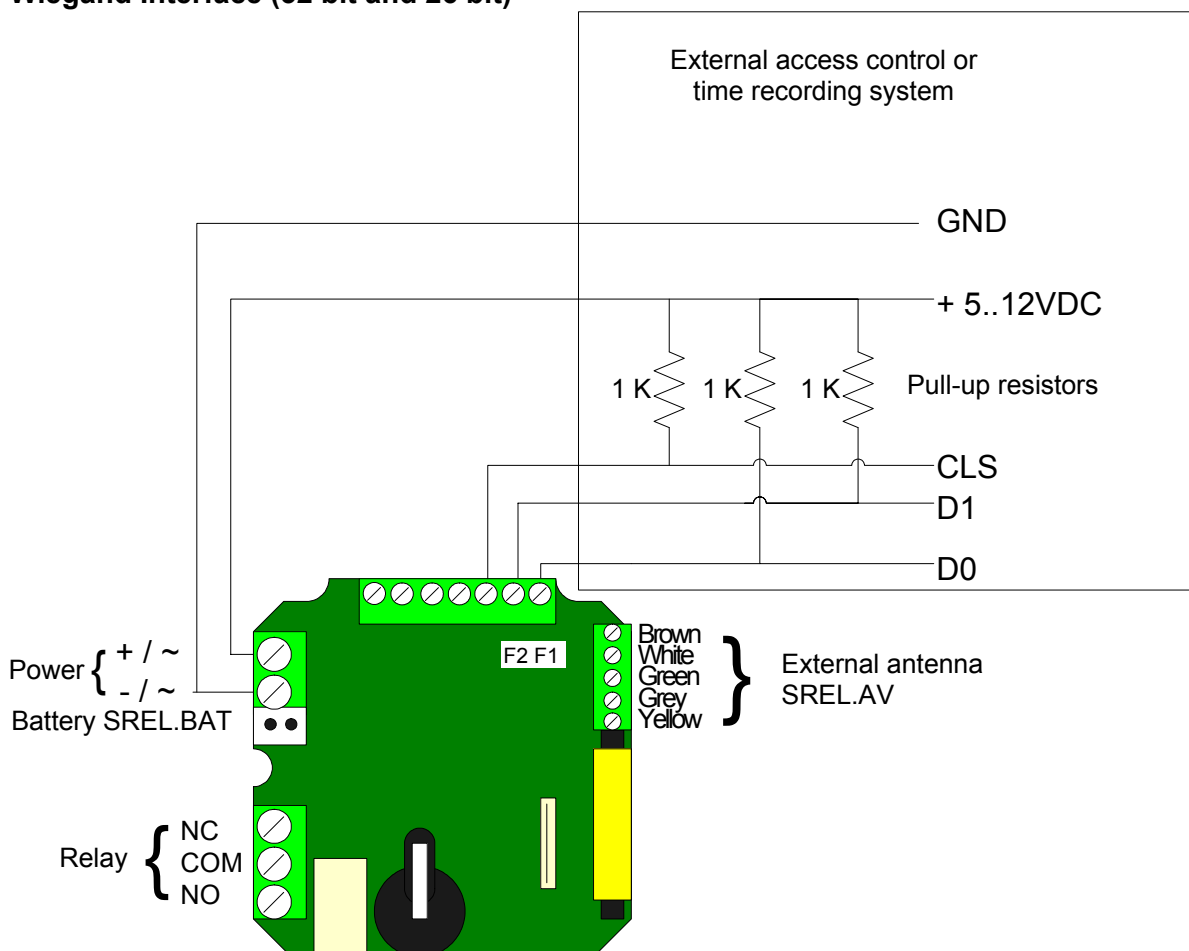
8.1 Functional Description

In order to use a Smart Relay as a card reader in an external access control or time recording system, both the hardware (cable and signal level) and the data formats must correspond exactly to those of the card reader. Only then can the external system understand and evaluate the data from the SimonsVoss transponders.

First the Smart Relay reads the transponder data. If the transponder is authorised in the Smart Relay, this data is forwarded to the external system via the serial interface. SimonsVoss Product Management will provide you with detailed specifications for the individual data formats.

You can select the correct reader type in the Smart Relay configuration using the SimonsVoss software, version 1.40 and later. The following sections describe the connections for the different reader versions.

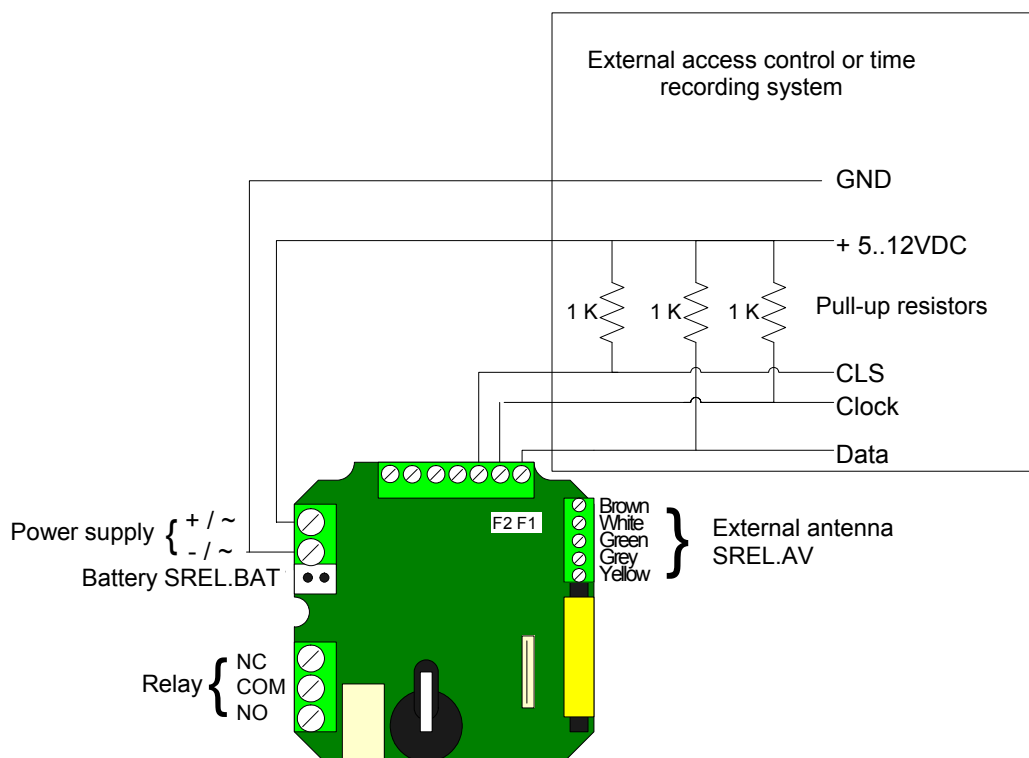
8.2 Wiegand Interface (32 bit and 26 bit)



Smart Relay: SREL, SREL.ZK, SREL.ADV

Page 19

8.3 Kaba Benzing, Siemens, Gantner Legic, Primion, Isgus Interface



9.0 Maintenance

9.1 Battery Warning and Battery Replacement if you are using the SREL.BAT battery

In case the battery capacity is no longer sufficient, a Smart Relay can issue a battery warning as follows:

SREL, SREL.ZK, SREL.ADV

- Internal LED blinks 8 times each time you operate the transponder and before the relay is switched.

If you are operating with a battery, you should make sure that this LED can be seen from the outside.

Only SREL.ADV

- External LED blinks 8 times or external buzzer beeps 8 times, each time you operate the transponder.

Approximately 100 operations are possible after the battery warning, so you should replace the battery as soon as possible.

9.2 Backup Battery

A discharged backup battery can cause the internal clock in the type SREL.ZK or SREL.ADV Smart Relay to stop. For this reason, we recommend that you check the time of day at routine intervals. A backup battery will last approximately 10 years if there is no power supply interruption. If the Smart Relay needs the backup battery often because of frequent power failures, you should replace this battery routinely.

If you operate the Smart Relay with a battery (SREL.BAT), you are not permitted to use the backup battery.

10.0 Data sheet

Housing made of black plastic: Dimensions [LxWxH]	72 x 57 x 25.5 mm (approximately 2.8 x 2.2 x 1.0 inches)
Degree of protection	IP 20, not tested for outside use
Temperature	Operation at: -22°C to +55°C (-31°F to +131°F) Storage at: 0°C to +40°C (32°F to +104°F)
Air humidity	<95% without moisture condensation
Printed circuit board dimensions [LxWxH]	50 x 50 x 14 mm (approximately 2.0 x 2.0 x 0.6 inches)
Line voltage	12 VAC or 5-24 VDC (no reverse voltage protection)
Power limit	Power supply must be limited to 15 VA
Quiescent current	< 5 mA
Max. current	< 100 mA
Programmable pulse width	0.1 to 25.5 seconds
Output relay type	Change-over
Output relay continuous current	Max. 1.0 A
Output relay switch on current	Max. 2.0 A
Output relay switching voltage	Max. 24 V
Output relay switching capacity	10 ⁶ operations at 30 VA
Multifunction connections: F1, F2, F3	Max. 24 VDC, max. 50mA
Vibrations	15G for 11 ms, 6 shocks according to IEC 68-2-27 Not released for continuous used under vibrations

Smart Output Module

State of: June 2006

Smart Output Module

Content

1.0	Important Information	4
2.0	Product Description	4
3.0	Before Ordering	5
3.1	Smart Relay	5
3.2	Determine the Number of Modules that are Needed	5
3.3	Obtain and Dimension the Power Supply	5
3.4	Determine the Installation Technique and the Installation Site	5
3.5	Cable Types and Paths	5
3.6	Outside Installation	5
3.7	Guidelines	5
4.0	Before Installation	6
5.0	Installation	6
6.0	Connections	7
6.1	Terminal Assignments	7
6.2	Connection Assignments	8
7.0	Connection to the Smart Relay	9
7.1	Standard Power Supply Connection	10
7.2	Emergency Release Connection for a Fire Alarm System	10
7.3	Protective Circuit to Prevent an Opening when the Supply Voltage Fails	11
7.4	Protective Circuit for the Signaling Option Outputs	12
8.0	Programming and Configuration	13
8.1	General Information	13
8.2	Enter the Number of Modules	13
8.3	Select the Module Addresses	13
8.4	Adjust the Pulse Length	14
8.5	Select Signaling	14
8.6	Automatic Name Assignment in the Software	14
8.7	Inverting the Outputs	14

Smart Output Module

Content

9.0	Meaning of the LEDs	15
9.1	LEDs for Each Output	15
9.2	State LED	15
10.0	Technical Specifications	16

1.0 Important Information

- Installation of a SimonsVoss Smart Output Module requires knowledge in the areas of approvals for electronic and electrical installation and in the use of SimonsVoss software and the SimonsVoss System 3060. For this reason, only trained and expert personnel should install the unit.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect installation.

- Incorrectly installed Smart Output Modules may block an entrance or opening. SimonsVoss AG is not liable for the consequences of incorrect installation, such as blocked access to injured or endangered persons, property damage or other damages.
- Should products from other manufacturers be driven with a Smart Output Module, the guarantee and installation conditions given by the respective manufacturer of these devices must be observed.
- Should the maximum permissible currents (see Technical Data) be exceeded at the outputs or should the maximum voltages be exceeded at the inputs of the Smart Output Module, the result can be damage to the module.

2.0 Product Description

The Smart Output Module is a product that provides eight floating relay outputs, which can be driven via a single Smart Relay, type SREL.ADV. Depending on the transponder ID, one or more outputs can be switched for some programmable time. This assignment (profile) can be selected as needed. This means that the Smart Output Module is suitable, for example, for implementing an authorisation-dependent elevator controller or a driver for opening lockers. Should more than eight outputs be required, up to 16 modules can be connected to one type SREL.ADV Smart Relay.

3.0 Before Ordering

3.1 Smart Relay

At least one type SREL.ADV Smart Relay is necessary for operating a Smart Output Module. Please read the Smart Relay Product Manual for information on ordering.

3.2 Determine the Number of Modules that are Needed

Up to 16 external modules can be connected to one type SREL.ADV Smart Relay. If you select the "Signalling" option in the configuration, the number of outputs per Smart Output Module is reduced from eight to four. Each module has a separate configuration in the software.

3.3 Obtain and Dimension the Power Supply

The type SREL.ADV Smart Relay and up to eight type SOM8 external modules can be operated with one power supply (SREL.NT). For the data regarding the power supplies, take the technical specifications (currents, voltages and powers) of the Smart Relay and the modules into consideration.

3.4 Determine the Installation Technique and the Installation Site

The modules are attached to DIN rails. The length of these DIN rails depends on the number of modules that have to be attached next to one another. The Smart Relay Advanced units are typically not mounted on DIN rails, but instead are installed at the place where the transponders should be read.

3.5 Cable Types and Paths

There should be enough room around a Smart Output Module to allow all cables to be laid without kinking them too much. We recommend cable type IY(ST)Y (Twisted-Pair, shielded cable), strand diameter 0.6 mm.

3.6 Outside Installation

A suitable IP 65 (SOM.IP65G) housing must be provided for outside installation.

3.7 Guidelines

The installation should be performed according to VDE guidelines, by experts who have been

4.0 Before Installation

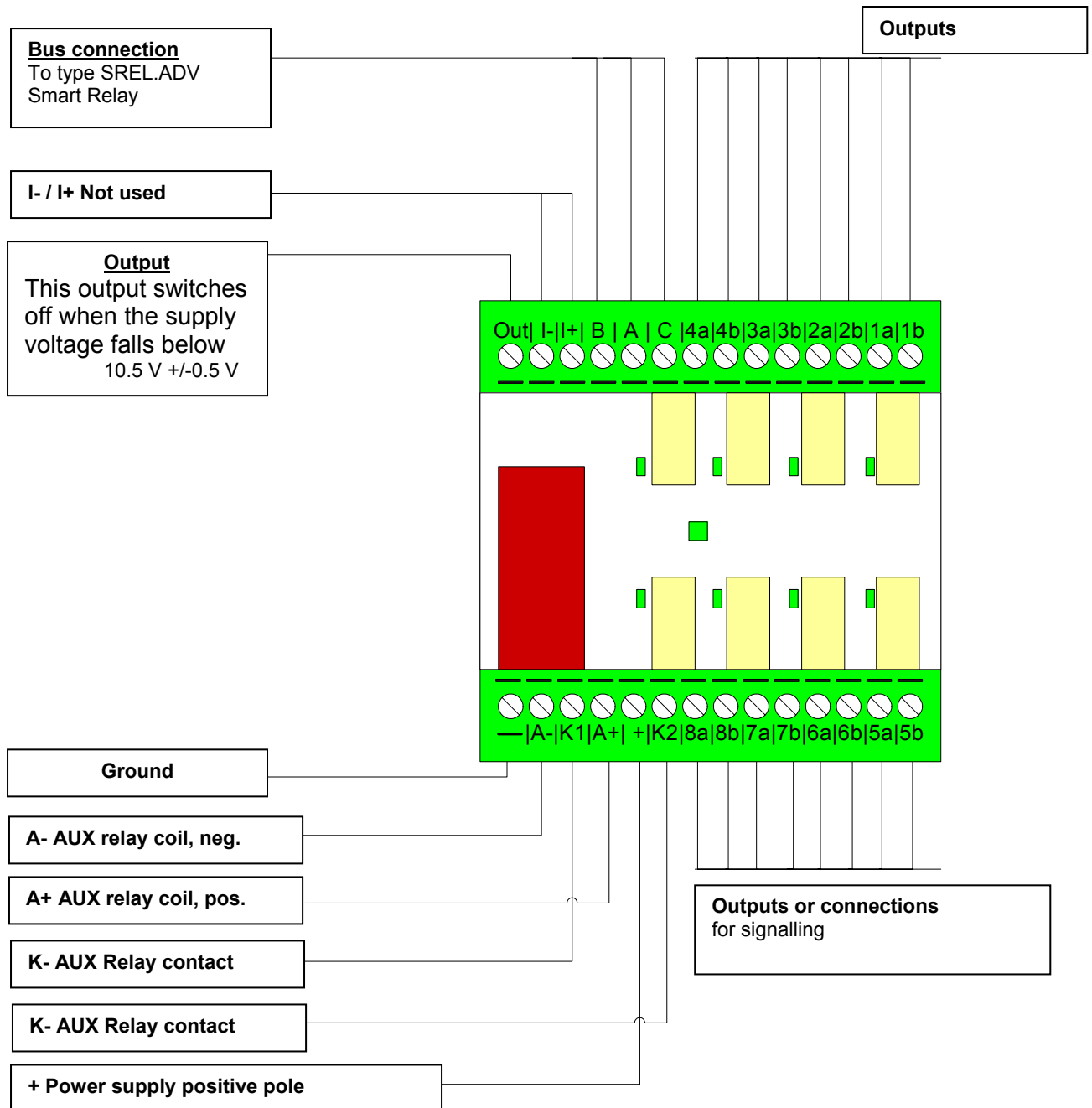
- Unpack the Smart Output Module and inspect it for external damages.
- Connect the Smart Output Module to a type SREL.ADV Smart Relay (see Connection to the Smart Relay) and provide both units with voltage over the power supply.
- Note the polarity.
- Activate the Smart Relay with a transponder in the condition as received from the factory. This activates all Smart Output Module outputs, which is shown by all LED's on the Smart Output Module lighting (green).

5.0 Installation

- Cut the DIN rails to size and tighten the screws.
- Switch off the supply voltage.
- Mount the units on the DIN rail (latch).
- Connect all cables (see Terminal Assignments and Connection Examples).
- Be sure to pay attention to the polarity when connecting the supply voltage.
- Switch on the supply voltage.
- Program the Smart Relay and the Smart Output Module with the SimonsVoss software (see Programming and Configuration).
- Then test the function with authorised transponders.

6.0 Connections

6.1 Terminal Assignments



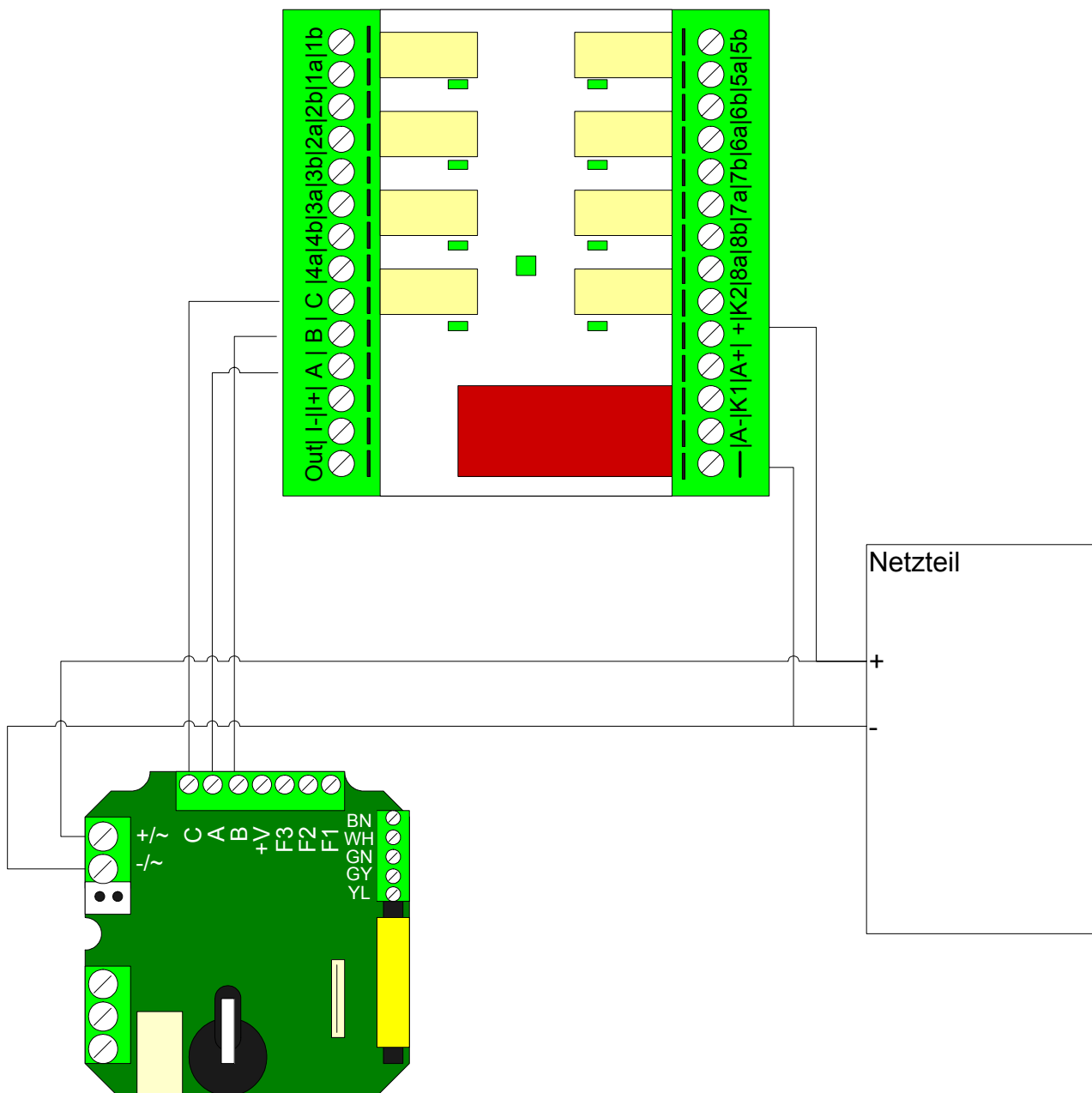
Smart Output Module

Page 8

6.2 Connection Assignments

Name	Symbol	Description
Output	Out	If the supply voltage falls below 10.0 VDC +/- 0.5V, this output switches off. Typically, this output is connected to A-, if it is necessary to switch the AUX relay before the switching functions fail. This is an open collector output.
Isolated digital input	I- I+	Not used at this time
Bus connection to the type SREL.ADV Smart Relay	A B C	These terminals are connected to the terminals with the same names on the type SREL.ADV Smart Relay.
Outputs	1a 1b 2a 2b 3a 3b 4a 4b	Floating outputs (make contacts) that are switched depending on the transponder authorisation.
Outputs or connections for signalling	5a 5b 6a 6b 7a 7b 8a 8b	Depending on the configuration Either: floating outputs (make contacts), that are switched depending on the transponder authorisation. Or: floating connections that generate an alternating signal when the assigned output is activated. Assignment: 1 → 5 2 → 6 3 → 7 4 → 8
Name	Symbol	Description
Ground		Connection for the power supply ground
Plus	+	Connection for +12 VDC
AUX relay coil	A- A+	To switch the AUX relay, this coil must be supplied with 12 VDC.
AUX relay contacts	K1 K2	Floating outputs (make contacts) of the AUX relay.

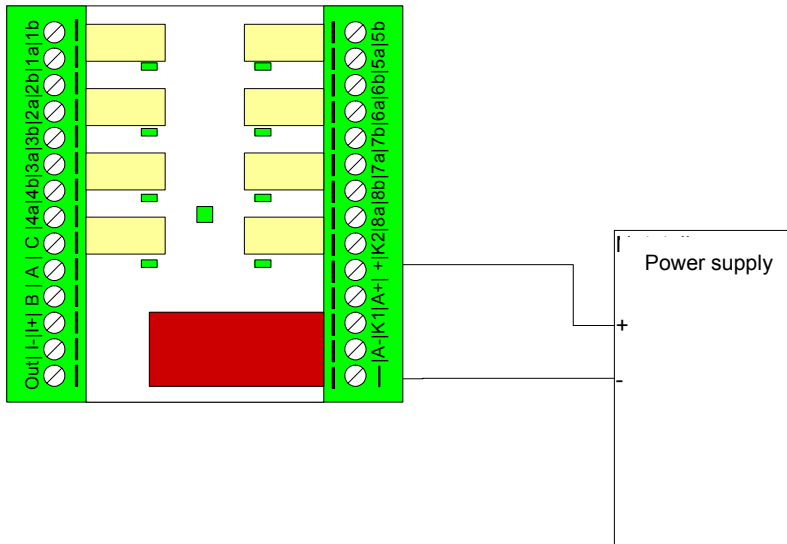
7.0 Connection to the Smart Relay



Smart Output Module

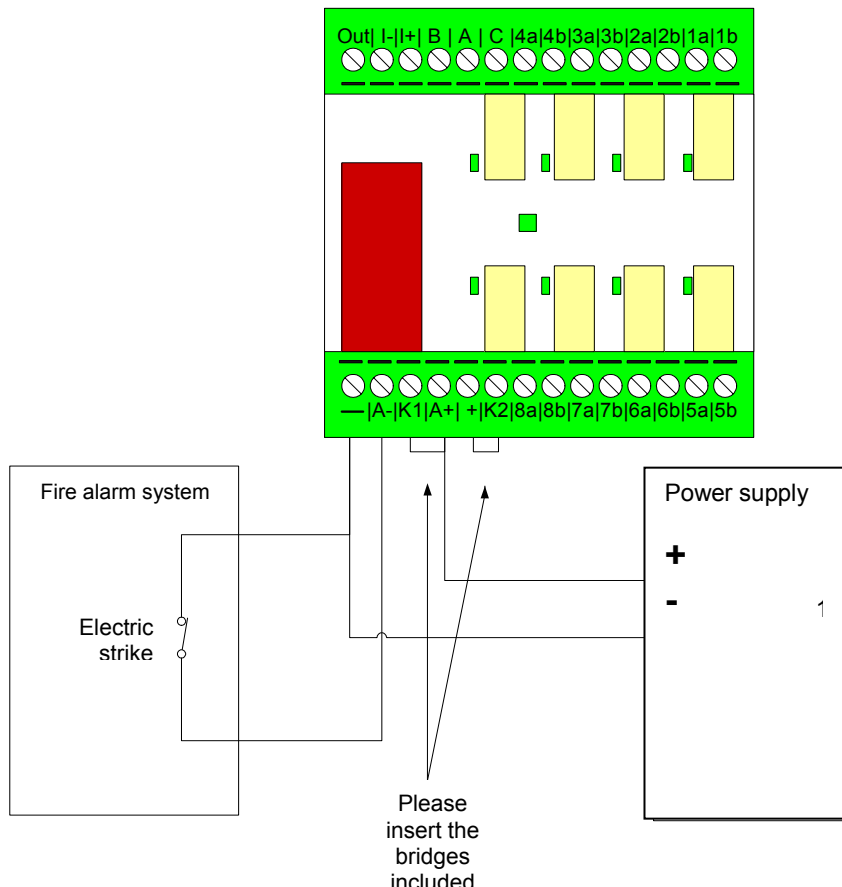
Page 10

7.1 Standard Power Supply Connection



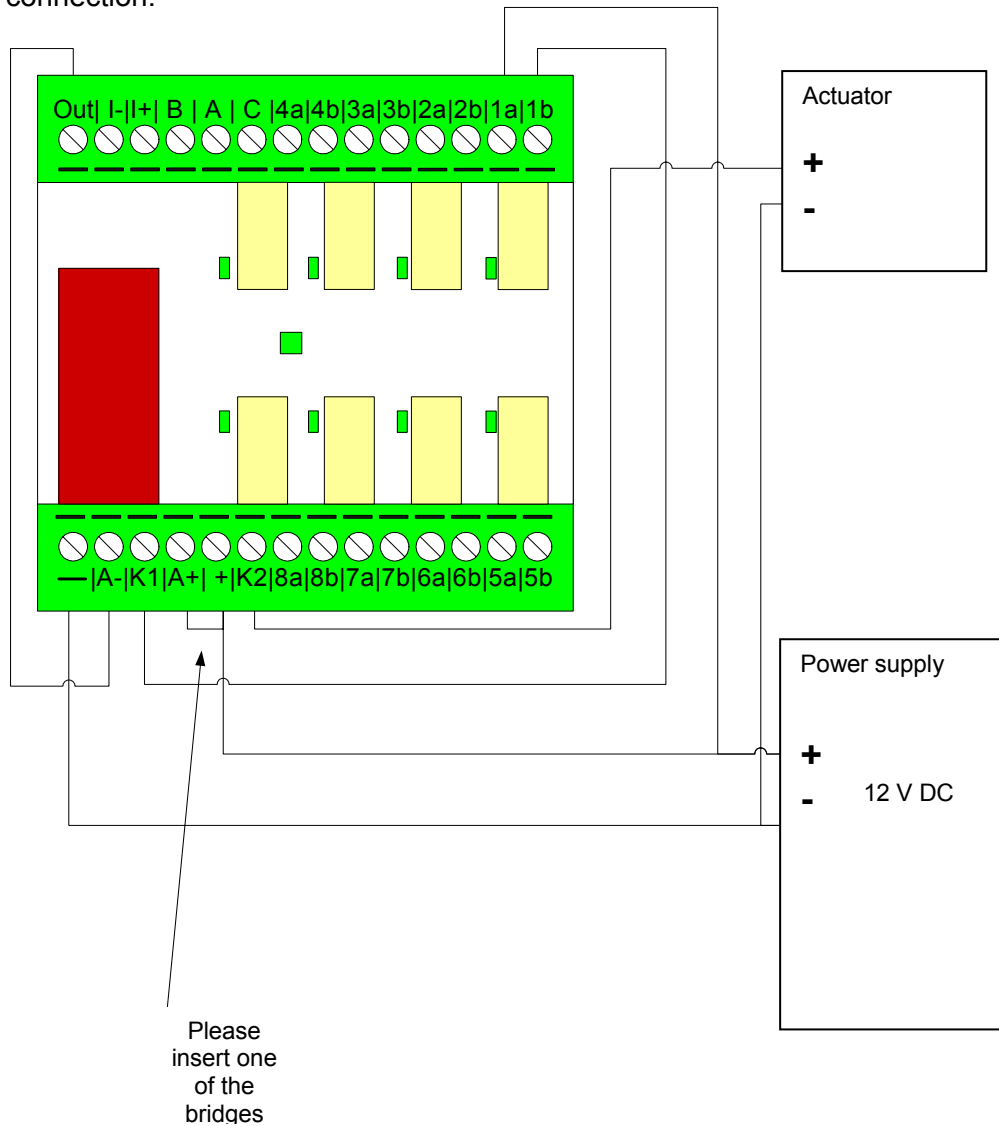
7.2 Emergency Release Connection for a Fire Alarm System

When the fire alarm system relay opens, the Smart Output Module supply voltage is stopped, consequently closing outputs 1 to 8.



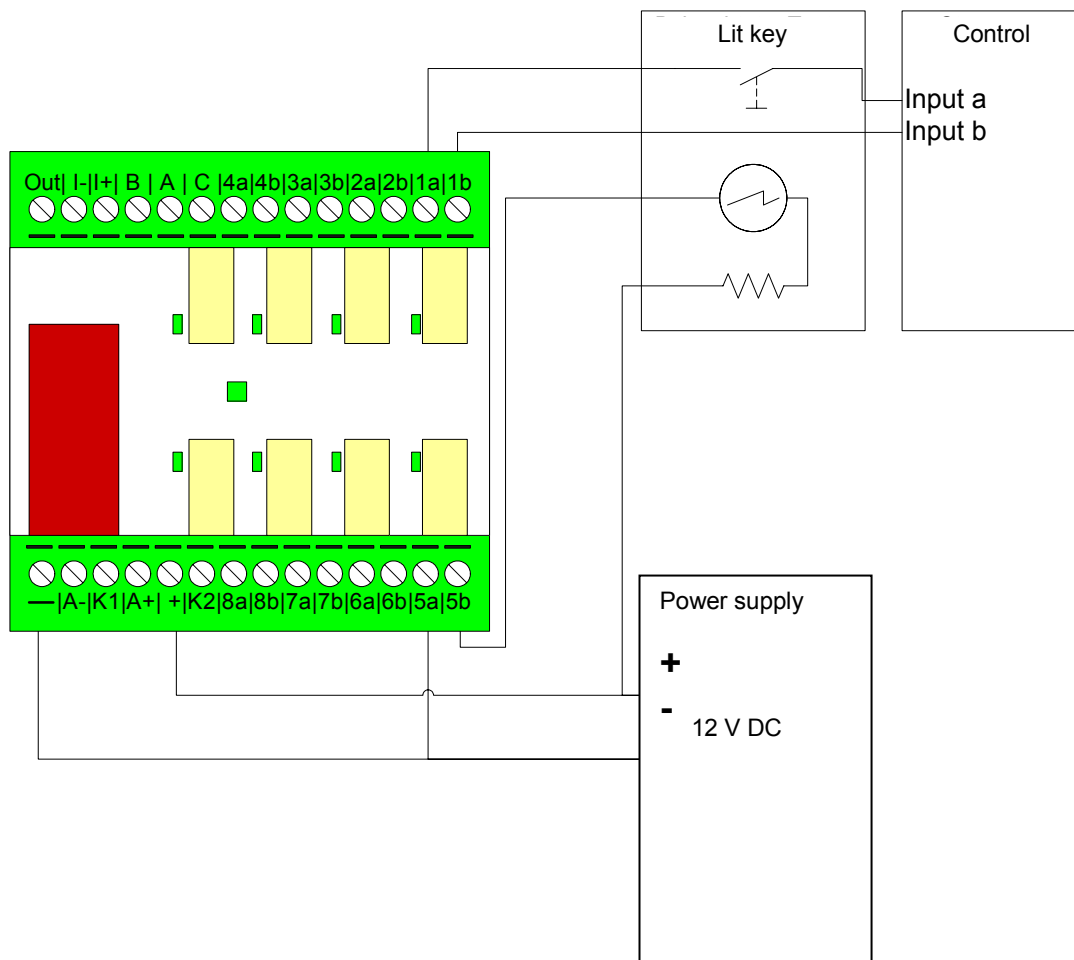
7.3 Protective Circuit to Prevent an Opening when the Supply Voltage Fails

When the supply voltage range falls below the acceptable level, the actuator supply over the AUX relay is interrupted. The switching output (OUT) is used in this connection.



7.4 Protective Circuit for the Signaling Option Outputs

Each pair of terminals opposite one another (1 and 5, 2 and 6, 3 and 7, 4 and 8) works together. When the lower output in the module is switched, the corresponding assigned output blinks.



8.0 Programming and Configuration

8.1 General Information

To program the Smart Output Module, connect it to a type SREL.ADV Smart Relay. Supply power to both the Smart Relay and the Smart Output Module and hold the programming device close to the Smart Relay. The Smart Output Module itself cannot communicate with the Config Device.

8.2 Enter the Number of Modules

Enter the number of connected Smart Output Modules in the Smart Relay configuration. The largest possible value here is 16 modules. This automatically creates lockings in the locking plan for each of a module's outputs.

8.3 Select the Module Addresses

The Smart Relay communicates with each connected module over its address. This address is set up in the Smart Output module using the address switches. The following addresses are permitted:

Modul	Adresse
Module 1	0 (default factory setting)
Module 2	1
Module 3	2
Module 4	3
Module 5	4
Module 6	5
Module 7	6
Module 8	7
Module 9	8
Module 10	9
Module 11	A
Module 12	B
Module 13	C
Module 14	D
Module 15	E
Module 16	F

8.4 Adjust the Pulse Length

The modules appear in the locking plan as the locking type "expansion module". You can select a pulse length from 0.1 to 25.5 seconds in the configuration for each module. This length then applies to all of the module's outputs.

8.5 Select Signaling

Signaling is a special function where two of a module's outputs always work together. The first output reacts completely normally, depending on transponder operation; the output assigned to it simultaneously generates an alternating signal. You can select this option, for example, if you want to have the keys that are released when an elevator is controlled blink.

Attention: If you select this option, the number of outputs that are switched when authorized is reduced from eight to four.

Output assignments for signaling:

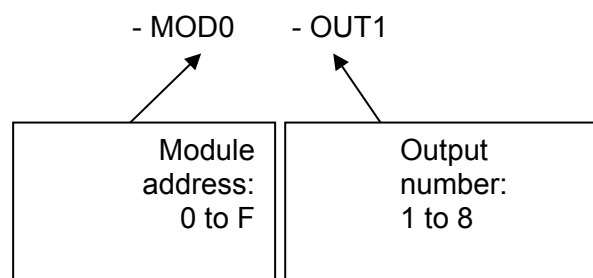
- 1 → 5
- 2 → 6
- 3 → 7
- 4 → 8

8.6 Automatic Name Assignment in the Software

The SimonsVoss software automatically assigns designation to modules when the modules are created. The following convention is used:

SMART RELAY NAME

(z.B. Aufzug1-MOD0-OUT4)



8.7 Inverting the Outputs

This option allows the output switching behavior to be inverted. If there is no supply voltage, all output relays are always closed.

9.0 Meaning of the LEDs

9.1 LEDs for Each Output

Each of the 8 outputs has an LED assigned to it. This LED displays the state of the output.

Green -> output closed

Off -> output open

9.2 State LED

In addition, there is a three-color LED that displays the state of the Smart Output Module:

- **Lights green every 5 seconds** → Communication with the Smart Relay is OK
- **Lights red every 5 seconds** → Communication with the Smart Relay is disrupted. (For example, the bus line has been seized for communication with other modules.
- **Blinks green/red** → Communication currently taking place with the Smart Relay.
- **Blinks red** → The supply voltage is too low.

10.0 Technical Specifications

Housing made of plastic with transparent cover for mounting on DIN rail.	Dimensions: L x W x H 75 x 75 x 53 mm (approx. 3.0 x 3.0 x 2.1 inches)
Weight	Approx. 170 g (approx. 6 ounces) (without packaging)
Degree of protection	IP 20 (not tested for outside use)
Ambient temperature	Operation: 0 – 60°C (32 – 140° F) Storage: 0 – 70°C (32 – 158° F)
Air humidity	<90% without moisture condensation
Supply voltage	11.0 to 15.0 VDC Recommended: 12 VDC regulated
Power limit	The power supply must be limited to a maximum of 15 VA
Quiescent current	<120 mA
Max. current	<150 mA
Programmable pulse width	0.1 to 25.5 seconds
Output relay type	Normally closed
Output relay and AUX relay continuous current	Max 1 A
Output relay and AUX relay switch-on current	Max 2 A
Output relay and AUX relay switching voltage	Max. 24 V
Output relay and AUX relay switching capacity	10 ⁶ operations at 24 VA
Vibrations	15 G for 11 ms, 6 shocks to IEC 68-2-27, not tested for continuous use under vibrations
Output 1 switching current	Max .1 A
Output 1 switching voltage	Max. 24 V
Output 1 switching capacity	Max. 1 VA
Output 1 switching behavior when voltage is too low	V < 10.5 +/- 0.5 V corresponds to off

Transponder 3064

State of: September 2006

Transponder 3064

Content



1.0	Method of Operation	3
1.1	General	3
1.2	Higher Priority Locking Level	4
2.0	Special Models	5
2.1	Password Transponder	5
2.2	Switching Transponder	5
2.3	Explosion Protection Transponder	5
3.0	Explosion Protection Transponder	6
3.1	General Information	6
3.2	Standards	6
3.3	Grouping	6
4.0	Additional Functions	7
4.1	Time Zone Control	7
4.2	Validity Date	7
4.3	Activation Transponder	7
5.0	Battery Replacement	8
5.1	Battery Replacement 3064	8
5.2	Battery Replacement for the Explosion Protection Transponder	8
6.0	Loss of the Transponder	8
6.1	Emergency Opening	8
6.2	Replacement Transponder	8
7.0	Data Sheet	9

1.0 Method of Operation

1.1 General

The Transponder 3064 is a digital “key” that is programmed with the locking plan software and that works over radio transmission with no physical contact. All functions, for example, opening and closing doors, gates, barriers, furniture locks, etc., are carried out by pressing a button. Communication with the digital components (cylinder, Smart Relay and activation unit) takes place by sending and receiving constantly changing crypto codes, which makes misuse practically impossible.

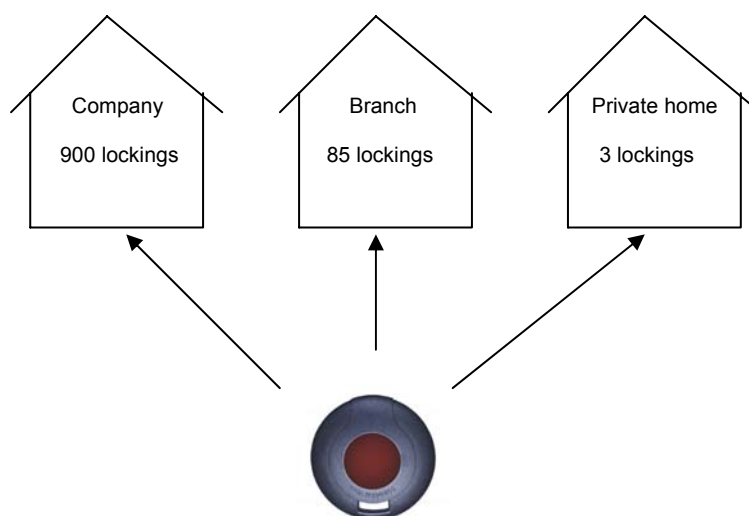
Since the System 3060 works with active transponder technology, the transponder has its own voltage source (battery) available. The advantage in comparison to passive technologies lies in the smaller energy requirements of the cylinder and the larger range.

In order to trigger an action, hold the transponder near the digital locking (refer to the separate chapters for information on maximum transponder ranges) and then press the transponder button. Provided that the transponder is authorised for this digital locking, the desired action, for example, opening or locking the door, can be carried out.

The housing of the transponder is protected against splash water. However it is not waterproof!

Each transponder can be used in three different, mutually independent locking systems (assuming that no validity areas were programmed). Each locking system has its own password and is administered separately.

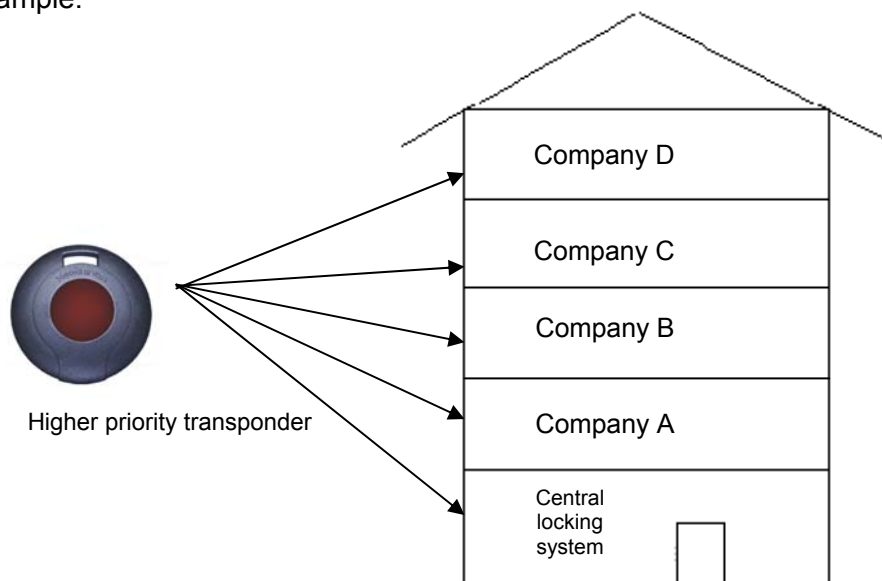
Example:



1.2 Higher Priority Locking Level

If it is necessary to have transponders that are authorised for more than 3 mutually independent locking systems, “higher priority locking levels” must be set up in these locking systems. There are a maximum of 3 higher priority locking levels available for this. All transponders of a higher priority locking level have the same authorisation. One digital locking distinguishes between a maximum of three higher priority levels.

Example:



Four companies are accommodated in an office building with a central locking that is used by all the companies. Each company administers its own locking system with its own password. Every employee receives a transponder that is authorised for 2 locking systems, namely the central locking and his or her own company.

However, the fire brigade, for example, needs a transponder that is authorised for all five of the building's locking systems. To accomplish this, a higher priority locking level with the same separate password must be set up in all five locking systems and the authorisations must be set up for the higher priority transponders. The transponders set up in this level all have the same authorisation. If higher priority transponders with other authorisations are required, an additional higher priority locking level must be set up (max. 3 higher priority locking levels per locking!). The higher priority transponder must then be programmed into all [shutdowns](#) of all 5 locking systems.

2.0 Special Models

2.1 Password Transponder

Instead of manually entering the locking system password, you can transmit it over radio frequency with the help of a special transponder. Standard transponders cannot be used as password transponders.

2.2 Switching Transponder

With this transponder, a two-wire cable (approx. 1m or 37 inches) is connected to the switch contacts of the button and guided outside the device. When both wires are connected, the transponder switches through.

Application examples:

- Connecting external systems
- Remote triggering of a Digital Locking Cylinder or Smart Relay
- Block Lock Function 3066: System activation from more than one location

2.3 Explosion Protection Transponder

This is a transponder with the same functions as the Transponder 3064. In addition, this transponder is released for use in explosion protection zone 1.
(Note Chapter 3 in this regard).

2.4 SmartClip

The special design of this transponder means that the SmartClip is suitable for holding an ISO 7816 format card.

2.5 Transponder, bonded

The standard transponder as described above, but with a glued-shut casing. This prevents end-users from opening the case and using the transponder electronics improperly.

2.6 Transponder, numbered

Sequentially numbered transponders can also be ordered if required.

Explosion Protection Transponder

2.7 General Information

This special product is a transponder that is permitted to be carried into and used in areas subject to explosion hazards, called Zone 1. An area is denoted as Zone 1 when atmospheres capable of exploding occur occasionally. It is crucial that you keep in mind the following issues:

- You are not permitted to open the housing.
- Unlike with the Transponder 3064, only SimonsVoss Technologies AG is permitted to change the battery.
- Normally, you must comply with the general operating instructions of the BGR132 (German rules for occupational safety and health) when using the device in Zone 1.

3.2 Standards

The transponder has been tested according to the applicable explosion protection standards. Refer to:

- Directive 94/9/EC
- DIN EN 50014 (Electrical apparatus for potentially explosive atmospheres)
- DIN EN 50020 (Intrinsic safety "i")

3.3 Grouping

The transponder is grouped in the following way:

- Explosion protection: zone 1
- Intrinsic safety: ib
- Explosion group: IIC
- Temperature class: T3
- Device group: II2 G

This applies to areas in which a potentially explosive atmosphere can arise due to gases, vapours or mists. The information quoted relates to an ambient temperature of from -20°C to +40° C (-4° F to +104° F) in the place of use.

3.0 Additional Functions

The following functions can be activated in the locking plan software:

3.1 Time Zone Control

For TZC version digital lockings, you can program transponders that have locking authorisation for specific times only. These time zones are deposited in the locking plan software, and the transponders are then assigned to an appropriate time zone group.

Example: Mr. Miller receives the following authorisation:

Monday to Friday	from 9:00 am, until 6:30 p.m.
Saturday	from 9:00 am, until 12:45 p.m.
Sunday	no authorisation

3.2 Validity Date

It is possible to program transponders whose authorisation is tied to a validity date (this also applies to non-TZC-versions):

- Transponders that are valid **from a specific point in time**
(e.g., from 8:00 a.m. on July 12, 2003)
 - Transponders that are valid **up to a specific point in time**
(e.g., until 5:00 p.m. on July 12, 2003)
 - Transponders that are valid **for a specific time interval**
(e.g., from July 1, 2003 until July 31, 2003)
- 👉 One data record is assigned for each activation or expiry date!

3.3 Activation Transponder

Within the scope of the block lock function, all authorised transponders for a digital locking in the security area are blocked when the alarm system has been activated in order to avoid false alarms. For emergency situations, transponders can be programmed (for example, for the fire brigade) that release this block. Afterwards, the door can be opened with an authorised transponder.

4.0 Battery Replacement

4.1 Battery Replacement 3064

If a battery warning occurs, then the transponder battery can be changed at any time (see the Manual on the 3061 Locking Cylinder – Battery warning). Open the casing carefully so that you can see the battery. Open the battery clip and remove the battery, insert a new one, and close the clip. Press the casing back together again.

When you change the battery it is important to ensure that the procedure does not take more than two minutes, that the transponder button is not pressed during that period, and that you do not short the battery – otherwise you may lose data.

Alternatively:

Send the transponder that needs its battery changing to:
SimonsVoss Technologies AG, Eichenweg 6, 07616 Petersberg.

4.2 Battery Replacement for the Explosion Protection Transponder

Attention:

Only SimonsVoss Technologies AG is permitted to change the transponder battery!

5.0 Loss of the Transponder

5.1 Emergency Opening

An emergency opening can be carried out using the SmartCD + PDA (only use devices approved by SimonsVoss) and with the input of the locking system password.

5.2 Replacement Transponder

If a transponder is lost, it can be deleted from the locking plan and a replacement transponder can be set up. When operating the locking system in overlay mode, the lost transponder is automatically blocked as soon as the replacement transponder is activated at the digital locking. (See the Software Operating Instructions Page H3 for programming and procedure information.)

6.0 Data Sheet

Housing	<ul style="list-style-type: none">• Made of weather-resistant plastic• Colour: Black• Degree of protection: IP 65• Diameter: 42 mm• Integrated lithium battery• Max. 1,000,000 operations, or 10 years standby• Access authorisations for up to 48.149 doors• Can be used in 3 mutually independent locking systems
---------	--

Q3007 Biometric Transponder

State of: September 2006

Q3007 Biometric Transponder

Content

1.0	General Instructions	3
1.1	Safety instructions	3
1.2	Product description	3
2.0	Overview of function	4
2.1	Basic information on operation	4
2.2	Operating states	4
2.3	How the transponder works	5
2.4	"Learn" mode: start-up, scanning in fingerprints	5
2.5	Querying the number of fingerprints scanned in	8
2.6	"Recognise" mode: one-off triggering of transponder	9
3.0	"Delete" mode: deleting fingerprints	10
4.0	Transparent mode	10
5.0	Programming the Transponder	11
	with the SimonsVoss software	11
6.0	Changing the Batteries	11
7.0	Technical Data	12
8.0	Table of Diode Signals	13

1.0 General Instructions

Please take 15 minutes to familiarise yourself with how your Biometric Transponder Q3007 works with the help of these operating instructions.

1.1 Safety instructions

Caution! – The batteries used in this product could burn or cause a fire if they are not handled properly. Do not charge, open or burn these batteries or heat to over 100°C. Make sure that the sensor surface is not dirty or scratched. Do not drop the Q3007 or expose it to any other strong impacts.

In addition, please make sure that the initial scanning in of fingerprints is not carried out by unauthorised persons!

We advise you to protect the Q3007 against unauthorised access if possible.

Handling a Q3007 assumes knowledge of how to use SimonsVoss software. Programming should therefore only be carried out by trained specialist staff.

SimonsVoss Technologies AG is not liable for any damage caused by incorrect programming.

An incorrectly programmed or faulty Q3007 can block access via a door. SimonsVoss AG is not liable for the consequences of such an occurrence, such as blocked access to persons who are injured or in danger, material damage or any other damage.

1.2 Product description

The Q3007 differs from normal transponders by the fact that it is also equipped with a highly sensitive Atmel Fingerprint Sensor. In just a few seconds, a high-powered processor in the transponder compares the saved fingerprint with the fingerprint read in by the sensor. In this way, only people whose fingerprints have been scanned in already can use the transponder. This guarantees maximum security against unauthorised use by third parties, e.g. if the transponder is unsupervised, or is lost or stolen. The Q3007 is therefore particularly suitable for applications where a transponder is provided with very many or very specific authorisations, e.g. if one person has a general transponder for all doors or access to high-security areas.



2.0 Overview of function

2.1 Basic information on operation

The Biometric Transponder Q3007 scans fingerprints using a fingerprint sensor. The finger is dragged across the sensor, rather than being pressed against it.

The following should be noted:

The fingerprint to be scanned/ memorised should always be dragged over the sensor in the same way.

To do this, place the tip of the finger that is to be stored or to be recognised at the upper edge of the Biometric Transponder and draw it across the sensor from top to bottom (towards the button) at a constant speed whilst applying slight pressure. The design of the housing means that the finger is guided properly through the slightly raised side walls. This more or less excludes the possibility of using the transponder incorrectly.

The fingerprint sensor can thus pick up the fingerprint line by line and reassemble it into a complete image in the integrated processor. If the reassembled image matches the saved image, the Transponder is released.

2.2 Operating states

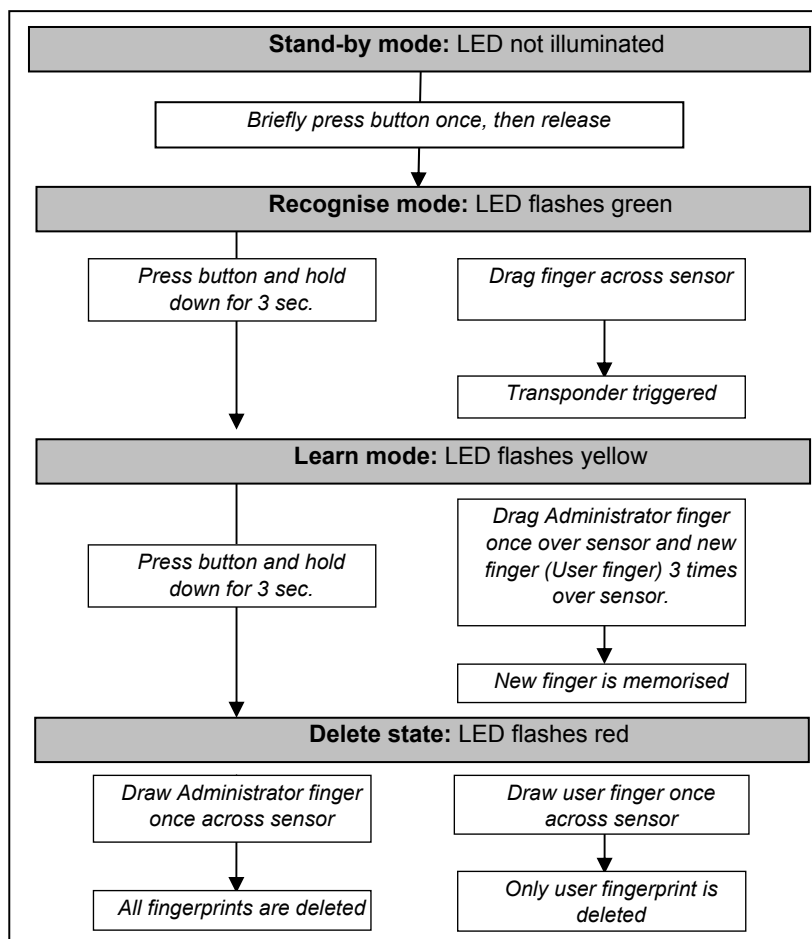
The Q3007 has four different operating modes:

Mode	Function
<i>Standby</i>	The Q3007 is normally on "Standby" in order to save the battery capacity. After it has completed a function (e.g. scanning), it always returns to the standby mode.
<i>Learn</i>	In the "Learn" mode, new fingerprints can be memorised. Up to 6 different fingerprints can be saved, two of which are what we call "administrator" fingerprints. New fingerprints (user fingerprints) can only be scanned in with the help of an administrator. The only exception is the scanning of the first two fingerprints (Administrator fingerprints), see below
<i>Delete</i>	In the "Delete" mode, fingerprints that have been memorised can be deleted. Individual prints can be deleted, or all fingerprints can be deleted at once.
<i>Recognise</i>	The "Recognise" mode is the mode before a door is opened. In this mode, the Transponder is released if a fingerprint is correctly recognised.

Q3007 Biometric Transponder

Page 5

2.3 How the transponder works



You can interrupt the action in each mode by pressing the button briefly to change to Standby.

2.4 "Learn" state: start-up, scanning in fingerprints

Initial start-up - scanning in the first 2 fingerprints (Administrator fingerprints)

To start the Q3007, two "Administrator fingerprints" need to be scanned in first of all. We recommend that a fingerprint from the left and right hand of one person, the administrator (e.g. safety officer) is used for this. However, you can also use one finger from two different people.

Q3007 Biometric Transponder

Page 6

Please note:

The first two fingerprints to be scanned in are automatically (!) the Administrator fingerprints. Without them, no further fingerprints can be scanned in or deleted later!

To scan in and store the first Administrator fingerprint (e.g. left thumb), please do the following:

1. Briefly press the transponder button; the LED will flash green.
2. Then press the button again and hold it pressed for at least 3 seconds (until the LED flashes yellow).
3. Release the button. The system is now ready to scan for 30 seconds, and this is indicated by rapid yellow flashing.
4. **As a high quality of the fingerprint to be taught in is important for good recognition during every day use, please make sure, that your finger to be scanned in is not too dry (e.g. breath on them before having them scanned in).**
5. Drag finger across the sensor; the LED goes off; after about 1 second, the LED flashes green once to indicate that the fingerprint has been accepted.
6. When the LED flashes yellow rapidly again, drag the finger to be scanned in across the sensor again.
7. Now repeat steps 4 and 5 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.



Using for the first time – 'learning' the first two fingers (Administrator Fingers)

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow light flashing at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.

The Q3007 can now be used by the Administrator, or other fingerprints can be scanned in. Please note that the second fingerprint that is scanned in also has Administrator rights!

Scanning in more fingerprints (User fingerprints)

Q3007 Biometric Transponder

Page 7

Further fingerprints (maximum 4) can be scanned in as the Administrator fingerprints have been, except that the Q3007 must first be cleared for this by an Administrator fingerprint. This prevents unauthorised persons from scanning in their own fingerprints and thus gaining access rights that are not allowed.

We recommend that every person who is to use the Q3007 should also be scanned in with two fingerprints, one per hand. This means that three people can be scanned in, with two fingerprints for each one. To scan in more fingerprints, please proceed as follows:

1. Briefly press the transponder button and wait until the LED flashes green.
2. Then press the button again and hold it pressed for at least 3 seconds until the LED flashes yellow, then release the button.
3. Draw the Administrator finger across the sensor; the LED goes off and then flashes green once after about 2 seconds. The system is now ready to scan for 30 seconds, and this is indicated by rapid yellow flashing light. Drag the User finger across the sensor; the LED goes off; after about 1 second, the LED flashes green once to indicate that the fingerprint has been accepted.
4. When the LED flashes yellow rapidly again, draw the finger to be scanned in across the sensor again.
5. Now repeat step 4 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow flashing light at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.

Fingerprints that are already known can always be scanned in, even if 6 fingerprints have already been saved. Unknown fingerprints are then rejected by the LED flashing red twice.

Tips:

- Care in scanning in is rewarded by reliable recognition in use.
- Scanning in the same fingerprint several times improves the quality of the scanned features and thus makes the recognition of the fingerprint more reliable.
- Use a firm base when scanning in fingerprints. We recommend operation with one hand when scanning in thumb prints.
- When scanning in fingerprints, drag the finger across the sensor in a straight line, not too quickly, at an even speed and pressure.
- **Make sure that the sensor is clean and that your fingers are not too dry (e.g. by breathing on them before having them scanned).**

6. Now repeat step 4 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow flashing light at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.

Fingerprints that are already known can always be scanned in, even if 6 fingerprints have already been saved. Unknown fingerprints are then rejected by the LED flashing red twice.

Tips:

- Care in scanning in is rewarded by reliable recognition in use.
- Scanning in the same fingerprint several times improves the quality of the scanned features and thus makes the recognition of the fingerprint more reliable.
- Use a firm base when scanning in fingerprints. We recommend operation with one hand when scanning in thumb prints.
- When scanning in fingerprints, drag the finger across the sensor in a straight line, not too quickly, at an even speed and pressure.
- **Make sure that the sensor is clean and that your fingers are not too dry (e.g. by breathing on them before having them scanned).**

2.5 Querying the number of fingerprints scanned in

You can query the number of fingerprints already scanned in as follows:

1. Press the button once briefly (the LED flashes green)
2. Press the button again and hold it down for 1.5 - 2 seconds (not as long as 3 seconds, which will take you into "learn" mode).
3. The LED flashes red.
4. Then the LED will flash green as many times as the number of fingerprints scanned in (max. 6).
5. The LED flashes red (for a long time if the maximum possible number of fingerprints has been reached, or briefly if it has not).

If no fingerprints have been scanned in, the LED flashes red twice and then returns to Standby mode.

2.6 "Recognise" mode: one-off triggering of transponder

The mode known as the Recognise mode is the normal operating state for the Q3007, i.e. a person whose fingerprint has been scanned in would like to trigger a Transponder signal, e.g. to open a door with a digital locking cylinder or to programme the Transponder within a locking plan.

To do this, proceed as follows:

1. Press the button of the Q3007 briefly (for around 0.5 sec.), and the LED will then flash green.
2. Now drag your scanned finger over the sensor. Make sure that it is in the same position as it was when you scanned it in.
3. If the recognition attempt was successful, the LED shows green and the Transponder is triggered.

If the LED shows red, the recognition attempt was not successful. You can now try three more times. If these are not successful, the Q3007 automatically returns to Standby mode.

Please note:

- It may occasionally happen that the Q3007 does not recognise your finger even though it has been properly scanned in.
- If the fingerprint is rejected with a single red flash, the quality of the fingerprint trace was not adequate. This may be due to the fact, for example, that you did not drag your finger properly across the sensor (too quickly, not straight or not even) or that the surface of the sensor is dirty. If a finger is too dry, it may happen that it "judders" across the sensor. If this happens, please repeat the attempt, or moisten your finger slightly before you do so by breathing on it, for example. With a little practice, however, you'll soon get the knack.
- If the features of your fingerprint cannot be assigned to any of the scanned fingerprints, the diode will flash red twice. You may have accidentally presented a fingerprint that has not been scanned in, or you may have drawn this finger across the sensor quite differently initially from the way you are doing it now (e.g. at an angle, or with more or less of your fingertip in contact with the sensor).

Tip:

Not every fingerprint from a person is recognised equally reliably. If you are often not recognised with one finger, you should perhaps scan in another finger.

Make sure that the sensor is clean and that your fingers are not too dry (e.g. by breathing on them before having them scanned)..

3.0 "Delete" mode: deleting fingerprints

Both individually scanned fingerprints and all the fingerprints can be deleted from the memory.

If normal fingerprints (not Administrator fingerprints) are deleted, the other fingers that have been scanned in are not deleted. No Administrator fingerprint is needed to do this (any normal user can delete his own fingerprint).

If one of the two Administrator fingerprints is deleted, all the fingerprints are automatically deleted. The first two fingerprints that are then scanned in are automatically the Administrator fingerprints again.

Fingerprints are deleted as follows:

1. Briefly press the transponder button and wait until the LED flashes green.
2. Then press the button again and hold it pressed for at least 3 seconds until the LED flashes yellow. Release the button.
3. Press the button again and hold it pressed for at least 3 seconds until the LED flashes red. Release the button. You are now in the "Delete" state.
4. Drag finger across sensor.
5. If the first recognition attempt was successful, the LED flashes green. If the fingerprint is a normal one (user fingerprint), only this fingerprint is deleted; if it was one of the two Administrator fingerprints, then all the fingerprints are deleted. Deleting all the fingerprints can take up to 15 seconds. During this time, the diode flashes red every 2 seconds.
6. If the LED flashes yellow, the recognition attempt was not successful. You can now try three more times. If these all fail, the Q3007 automatically returns to Standby mode.

4.0 Transparent mode

It is possible to switch the Biometric Transponder to what is called Transparent mode. In this state, the biometric inquiry is interrupted for 5 minutes and the Biometric Transponder can be used as a normal transponder (doors can be opened simply by pressing a button). At the end of 5 minutes or so, the Biometric Transponder returns to Standby mode.

Transparent mode is required, for example, for setting/cancelling alarms (if an SV Shuntlock VdS is installed) or if several doors need to be passed through in a short time.

To enter Transparent mode, please proceed as follows:

1. Press and hold the transponder button (longer than 1.5 seconds, < 3 sec.). The LED will flash green rapidly. The Transponder will now react to the button as if it were in Recognise mode.
2. Drag finger across sensor (LED shows green if the fingerprint is recognised).
3. The Biometric Transponder is triggered and switches to Transparent mode. The LED flashes red.
4. Pressing the button triggers the system and the LED shows green, followed by red flashing.

After 5 minutes, the Transponder switches off Transparent mode and returns to Standby.

Transparent mode can also be switched off manually by pressing the Transponder button before automatic switch-off until the green LED goes out (approx. 1.5 sec).

5.0 Programming the Transponder with the SimonsVoss software

The "Set validity" function and the "Quasi-proximity mode" are not available for the Q3007.

6.0 Changing the Batteries

To replace the batteries, push the battery cover downwards and remove. Take out all the batteries and replace with new ones. Make sure that the polarity is correct (stamped into the base of the battery compartment).

Q3007 Biometric Transponder

Page 12

7.0 Technical Data

Dimensions: H x W x D	65 x 32 x18 mm
Weight	22 g
Colour	Grey, with blue button
Operating distance, locking cylinders	approx. 40 cm (if the transponder (lengthways) is held parallel with the cylinder antenna)
Operating distance, Smart Relay	approx. 120 cm (if the transponder is parallel with the antenna of the Smart Relay)
Protection category	IP 54
Operating temperature range	0°C to 40°C without condensation
Battery type	3 V DC lithium battery type CR-1/3N

8.0 Table of Diode Signals

LED	Mode
off	Standby
off	moving finger on sensor followed by comparison with scanned fingerprint, please wait (max. 4 seconds)
Slow green flashing light	Recognise mode, wait for finger (max. 30 seconds)
Fast green flashing light	Release for transparent mode, wait for finger (max. 30 seconds)
One green flash	Successful action (recognise, learn, save, delete, trigger)
Slow yellow flashing light	Release for Learn mode, wait for Administrator finger (max. 30 seconds)
Fast yellow flashing light	Learn mode, wait for finger (max. 30 seconds)
Yellow flashing light	Save scanned finger, please wait (max. 5 seconds)
One or two yellow flashes	Error message in Delete state (cf. 1x or 2x red flashing)
Slow red flashing light	Delete state, wait for finger (max. 30 seconds)
Red flashing light	Delete scanned fingerprint, please wait (max. 15 seconds)
Red flashing light	Transparent state (max. 5 minutes)
Flash red 1x	Action unsuccessful
Flash red 2x	Fingerprint not recognised
Red, 0 to 6 times green, red	Query number of scanned-in fingerprints

PinCode Keypad 3068

State of : September 2006

PinCode Keypad 3068

Content

1.0	General information	4
1.1	Safety Remarks _____	4
1.2	Product Description _____	5
2.0	Functional Overview	5
2.1	Function Overview _____	5
2.2	Operating modes _____	6
2.3	Operating _____	6
3.0	Start-up	7
4.0	Programming PINs	8
4.1	First Startup _____	8
4.2	Programming Additional PINs. _____	8
4.3	Procedure _____	9
5.0	Deleting PINs	9
5.1	Description _____	9
5.2	Procedure _____	10
6.0	Programming the Transponder Data Records with the	10
6.1	Assignment of PINs and Transponders _____	10
6.2	Description _____	11
6.3	Procedure _____	12
7.0	Reading out Transponders	12
7.1	Description _____	12
7.2	Procedure _____	12
8.0	Resetting Transponders	13
8.1	Description _____	13
8.2	Procedure _____	13
9.0	Opening	14
10.0	Meaning of the LED	14
11.0	Battery Warning	15
12.0	Battery Replacement	15

PinCode Keypad 3068

Content

13.0 Special Functions	17
13.1 Hidden Lock for SimonsVoss VdS Shuntlock 3066 _____	17
13.2 Miscellaneous _____	18
14.0 Technical Specification	18

1.0. General information

Please take 15 minutes and read through these Instructions in order to familiarise yourself with the function of your PinCode Keypad..



1.1 Safety Remarks

Caution! Incorrect handling of the batteries used in this product can result in the risk of fire or burns. Do not charge, open or burn these batteries or heat them to more than 100° C (212° F).

Make sure that the PinCode Keypad remains free of dirt and scratches; do not drop the Keypad or otherwise subject it to heavy impacts.

Furthermore, please note that you should program the Keypad with a PIN code immediately after you start it up.

Use of a SimonsVoss PinCode Keypad requires knowledge of the use of the product and of the SimonsVoss software. For this reason, only trained and authorised personnel should program the PinCode Keypad.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect programming.

If the PinCode Keypad is incorrectly programmed or is defective, access through a door may be blocked. SimonsVoss AG is not liable for the consequences, such as blocked access to injured or endangered persons, property damage or other damages.

The casing of the PinCode keypad is secured with two Torx screws (TX6) for increased security against unauthorised opening.

1.2 Product Description

The PinCode Keypad 3068 is a digital "key" (transponder), which opens SimonsVoss lockings without contact via radio transmission after the correct numerical codes are entered.

To configure the system, you must first correctly configure at least one PIN and the associated integrated transponder for the locking. The associated locking is then released after a correct PIN has been entered.

The PinCode Keypad that you have purchased is a product that can be used both inside and out. The product has its own power supply, so that it can be operated completely self-sufficiently. Installation is very simple, because absolutely no cabling is required.

Because of the modularity, this component can be seamlessly integrated into the SimonsVoss System 3060, and, like all SimonsVoss components (on the transponder side), it can be programmed with the locking plan software.

2.0 Functional Overview

2.1 Function Overview

The PinCode Keypad comprises the following components:

- PIN code input and evaluation
- Integrated digital key (transponder), which opens the associated locking when it is triggered after the PIN code has been evaluated successfully.

Consequently, the PinCode Keypad allows you to address all SimonsVoss lockings (such as cylinders, Smart Relays, and even activation units, etc.) using the PIN code.

Three different PINs are available, so that individual PINs can be assigned to up to 3 people or groups of people. When a PIN is reprogrammed, only one of up to three user groups needs to be informed. Furthermore, in SimonsVoss lockings (with the time control function, meaning access control and time zone control), it is possible to grant a person or group of people access to a building only during certain times, and to keep a record of which PIN accessed the locking at what time.

2.2 Operating modes

The PinCode Keypad has four distinct operating modes:

Mode:	Explanation:
Standby	The PIN Code Keypad is in standby mode, and uses only very little power.
Opening	After a correct PIN has been entered, the locking is addressed via radio transmission and can be operated.
Programming	In this mode, the following can be programmed or reset: <ul style="list-style-type: none">• the individual PINs (max. 3) - directly via the Keypad• or the associated integrated transponders (max. 3) - using the SimonsVoss software
Battery warning	A two-level battery warning system provides plenty of advance notice when it is almost time to change the batteries.

2.3 Operating

After starting up and configuring the PinCode Keypad, it and a SimonsVoss locking represent a so-called "hidden lock" within the System 3060. You can program the PIN directly by making entries on the Keypad. On the other hand, the integrated transponders are programmed by means of the SimonsVoss software, and incorporated into the locking system in this way. The following sections describe the precise procedure for programming individual PIN codes and for programming the associated transponder data records, and the use of the PinCode Keypad.

3.0 Start-up

The first time the system is started up, you will need to replace the factory-set

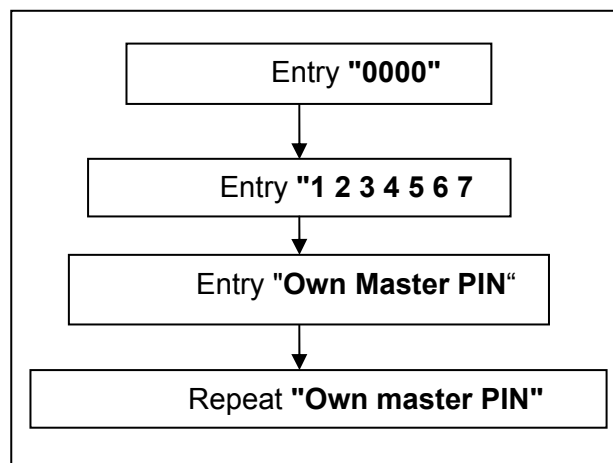
master PIN: **1 2 3 4 5 6 7 8**

with your own master PIN.

Requirement:

- 8 digits
- may not start with a "0"

Your personal master PIN is needed for all programming processes for authentication purposes. Please keep it in a safe place where it cannot be accessed by unauthorised persons.



4.0 Programming PINs

The Master PIN required for all programming procedures is defined by the user (e.g. the System Administrator). Please keep it safe and inaccessible to unauthorised persons, since the Master PIN is required for all programming procedures.

4.1 First Start-up

For the first start-up, the safety of your locking system requires that you program at least one PIN. Only after the PinCode Keypad has been programmed can it be guaranteed that only authorised users receive access.

Proceed as follows:

1. Press the **"0"** to change to programming mode.
2. Enter the **"master PIN "**.
3. Select the PIN that you want to program; in this case, press **"1"** for **"PIN 1"**.
4. Enter the length of the PIN (you can choose a number with from **4-8** digits).
5. Enter the **"PIN"**
6. If the input was correct, the PIN is saved and confirmed.

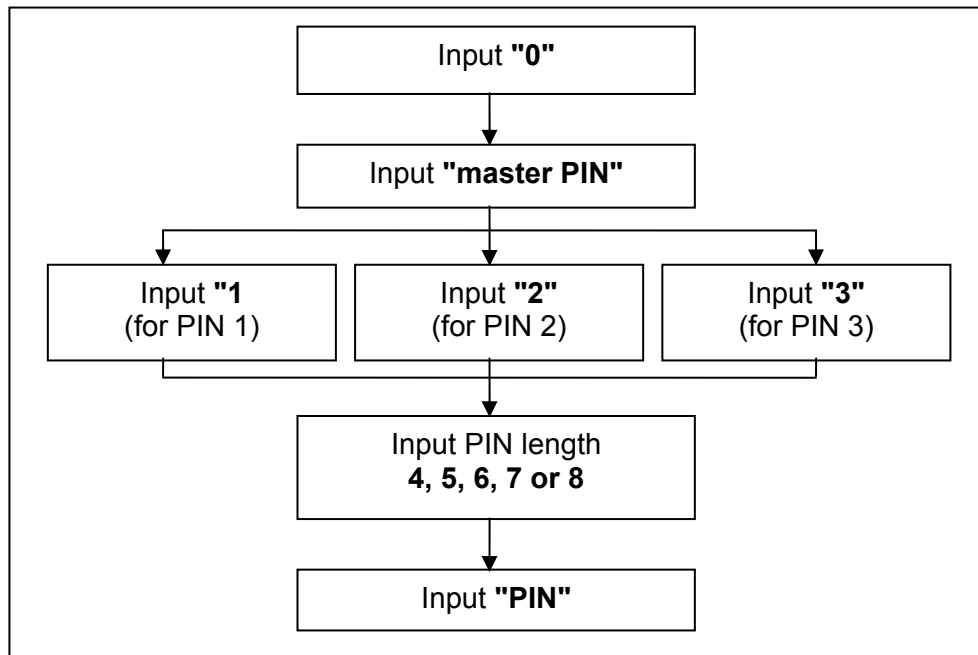
A PIN is not permitted to begin with **"0"** and you may not assign the same PIN more than once. The master PIN is used only for programming the PIN. It is not possible to operate lockings with the master PIN.

4.2 Programming Additional PINs.

1. To program additional PINs, please proceed as follows: Press the **"0"** to change to programming mode.
2. Enter the **"master PIN"**.
3. Press
 - **"2"** for **"PIN 2"** or
 - **"3"** for **"PIN 3"**.
4. Enter the length of the PIN (you can choose a number with from **4-8** digits).
5. Enter the corresponding **"PIN"**.
6. If the input was correct, the PIN is saved and confirmed.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot change or delete a PIN. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement").

4.3 Procedure



5.0 Deleting PINs

5.1 Description

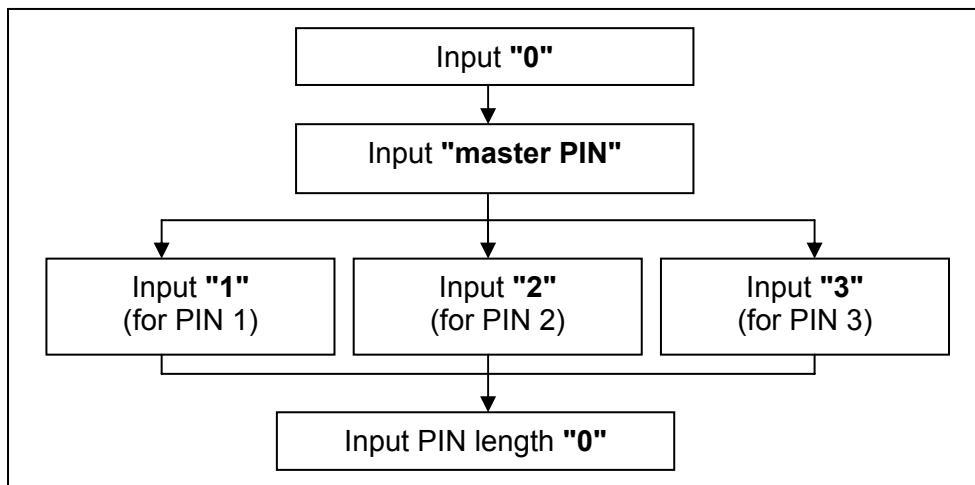
To deactivate PINs again, follow these steps:

1. Press "0" to change to programming mode.
2. Enter the "master PIN".
3. Press
 - "1" for "PIN 1" or
 - "2" for "PIN 2" or
 - "3" for "PIN 3".
4. For the PIN length, enter "0".
5. If the input was correct, the PIN in question is deleted.

In this way, you can deactivate one or more PINs again. They can only be reactivated if you program them again. If you do not need all the PINs, you can leave the extra one unprogrammed.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that it is not possible to change or delete PINs when there is a weak battery. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement").

5.2 Procedure



6.0 Programming the Transponder Data Records with the Simons Voss Software

6.1 Assignment of PINs and Transponders

- PIN1 ⇒ Transponder 1
- PIN2 ⇒ Transponder 2
- PIN3 ⇒ Transponder 3

Each integrated transponder has its own transponder ID (TID); the TIDs are saved in the SimonsVoss lockings when there is an access if the lockings have the time control function (i.e., access control). In this way, you can tell precisely which PIN was granted access and when.

6.2 Description

To program the various transponders with the SimonsVoss software, please follow the procedure described in the following (also see the SimonsVoss "Software Manual"):

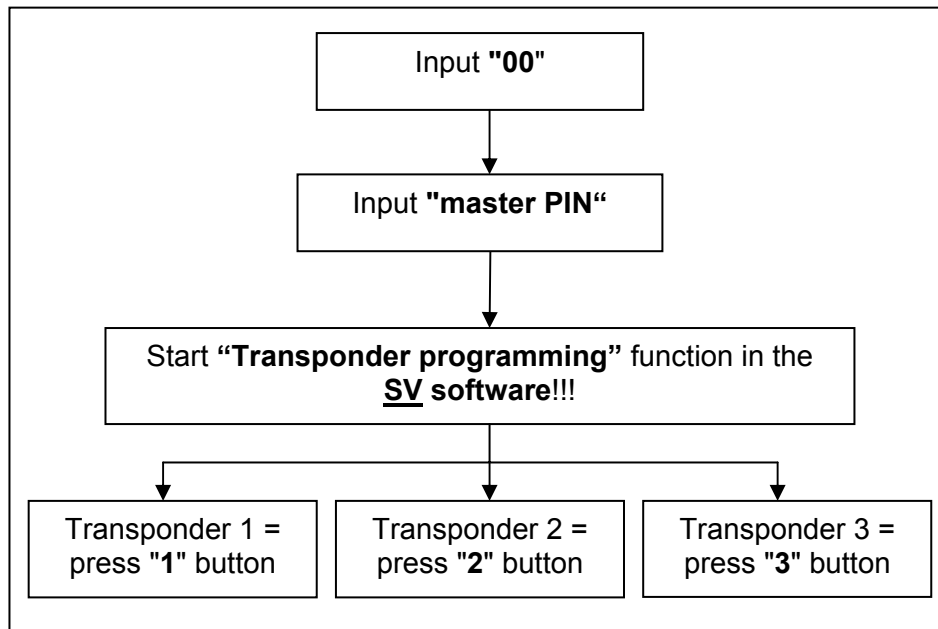
1. Press the "0" button twice in order to enter the transponder programming mode.
2. Enter the "**master PIN**".
3. Start the **Transponder programming** function in the SV software
4. For the particular transponder:
 - Transponder 1 = press the "1" button
 - Transponder 2 = press the "2" button
 - Transponder 3 = press the "3" button
5. Please check in the user interface to see that the programming was successful (yellow programmer flash must have been removed in the locking plan).

In order to be able to carry out the programming without problems, please first start the programming command in the SV software and only then select the required transponder using the PinCode Keypad. Otherwise it is not possible to guarantee successful programming.

The PinCode Keypad's three integrated transponders must be located in the same locking plan as the locking that you wish to address.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that it is not possible to change or delete transponders when there is a weak battery. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement").

6.3 Procedure



7.0 Reading out Transponders

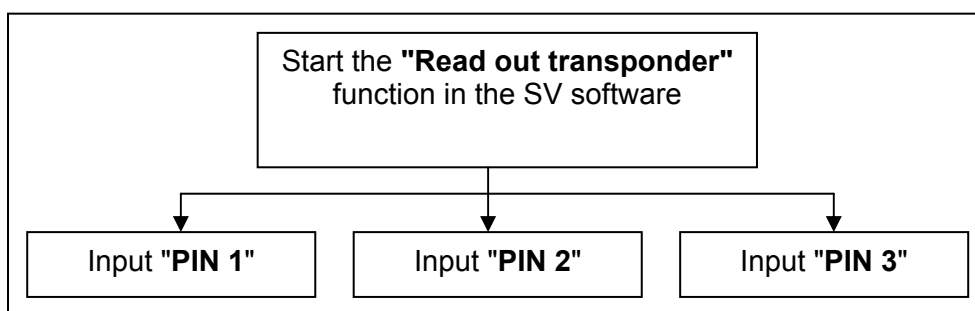
Anytime it is possible to read out the integrated transponders (after they were programmed) with the SimonsVoss locking plan software.

7.1 Description

To do this, proceed as follows:

1. Start the **"Read out transponder"** function in the SV software
2. For the particular transponder:
 - Transponder 1 = enter **"PIN 1"**
 - Transponder 2 = enter **"PIN 2"**
 - Transponder 3 = enter **"PIN 3"**

7.2 Procedure



8.0 Resetting Transponders

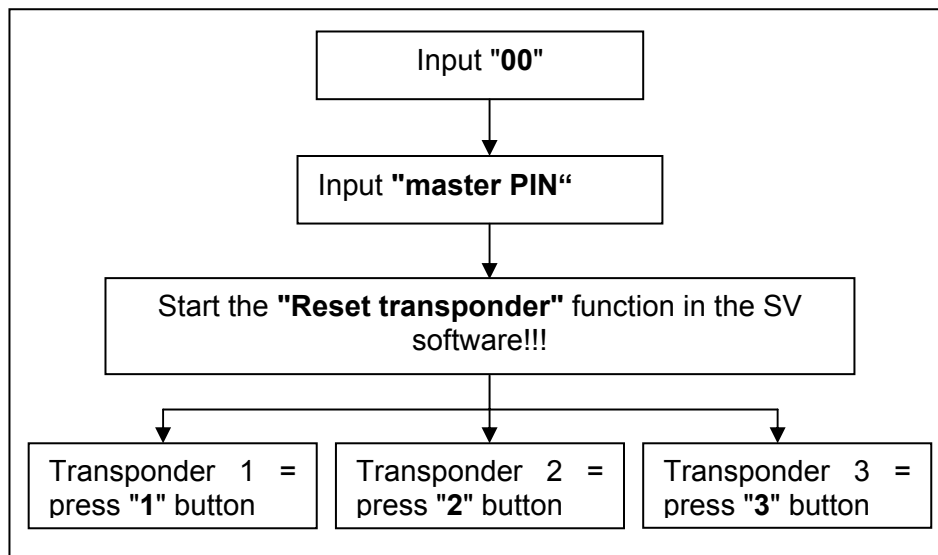
8.1 Description

To reset the various transponders, please proceed as follows:

1. Press the **"0"** button twice.
2. Enter the master PIN.
3. Start the **"Reset transponder"** function in the SimonsVoss software.
4. For the particular transponder :
 - Transponder 1 = press **"1"** button,
 - Transponder 2 = press **"2"** button
 - Transponder 3 = press **"3"** button

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot reset a transponder. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement").

8.2 Procedure



9.0 Opening

In order to use the PinCode Keypad to open the associated locking, proceed as follows:

Enter a PIN that has already been programmed. You are not permitted to wait more than 5 seconds between the entries of the individual numbers.

If you have entered the correct number and the integrated transponder has been programmed, the LED lights GREEN and a signal is sounded. Then the integrated transponder opens the locking.

10.0 Meaning of the LED

The built-in LED can light in one of three colours: green, yellow and red. These colours have the following meanings:

- Green Digit that was input has been accepted

PIN input was OK, which means that
the correct PIN has been recognised, open signal is being sent

PIN length OK
PIN programming procedure was successful
- Yellow battery warning
- Red PIN input was incorrect

Input of master code was incorrect
Repeated incorrect input of the PIN (manipulation)
PIN length was not entered correctly.

11.0 Battery Warning

To obtain a defined status for the PinCode Keypad and to minimise operating errors, a 2-level battery warning system has been integrated.

When the battery capacity begins to drop, you will be notified of this in plenty of time to allow you to replace the batteries.

Battery warning level 1: The opening procedure is carried out after a delay. The diode blinks YELLOW and the buzzer sounds for 10 seconds. The PinCode Keypad does not send the open command until after these 10 seconds.

Battery warning level 2: In this case, the opening procedure is again carried out after a delay. The diode blinks YELLOW and the buzzer now sounds for 20 seconds. The PinCode Keypad does not send the open command until after these 20 seconds.

You should not wait any longer to replace the battery. Otherwise, the system will stop functioning after a short time.

12.0 Battery Replacement

In general, the batteries must be replaced by trained experts only. To do this, proceed as follows:

1. Completely unscrew the two screws in the bottom of the housing.
2. Remove the front of the housing.
3. Carefully release the battery clip from the printed circuit board (Figure 1).
4. Remove both batteries (Figure 1).
5. Insert the new batteries; the positive pole must be pointing up (Figure 2).
6. Carefully hook the battery clip back into the printed circuit board (Figure 3).
7. Put the housing back on.
8. Screw the two housing screws back into the housing from below.

After you have replaced the batteries, all functions will be available again. Please always replace both batteries at the same time, because they have been charged to approximately the same level.

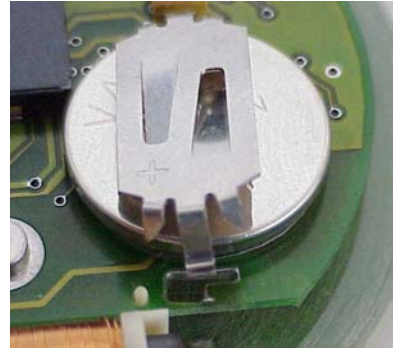
PinCode Keypad 3068

Page 16

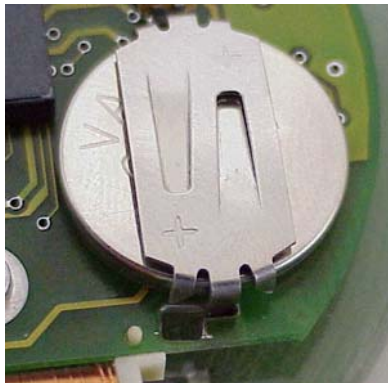
When replacing the batteries, be absolutely sure that no water is allowed to penetrate into the housing and that the electronics do not come into contact with water. If necessary, carefully wipe dry the housing section that is attached to the wall.



(picture 1)



(picture 2)



(picture 3)

13.0 Special Functions

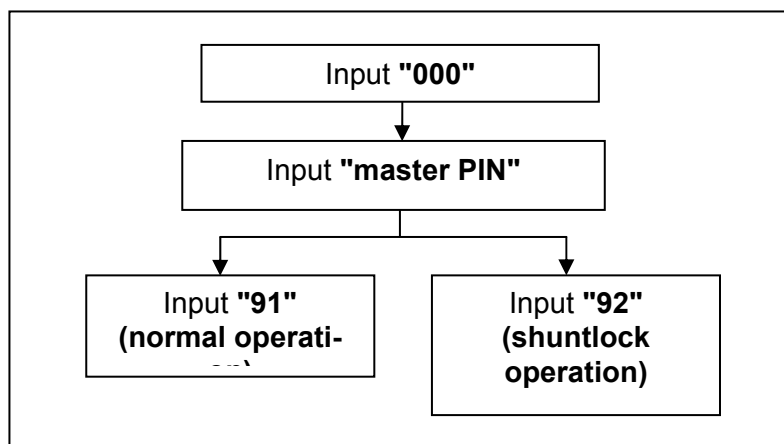
13.1 Hidden Lock for SimonsVoss VdS Shuntlock 3066

The PinCode Keypad can be used for activating SimonsVoss activation units (VdS Shuntlock 3066). This is done by mounting the Keypad within the transmitting range of the activation unit. After you have input the correct PIN, the activation unit is addressed and the alarm system is activated or deactivated via the shuntlock. This allows the requirements of VdS Class C up to SG 6 to be fulfilled by including a hidden lock.

The VdS-certified activation units from SimonsVoss need a doubled opening protocol for activation/deactivation procedures (double-click when the transponder should activate or deactivate the system).

The following explains the configuration of the PinCode Keypad in order to have it emulate the "double-click" and consequently be suitable for carrying out activation/deactivation procedures. To set the configuration for this purpose, proceed as follows:

1. Press the **"0"** button three times.
2. Input the master PIN.
3. Then press:
 - either **"91"** for normal operation (default setting)
 - or **"92"** for a double-click for shuntlock operation.



If the input was correct, the PinCode Keypad stores the change and gives a positive acknowledgement (LED and buzzer).

Important: Please set the two-time opening protocol (double-click) only when you are using a SimonsVoss VdS Shuntlock 3066. Otherwise, there may be malfunctions or unwanted effects.

You can switch from one configuration to the other at any time.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot change or delete any functions. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement").

13.2 Miscellaneous

The quasi-proximity and validity and expiry mode functions are not available with the PIN Code Keypad.

14.0 Technical Specification

Dimensions W x H x D	96 mm x 96 mm x 14 mm
Weight	102 g (incl. batteries)
Material	Plastic
Colour	Grey with transparent ring
Maximum number of operations with one battery set	Approx. 100,000 operations or 10 years on standby
Operating distance from locking cylinder	Up to a max. of 40 cm (when the transponder antenna is parallel to the cylinder antenna)
Operating distance from SmartRelay	Up to a max. of 120 cm (when the transponder antenna is parallel to the SmartRelay antenna)
Protection class	IP 65
Working temperature range	-20° C to 50° C (-4° F to 50° F) without moisture condensation
Battery type	2 x 3 V DC lithium battery type CR2032
Battery replacement	Only by trained personnel

LON – Network 3065

State of: September 2006

1.0	Introduction	4
1.1	General Information	5
1.2	Connection to LPI-10	
	(Version: Open PCB With External Plug-in Power Supply)	6
1.3	Connection to LPI-10 Compact	6
2.0	The Software	7
3.0	Central Node	8
3.1	Method of Operation	8
4.0	Lock Node	9
4.1	Method of Operation	9
4.2	Assembly Instructions	9
4.3	Antenna Extender	10
4.4	LockNode Inputs and Outputs	12
5.0	LPI-10	13
5.1	General Warnings	13
5.1.1	Risk of Electric Shock	13
5.2	LPI-10	13
5.2.1	Method of Operation	13
5.2.2	Assembly Instructions	14
5.3	LPI-10 Compact (Version: compact construction with 230V	
	power supply from the customer)	15
5.3.1	Installation	15
5.3.2	Method of Operation	16
5.3.3	Assembly Instructions	16
6.0	Router	17
6.1	Method of Operation	17
6.2	Assembly Instructions	18
6.3	Installation Example	19

LON – Network 3065

Content

7.0	Repeater	20
7.1	Method of Operation	20
7.2	Assembly Instructions	20
8.0	Terminators	20
9.0	Network Cable	21
9.1	General Information	21
9.2	Cable Laying	21
9.3	Cable Types	21
9.4	Bus-Shaped Cabling (Example)	22
9.5	Star-Shaped Cabling (Example)	22
10.0	Planning Examples	24
10.1	Connecting External Buildings via Twisted Pair, Modem & TCP/IP	24
10.2	Network via Modem	25
10.3	Network via Ethernet	25
11.0	Security	26
11.1	Secure Communication Between the Network Nodes	26
11.2	Automatic Tests of Separate System Components	26
11.3	Alarms	26
12.0	Answers to the Most Common Questions	
	Regarding the Network	27
13.0	Data sheet	29

1.0 Introduction

In the following, we always speak of locking(s) and doors as the System 3060 components (locking cylinder, control unit, Smart Relay, shuntlock). Unless otherwise expressly mentioned, however, this information is valid for all other System 3060 components.

Programming the System 3060 with a laptop and SmartCD is advisable up to a certain object size or for customers with a limited number of doors, because changes in the configuration of the lockings usually do not have to be made often in this case.

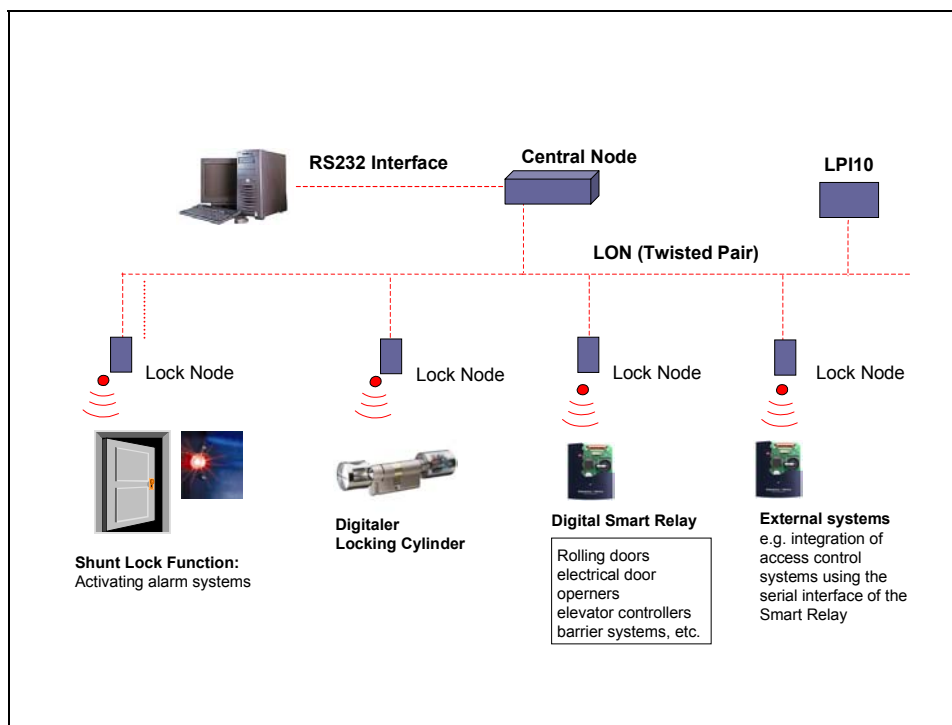
For medium-sized or large objects, where it happens more often that keys are lost, new transponders have to be approved, and there are organisational changes, there is the possibility of caring for and maintaining the locking system via the network. This does not necessarily mean that all doors have to be networked, however. The entire system can also be designed for mixed operation (networking/standalone).

In a networked system, it is not only possible to take care of all maintenance and programming tasks from one central PC, it is also possible to obtain an overview of the current status of the entire network. For example, it is possible to check locking and door conditions, such as door open/door closed and door locked, and to display battery warnings, the access journal and burglar alarms from a central location. This makes it possible to react to an event directly from the control center.

In summary, it can be stated that using networking, it is possible to configure and monitor the entire access control system from one central PC. This means that the user can react to critical conditions in a short time.

1.1 General Information

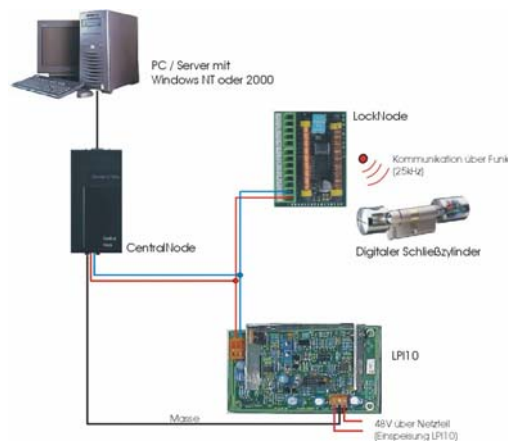
A so-called LockNode is placed next to the digital locking at a distance of about 30 cm (12 inches), depending on the particular components installed (refer to page N7). This LockNode maintains radio contact with the locking. The digital lockings do not need additionally wiring. The CentralNode forms the interface between the computer and the network.



Before starting to install the components, you should check the cable for continuity and short circuits, in order to avoid any hardware defects.

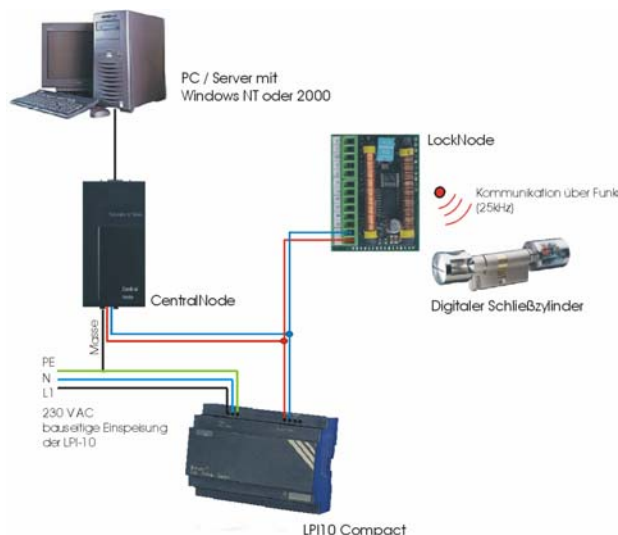
1.2 Connection to LPI-10 (Version: Open PCB With External Plug-in Power Supply)

The LockNodes are connected to the CentralNode using a two-wire line (twisted pair). The LPI-10 (version: open printed circuit board with external plug-in power supply) provides the LockNodes with voltage over the same line.



1.3 Connection to LPI-10 Compact

The LockNodes are connected to the CentralNode using a two-wire line (twisted pair). The LPI-10 (version: compact construction with 230V supply from the customer) provides the LockNodes with voltage over the same line.



2.0 The Software

If you use a PC to administer the locking system, you only need the locking plan software LDB^{*1} or LSM^{*2}. To access the locking system from more than one workplace, you must have LSM installed.

In network operation, the LDB^{*1} software handles functions for visualisation, filtering, encoding, network management and data calibration. You can read out, change and verify all network components. Only trained personnel are permitted to install the network, in order to guarantee trouble-free function.

^{*1} LDB = Lock Data Base

^{*2} LSM = Locking System Management

- Please refer to the chapter on "Commissioning" in the software operating instructions for information on the system requirements for the locking plan LDB.
- Please refer to the LSM - Locking System Management handbook for information on LSM system requirements.

To operate the Network 3065, you must have a license, which depends on the size of the network. These licenses are available in the following progressive sizes:

For networks with max.	12	LockNodes
For networks with max.	48	LockNodes
For networks with max.	128	LockNodes
For networks with max.	258	LockNodes
For networks with max.	516	LockNodes
For networks with max.	1032	LockNodes

3.0 Central Node

3.1 Method of Operation

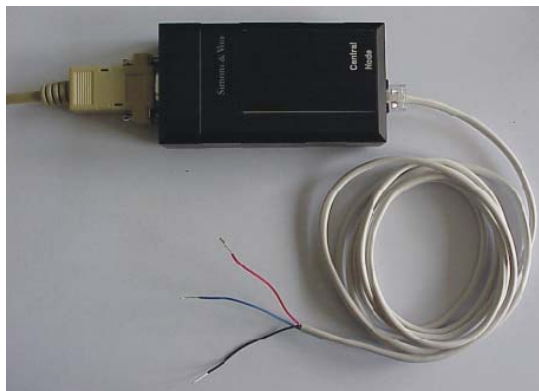
The CentralNode produces the interface between the PC and the network. One CentralNode is needed per network.

- ☺ To use a CentralNode in combination with LSM, please contact your trade partner or the manufacturer.

The CentralNode is connected to a free serial interface (e.g., COM1) on the PC. The ConfigDevice (or SmartCD) needed for programming transponders is connected to a different free interface on the PC (e.g., COM2). If only one interface is available, you can alternately connect the ConfigDevice (or SmartCD) and the CentralNode, depending on which you need. To do this, you must specify the device currently being used in the locking plan software. Insert the connection cable, which is delivered with the system, to the RJ-45 socket of the CentralNode.

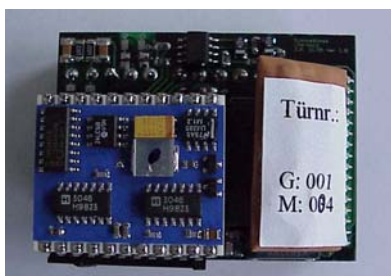
The red and blue lines on this cable are available for connection to the in-house network cable; the black line on the cable is for grounding. In order to guarantee flawless functioning of the network, the black line must be connected to the LPI-10's potential compensation. The cable's screening can be used for grounding.

- ☺ The CentralNode does not need a supply voltage. This is already provided by the LPI-10 over the network cable.



4.0 Lock Node

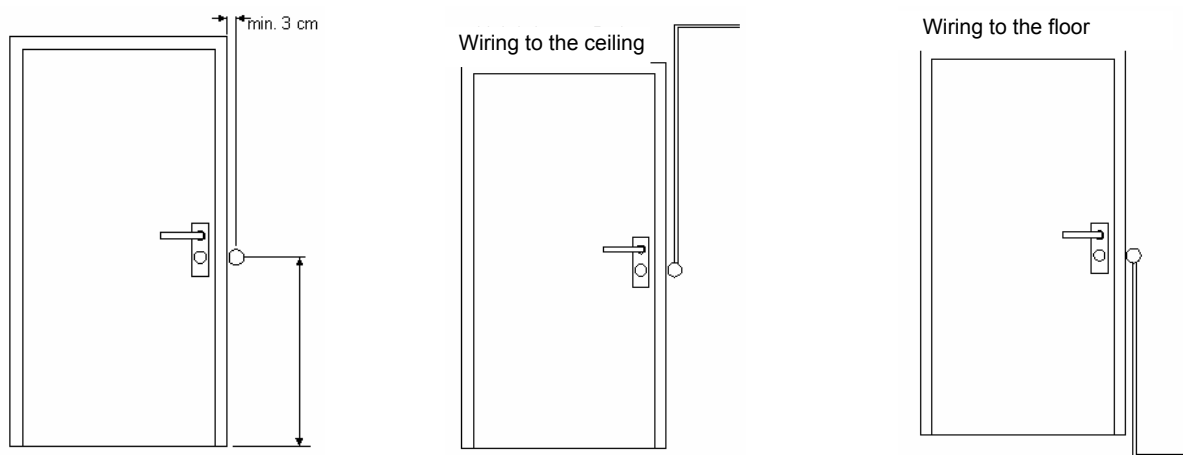
4.1 Method of Operation



The LockNode takes on all programming assignments in the network. Data is also transmitted to the digital components by radio.

4.2 Assembly Instructions

The LockNodes are pre-configured by SimonsVoss and are provided with numbers (see the picture on page N6). These numbers (GID: GroupID, M: MemberID) are entered in the set-up diagram for the building that is to be networked. During installation, assign the LockNodes in the software on the basis of this set-up diagram. Do not exchange the LockNodes, since otherwise no network connection can be made to the digital components.



The LockNodes can be built into the lighting strip next to the door in a commercially available flush-socket device or cavity socket (at least 40 mm deep) with accompanying dummy cap. You should completely remove the network cable screening in the flush socket device or cavity socket (only star-shaped wiring).

In networks with no topological structure and for BUS wiring, the screening of the respective network cables should be connected in such a way (external terminal or soldering, each with shrink sleeve) that screening is guaranteed for the entire network cable.

The terminator is then inserted at the last LockNode in the BUS wiring, and its grounding cable (green-yellow) is connected to the screening (shield) or equipotential bonding.

In order to guarantee proper radio transmission, you should maintain the following distances between the LockNode and the digital locking:

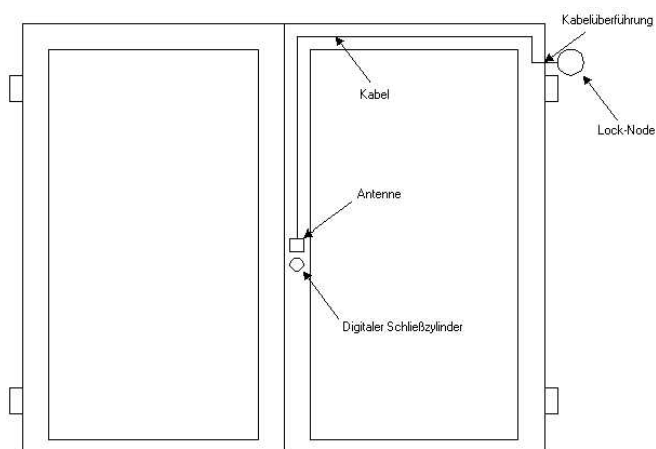
	Minimum	Maximum
LockNode to the digital locking cylinder	10 cm	30 cm
LockNode to the digital control unit	20 cm	100 cm
LockNode to the Smart Relay	50 cm	100 cm
LockNode to the activation unit	20 cm	100 cm

- For distances between the LockNode and the control unit of less than 20 cm or less than 50 cm between the LockNode and the Smart Relay, we ask that you contact your dealer or the manufacturer.
- The LockNodes must be built according to the layout plan drawn up during planning. The plan indicates the position of the LockNodes and specifies the group and member IDs. This information is printed on the LockNode. All necessary wires must be connected to the LockNode terminal strip. (Network cable connection: terminals 1 and 2. The polarity is not relevant).

4.3 Antenna Extender

Since the standard range of the LockNode is not sufficient for double doors, a LockNode with an extended antenna must be used in this case. The extended antenna is mounted in the door (in the immediate vicinity of the cylinder) and connected to the LockNode via a cable transfer on the door.

- To guarantee that the radio transmission functions correctly, we recommend that you provide a plastic inspection flap at the level of the antenna.

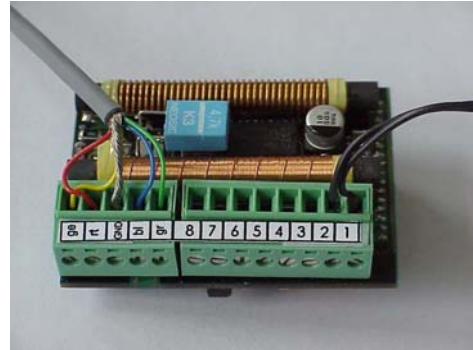


- You can always attain wider ranges by using FH versions.
- Make sure that the cable of the extended antenna is exactly the length needed. You should always cut off any extra cable length.

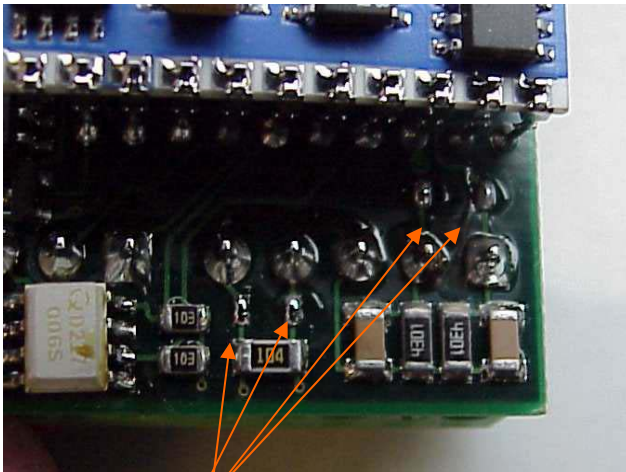
LON – Network 3065

Page 11

Connect the network cable to terminals 1 and 2 of the LockNode. If you need an antenna extender because of a double door, connect the antenna extender cable to the terminals, according to the line colours.



When connecting the extended antenna, also remove the four solder bridges (0 Ω resistors) on the LockNode printed circuit board. Otherwise, the LockNode cannot function with the extended antenna.



Solder bridges (closed)

To open the solder bridges, please use an appropriate tool (adjustable soldering iron and unsoldering suction pump).



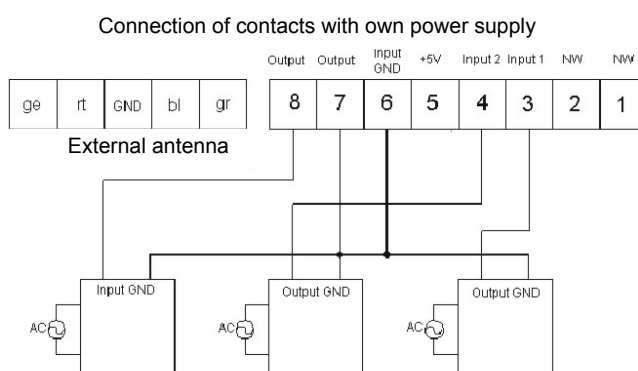
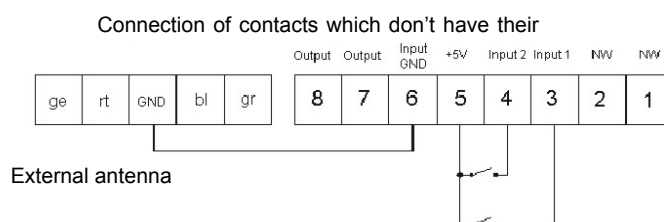
Only authorised personnel should install and open the solder bridges.

4.4 LockNode Inputs and Outputs

Terminals 3 to 8 are available for floating inputs or one output. The inputs transmit the state of the door or lock contact, for example. However, you can also incorporate external systems, such as motion detectors, photoelectric barriers, etc., into the system and then also report their signals to the central computer. You can use the output to pass on signals to external systems, such as heating, light, etc.

You can use the internal power supply of the node to connect switches or contacts without a separate power supply and without a ground connection.

Follow the technical specifications for the inputs or the output when connecting them. Refer to the data sheet for this information.



5.0 LPI-10

5.1 General Warnings

The LPI-10 is a regulated power supply, designed for use in single-phase AC power networks. Furthermore, it is a built-in device, so that it is intended for installation in a distribution box or control cabinet. You must comply with the relevant DIN/VDE regulations or the regulations that apply to your country when installing the device. You must connect the supply voltage in compliance with VDE 0100 and VDE 0160. You must provide a protective device (fuse) and a power supply disconnecting device.

Correct and safe operation of this device requires proper transport and professional storage, assembly and installation.

5.1.1 Risk of Electric Shock

Operation of electrical devices inevitably requires that certain parts of these devices carry hazardous voltage. Improper handling of these devices can therefore result in death or serious bodily injury, as well as in considerable property damage.

5.2 LPI-10 (Version: open printed circuit board with external plug-in power supply)

5.2.1 Method of Operation

You need at least one LPI-10 for each network segment in order to supply the LockNodes. The LPI-10 also needs a separate supply voltage of 48 Volts DC.

There are two models available for this, depending on the size of the network:



- LPI-10 with 48V plug-in power supply for max. 40 LockNodes
- LPI-10 with 48V plug-in power supply for max. 62 LockNodes

Larger networks use proportionately more LPI-10 modules.

5.2.2 Assembly Instructions

The LPI-10 is intended for installation in distribution boxes with DIN rails. You will also need an outlet for the plug-in power supply of the LPI-10. Depending on the structural situation and number of groups, you can also put several power supplies and routers in one distribution box.



Connect the network cable (twisted pair) here. You can also lay a network cable to the router (if there is one). Connect the cable to terminals 17 and 18 there. An additional network cable goes from the router to the Lock-Nodes.

Connect the plug-in power supply to these terminals. Make sure that the polarity (+/-) is correct. This is printed on the connecting terminals. Ground the LPI-10 on the middle terminal.

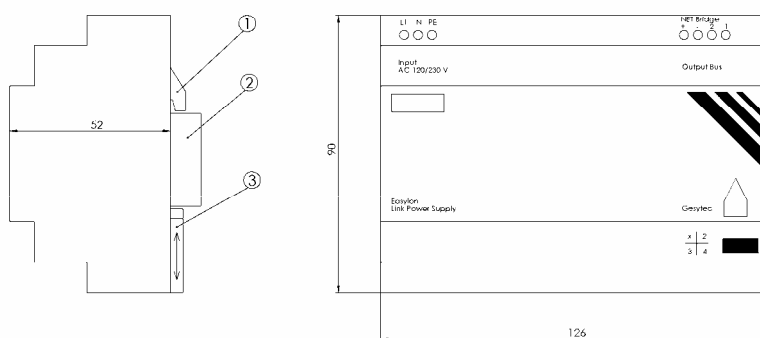
- 👉 Build the LPI-10 into the separate segments in such a way that there is voltage of at least 35V DC on each LockNode.
- 👉 Consequently, the installation location depends on the number and particular distribution of the LockNodes in the corresponding segment.
- 👉 If it is not possible to guarantee voltage of 35 VDC at each LockNode with one LPI-10, you must install a repeater (including power supply) and an additional LPI-10 (including power supply) in the segment.
- 👉 The LPI-10, as it comes from the factory, does not have any over voltage protection. For this reason, this protection should be already provided for by the customer.
- 👉 When commissioning the LPI-10 and the network, you must make sure that the line voltage that is applied is 230V~ (+/- 10%). Higher or lower line voltage input to the LPI-10 can lead to disturbances in the network.

5.3 LPI-10 Compact (Version: compact construction with 230V power supply from the customer)

5.3.1 Installation

Only a qualified expert who is familiar with and who complies with the generally applicable rules of the technology and the regulations and standards valid at the time is permitted to assemble and wire the LPI-10.

The device can be snapped on to DIN EN 50022-35 x 15 and DIN 50022-35 x 7.5 standard mounting rails. To snap the device in, hang it in with the catch ① in the top-hat rail ③ and press until the spring ② snaps into place (see following drawing). If it is too hard to snap it in, loosen the spring ② somewhat. To remove it from the DIN rail, use a screwdriver to loosen the spring ② in the direction of the arrow and remove the device.



To ensure proper heat dissipation, you must install the device vertically, so that the input and output terminals are at the top. There should be at least 5 cm (2 inches) of clearance above and below the device in order to prevent interference with the air circulation.

- ⚡ Before beginning installation or maintenance work, switch off the system's main switch and ensure that the system cannot be switched on again. During maintenance work, provide a suitable disconnection device to disconnect the unit from the electrical supply circuit.
Use a screwdriver with a blade 3 mm (approximately 0.12 inches) wide. You do not need any wire end ferrules for the terminals. You can use lines up to thickness of 1 x 2.5 mm² or 2 x 1.5 mm².

5.3.2 Method of Operation

You need at least one LPI-10 for each network segment in order to supply the Lock-Nodes.

The LPI-10 (new construction) has 3 terminals for connection to the supply voltage:

Terminals:

INPUT AC 230V:

- L1: 230V~ connection
- N: 230V~ connection
- PE: Potential compensation connection

OUTPUT BUS:

- NET+: Network cable connection
- NET-: Network cable connection

BRIDGE 1 + 2:

- For a network with no topological structure or with a star-shaped structure, bridge the "Bridge 1-2" connection
- You are not permitted to bridge this connection if you are using a bus topology.



5.3.3 Assembly Instructions

The LPI-10 is intended for installation in distribution boxes with DIN rails. Clamp the voltage supplied from outside to the terminals marked for that purpose. Depending on the structural situation and number of groups, you can also put several power supplies and routers in one distribution box.

Connect the outside 230V~ plug-in power supply to these terminals. This is printed on the connecting terminals. Ground the LPI-10 on the terminal labeled PE.



Connect the network cable (twisted pair) here. For BUS wiring, the connection between "Bridge 1-2" stays open, but for other wiring you must insert a bridge here. You can also lay a network cable to the router (if there is one). Connect the cable to connecting terminals 17 and 18 there. An additional network cable goes from the router to the LockNodes.

Build the LPI-10 into the separate segments in such a way that there is voltage of at least 35V DC at each LockNode.

Consequently, the installation location depends on the number and particular distribution of the LockNodes in the corresponding segment.

If it is not possible to guarantee voltage of 35 VDC at each LockNode with one LPI-10, you must install a repeater (including power supply) and an additional LPI-10 (including power supply) in the segment.

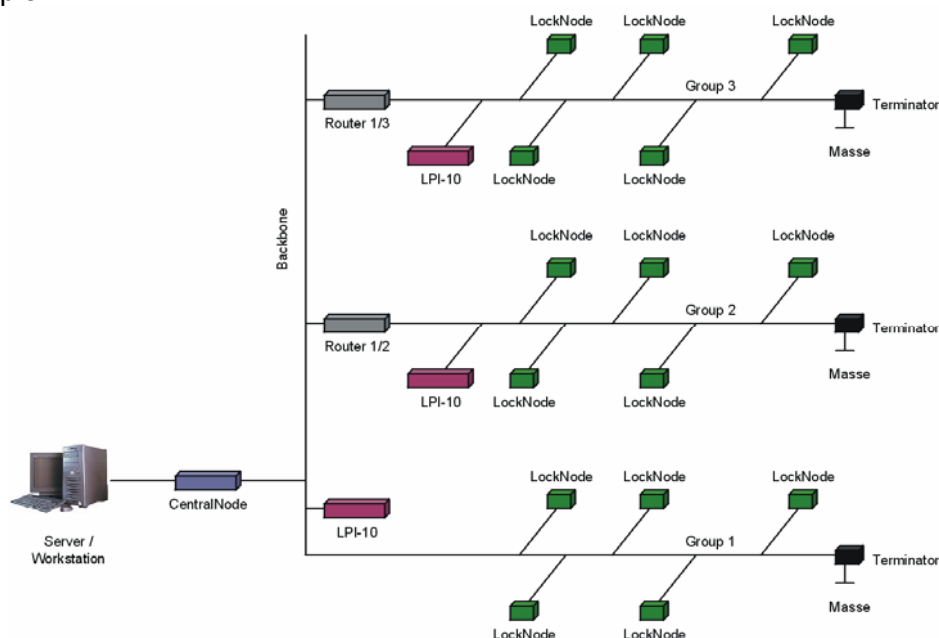
The LPI-10, as it comes from the factory, does not have any over voltage protection. For this reason, this protection should be already provided for by the customer.

6.0 Router

6.1 Method of Operation

Routers are needed in order to separate individual segments, such as floors or buildings, from one another in large networks. From the entire data stream that arrives at one side, they are able to filter out the data that is intended for the segment lying behind them (data segmentation). Because the routers receive a Group ID, they must be configured by SimonsVoss.

Example:



One segment can have a maximum of 62 LockNodes. As soon as this number is exceeded, you must open a new segment with a router and an additional LPI-10 module + plug-in power supply. A network can have a maximum of 63 segments. In large networks, you should choose the segments to fit the structural conditions, for example, one segment per building or floor.

- 👉 Routers need a 230 V AC power supply from the customer (outlet).
- 👉 Routers, as they come from the factory, do not have any over voltage protection. For this reason, this protection should be already provided for by the customer.
- 👉 If elevators are to be integrated into the networking, they are not permitted to be installed in the backbone. Instead, they must be separated from the backbone by a router.

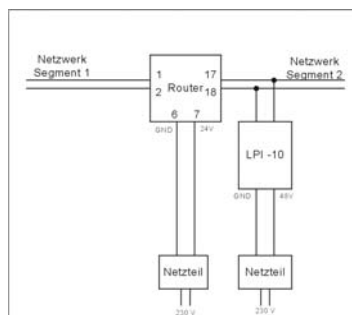
6.2 Assembly Instructions

You can attach routers to a DIN rail. Please refer to the following figure for the connection assignments:

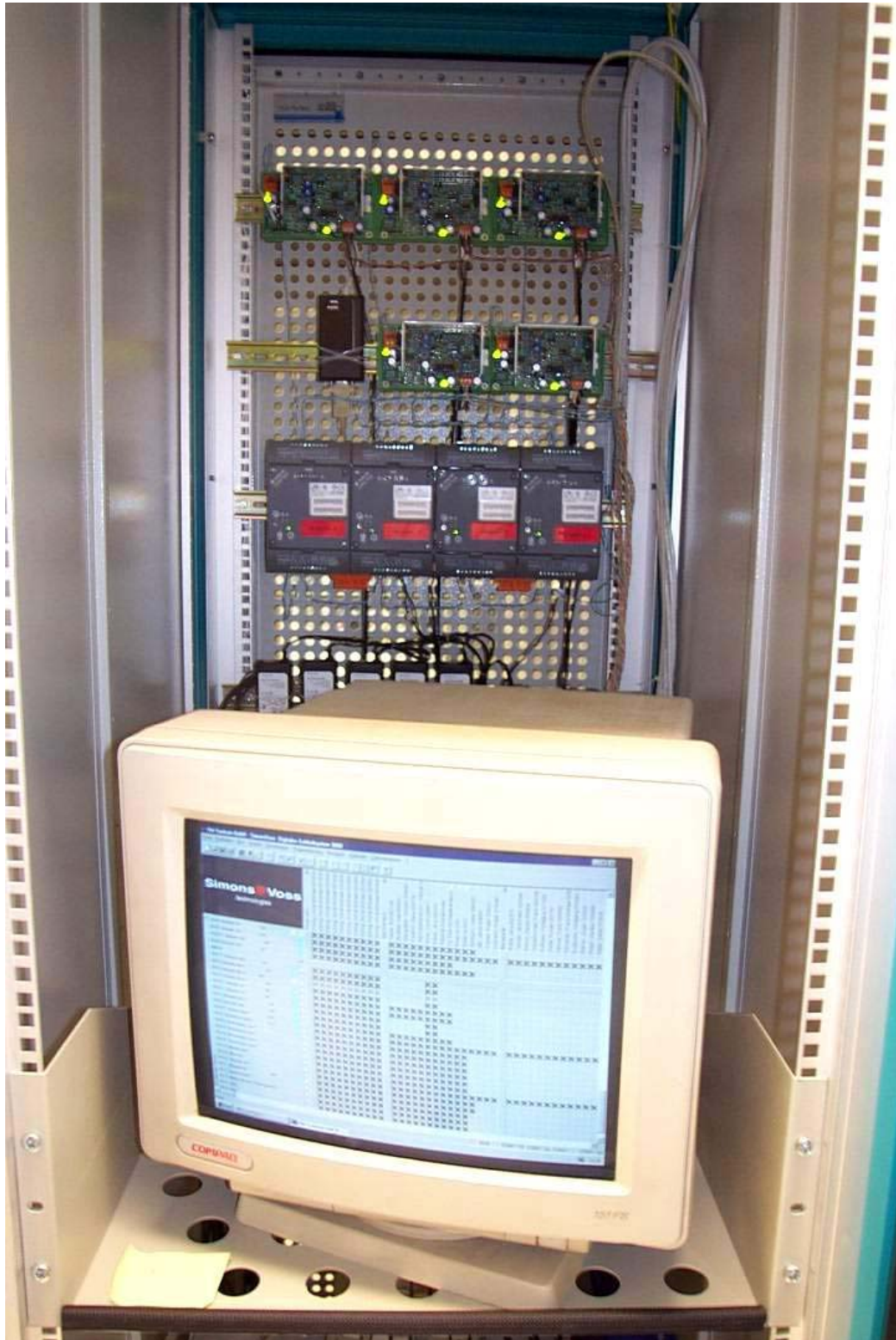


- 1+2 Input A of network
- 3+4 Additional input A (internal bridges from 1-3 and from 2-4)
- 5 Not used
- 6+7 Supply voltage: power supply connection
- 8+9 Additional supply voltage (internal bridges from 6-8 and from 7-9)
- 10-14 Not used
- 15+16 Output B of network
- 17+18 Additional output B (internal bridges from 15-17 and from 16-18)
This output can be used for connecting the LPI-10, for example.

- 👉 Connect the inputs of all routers in parallel. It is very important that you do not confuse input A and output B with one another.



6.3 Installation Example



7.0 Repeater

7.1 Method of Operation

The repeater increases the allowable communication distance by regenerating the signals. Unlike routers, the repeater does not have a group ID, so it does not have to be configured by SimonsVoss.



7.2 Assembly Instructions

Install it in a small housing that is suitable for DIN rail assembly. Connect the (LON) network lines to terminal screws on both sides. The power supply – which can be either AC or DC – is on one side of the housing. Feed the cable screen through to the opposite side.

The repeater always needs a separate power supply, which is not included in the delivery!!!

Repeaters, as they come from the factory, do not have any over voltage protection. For this reason, this protection should be already provided for by the customer.

8.0 Terminators



To avoid disturbances, you must use a so-called terminator (pull-up resistor) in the bus system as the segment termination. Connect this pull-up resistor to terminals 1 and 2 of the last LockNode and also to the network equipotential bonding.

9.0 Network Cable

9.1 General Information

Every LockNode is networked with one line consisting of two twisted wires (twisted pair). The data and the supply voltage are both transmitted over this line (see Fig. on page N2 or N3). An LPI-10 or LPI-10 Compact module feeds the twisted pair line with voltage (approximately 48 V DC).

9.2 Cable Laying

There are almost no restrictions placed on the cable laying when the given cable types are used. As a matter of principle, however, placement parallel to cables with strongly pulsating high voltage should be avoided. If, however, due to structural reasons, it is possible to use only cable that has already been laid but which either does not meet the required demands or which meets them only partially, the result can be interference due to radiation from other cables or systems. This interference can affect the performance capability of the network or can even lead to a complete network blackout. Therefore, it is important in these cases to pay special attention to cables or external systems that are in the vicinity of the transmission cable. This means high power machine systems, elevators, microwave systems, or transmission systems, for example.

👉 Connect the shields of all network cables to one another. Normally, these are connected to the potential compensation on the LPI-10.

9.3 Cable Types

The type cable that you use depends on the following factors:

1. Total cable length (from the CentralNode to the last LockNode)
2. Cable length between the LockNodes
3. Network topology: wiring plan (star or bus system)

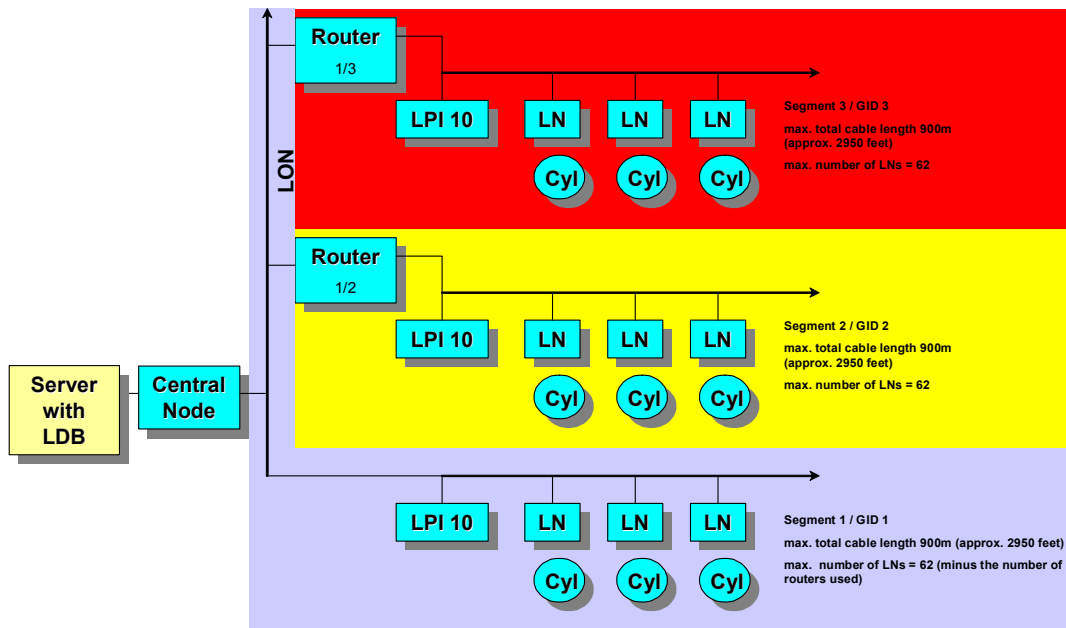
	With no topology	With no topology	Bus topology with terminators
	<i>Total length</i>	<i>Distance between nodes</i>	<i>Total length</i>
JY (ST) Y 2x2x0.8	500 m	320 m	900 m
Category 5	450 m	250 m	900 m

LON – Network 3065

Page 22

9.4 Bus-Shaped Cabling (Example)

Simons  Voss
technologies

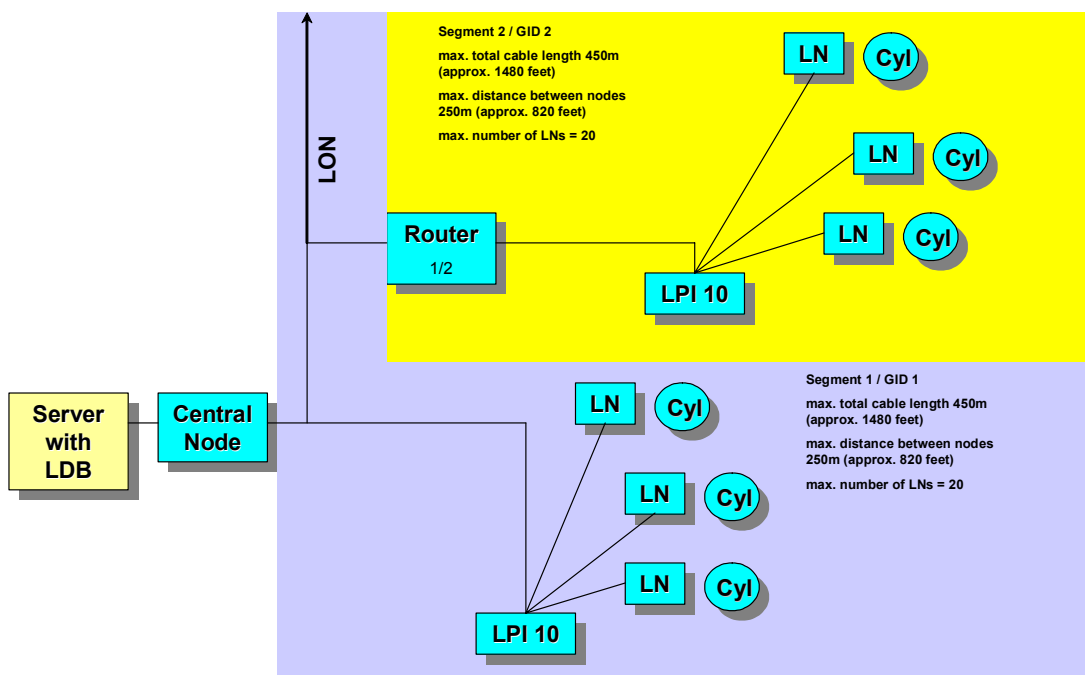


Bus System Cabling (Values for Cat5 Cable)

2

9.5 Star-Shaped Cabling (Example)

Simons  Voss
technologies

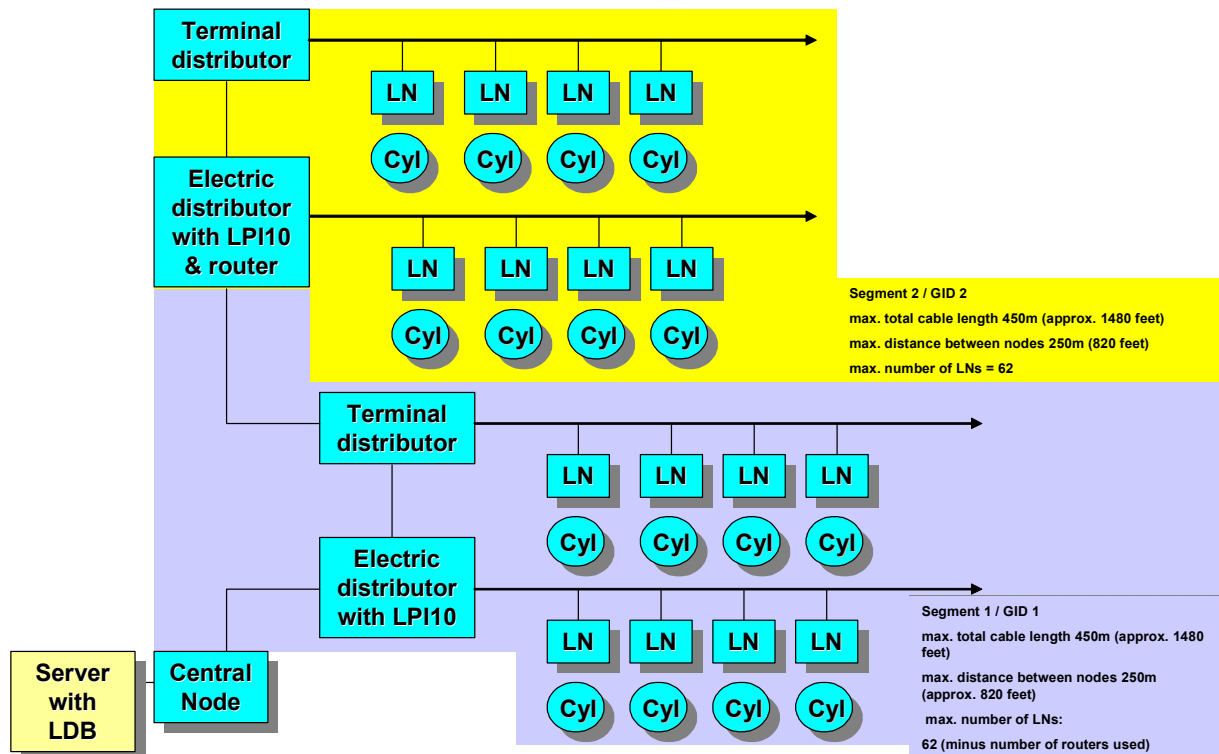


Star-Shaped Cabling (Values for Cat5 Cable)

1

9.6 Cabling With no Topology (Example)

Simons  Voss
technologies

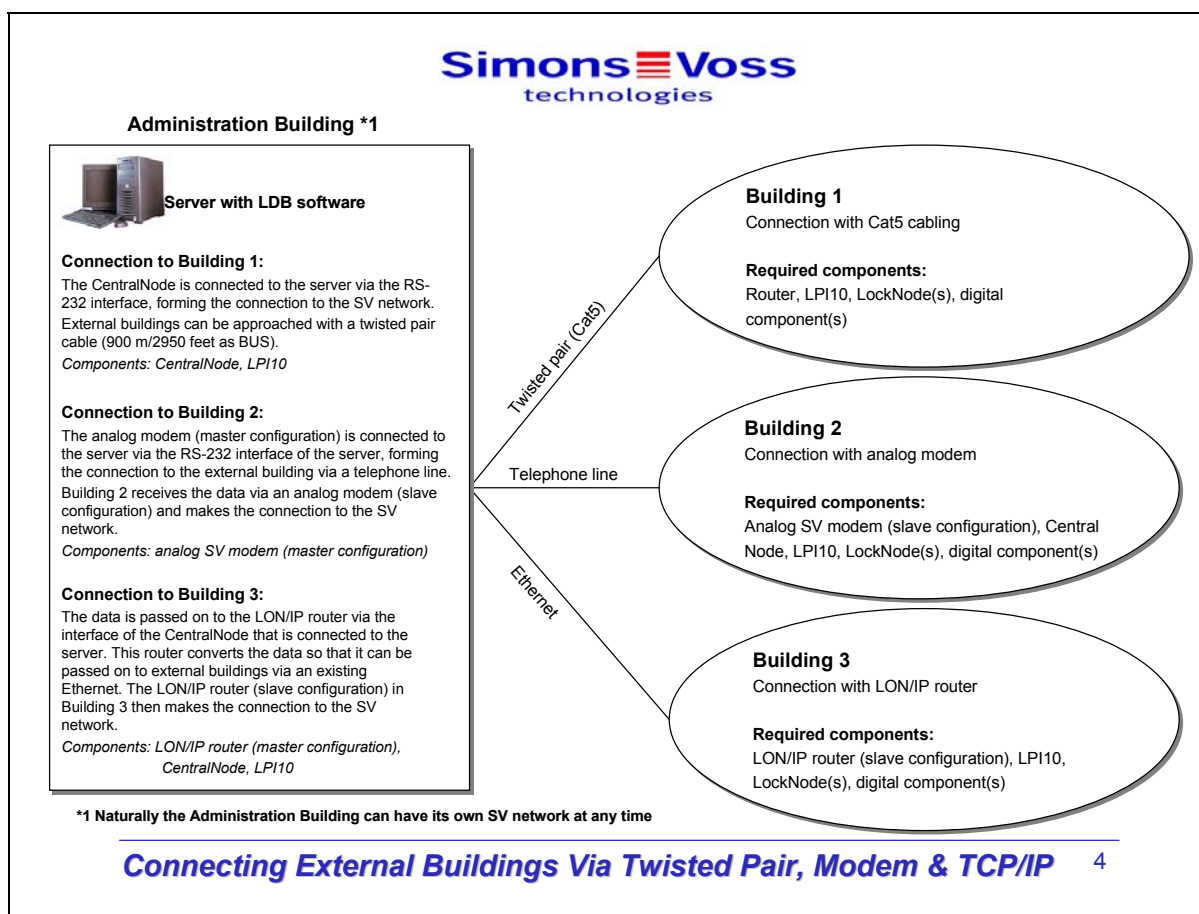


Cabling With no Topology (Values for Cat5 Cable)

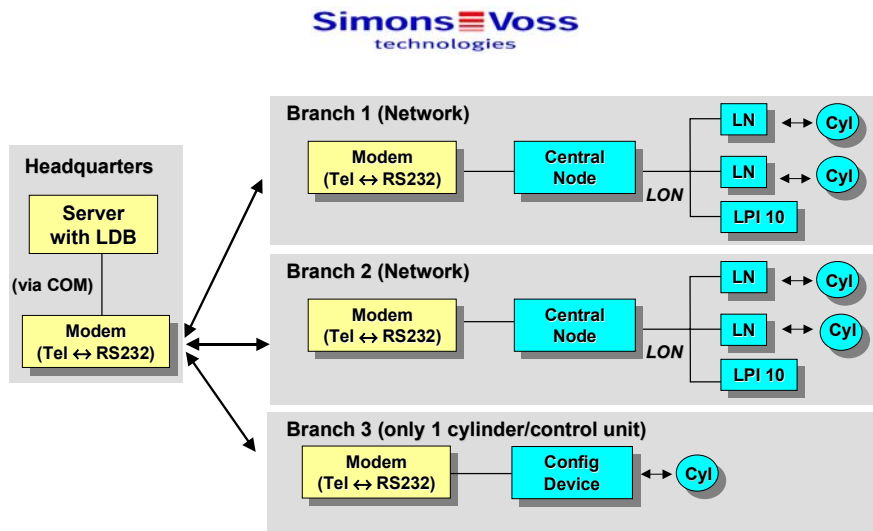
10.0 Planning Examples

10.1 Connecting External Buildings via Twisted Pair, Modem & TCP/IP

Remark: The planning and implementation of the following planning examples must be carried out by SimonsVoss. This chapter therefore offers only a short description of networking via modem and TCP/IP router.



10.2 Network via Modem

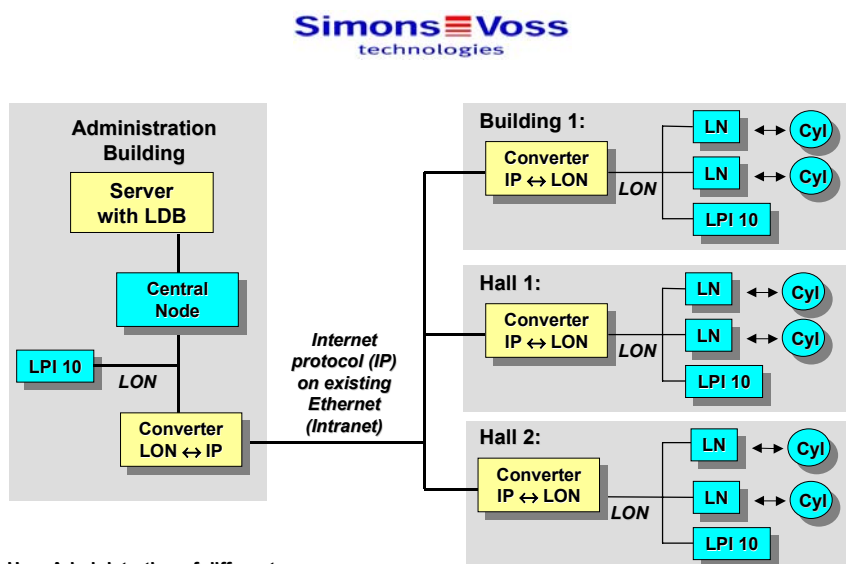


Use: Administration of many branch offices in different locations via one server/PC (via normal telephone network)

Network via Modem

5

10.3 Network via Ethernet



Use: Administration of different buildings/halls (in one location) via existing Ethernet (Intranet)

Network via Ethernet (IP-LON router)

7

11.0 Security

Because the Network 3065 records and logs critical data, it must be reliably protected from unauthorised accesses. This demands a great deal from the system as far as information and manipulation security.

11.1 Secure Communication Between the Network Nodes

Network communication is protected against data tapping in the following ways:

- In order to prevent the data stream from being monitored, the data is encoded for transmission.
- The encoding also provides sufficient protection during professional attacks using cryptoanalysis.

11.2 Automatic Tests of Separate System Components

Because separate components can be distributed widely across parts of a building, a malfunction, manipulation and forcing of a door must be detected and reported to the central PC automatically.

Important: If a door is equipped with a forced opening alarm function, it must have a lockcontact.

All nodes report to the central PC at time intervals that can be configured. These time frames can also be selected to be variable for certain time frames, so that, for example, critical doors report more often at night than during the day.

11.3 Alarms

Alarms are messages that require a prompt response (such as in case of a burglar or fire). If the same alarm occurs repeatedly, it is only reported once, in order to keep a better overview and to reduce the load on the alarm control centers.

12.0 Answers to the Most Common Questions Regarding the Network

- *Is it possible to use a cable that is already there for a twisted pair?*

Yes, you can use a cable that is already there, as long as it holds two strands that are not in use yet. However, the maximum range that can be attained with this cable is considerably less than that reached with special Twisted-Pair cables, depending on the nature of the cable.

- *How long can a line be with a twisted pair?*

Under optimum conditions, the maximum distance that can be attained is approximately 900 m (roughly 2953 feet). By using routers and repeaters, however, this distance can be extended to practically any length.

- *Are there restrictions on the line topology?*

In principle, the network is designed for mixed topology, which means that star and series interfacing can be mixed in any combination and adapted to the local conditions. In practice, there are restrictions regarding range and reaction time, depending on the set-up used and the line lengths. Therefore, if structured cabling is possible, especially in new buildings, it is better to pick a topology, usually BUS cabling.

- *After what line length should I use a router or repeater?*

The number and position of routers/repeaters used depends greatly on the structure of the planned network. If different buildings are networked together, however, a router should always be provided.

- *What is a router?*

A router is needed in order to separate individual segments (such as floors or buildings) from one another in large networks. From the entire data stream that arrives at one side, it can filter out the data that is intended for the segment lying behind it (data segmentation). Routers must be configured by SimonsVoss before they are installed. Routers require a 230 V~ connection (outlet) via a separate plug-in power supply for their own supply voltage.

- *What is an LPI-10?*

The LPI-10 is the power supply for the Twisted-Pair LockNodes. It consists of an interface module and the power supply. The interface module prevents attenuation of the data packets by the power supply and a defect of the supply voltage when there is a short circuit on the network. The required input voltage of 48 V direct current is supplied either by a plug-in power supply that can feed a maximum of 40 LockNodes, or a larger plug-in power supply that is designed for a maximum of 62 LockNodes.

- *What is an LPI-10 Compact?*

An LPI-10 Compact essentially corresponds to the LPI-10, but with the difference that the LPI-10 Compact is always designed for 62 LockNodes and does not need a separate plug-in power supply. It is connected directly to the 230V~ at the customer.

- *How many LPI-10 or LPI-10 Compact modules are needed?*

At least one LPI-10 or LPI-10 Compact must be used for each segment (divided by routers). The number depends on the particular segment structure. In principle, however, it can be said that each LockNode in the segment must be supplied with at least 35 V DC in order to guarantee perfect operation.

- *Where should the LPI-10 or LPI-10 Compact be placed in the segment?*

At least one LPI-10 or LPI-10 Compact must be used for each segment (divided by routers). The position of the LPI-10 or LPI-10 Compact depends on the particular segment structure. In principle, however, it can be said that placement in the middle of the segment is the most sensible.

If you have other questions, please contact your trade partner or the manufacturer.

13.0 Data sheet

CentralNode	Dimensions Network connecting cable RS232 connecting cable	100 x 54 x 30 mm [L/W/H] 200 cm (approx. 6.6 feet) 300 cm (approx. 9.9 feet)	
LockNode	Dimensions Input Output:	53 x 40 x 20 mm [L/W/H] Input voltage range Maximum switching voltage Maximum switching current Intrinsic resistance (AN)	5–24 V 24 V 300mA 1.5Ω
Router	Dimensions Input voltage	120 x 100 x 40 mm [L/W/H] 24 V DC	
Router plug-in power supply	Dimensions Output voltage	90 x 56 x 81 mm [L/W/H] 24 V DC	
LPI-10 (Version: open printed circuit board with external plug-in power supply)			
	Dimensions Input voltage Output voltage	135 x 80 x 60 mm [L/W/H] 48 V DC approx. 41-42 V DC	
Plug-in power supply 40	Dimensions Input voltage Output voltage	60 mm x 80 mm [W/H] 230 V AC 48 V DC	
Plug-in power supply 64	Dimensions Input voltage Output voltage	107 x 45 x 25 mm [L/W/H] 230 V AC 48 V DC	

LPI-10 (Version: Compact)

Input quantities

Nominal input voltage U_E	AC 120 / 230V
Input voltage range	AC 85 to 264V
Nominal frequency range	50/60Hz, 47 to 63Hz
Power failure buffering	> 50 ms at $U_E=195V$
Nominal input current I_E	0.8 / 0.5A
Making current impulse	$\leq 30mA$
Efficiency η	$\geq 75\%$ in operation at nominal value at 230 V AC
Recommended circuit breaker (IEC898) in the power supply lead	from 6A Char. D from 10A Char. C from 16A Char. B

Output quantities

Nominal output voltage U_A	DC 41.5 V $\pm 2\%$
Residual ripple	$< 100mV_{ss}$ at $10kHz < f < 200kHz$
Spikes (switching peaks)	$< 200mV_{ss}$ at $200kHz < f < 1MHz$
Nominal output current I_A	1A at U_E 85 to 195V 1.3A (1.5A max. permitted continuous current from U_E 195V)
Overload protection typically at	1.6A; continuous short-circuit-proof with pulsating restart attempt
Overvoltage protection typically at	54 V
Start and restart time	$5s < t < 10s$

Environmental Conditions

During transport/storage	$-40^\circ C$ to $+70^\circ C$ ($-40^\circ F$ to $+158^\circ F$)
During operation	$0^\circ C$ to $+40^\circ C$ ($32^\circ F$ to $+104^\circ F$)
Rel. air humidity	5 to 95%, w/o moisture condensation

Security

Degree of protection to EN 60529	IP20
----------------------------------	------

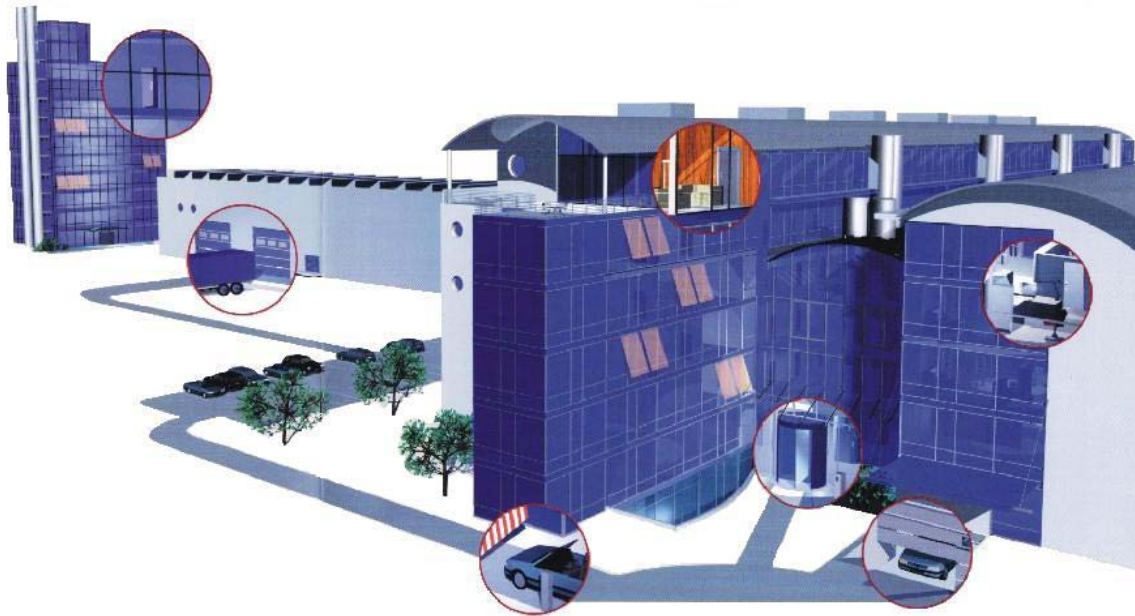
Protection class to VDE 0106 Part 1	I (with ground terminal)
Electrical isolation, primary/secondary	SELV to EN 60950
Electromagnetic compatibility	
Emitted interference (EN 500081-1)	Class B to EN 60950
Noise immunity (EN 50082-2)	EN 61000-4-2/3/4/5/6, level 3
Weight	
Weight	Approx. 0.5 kg
Approvals	
Approvals	CE (98/336 EEC, 73/23 EEC)

WaveNet Radio Network 3065

Version: September 2006

WaveNet Radio Network 3065

Page 2



1.0	Introduction	3
2.0	Transmission media	4
3.0	Usable radio wavelengths	4
4.0	What are the factors to look out for?	6
5.0	Secure message transmission	7
6.0	WaveNet System 3065 Network components	7
7.0	Network structure	15
8.0	Security	18
9.0	Battery warning	19
10.0	Installing WaveNet Lock Nodes	20
11.0	Technical specifications	21

© Copyright SimonsVoss Technologies AG

All rights reserved

This work contains information supplied by SimonsVoss AG, and all such information is supplied without liability for errors or omissions. No part may be reproduced or used except with the express written permission of SimonsVoss AG. The copyright and the aforementioned restriction on reproduction and use extend to all media in which the information may be used.

1.0 Introduction

In the following, the components of the System 3060 (locking cylinders, Smart Relays, block locks) are always referred to as locks or doors. However, unless stated otherwise, the descriptions also apply to all the other components of the System 3060.

For customers with only a few doors and a building which is not too large, the best way to programme the System 3060 is with a laptop and a ConfigDevice (SmartCD or PalmCD), since the configuration of the locks seldom needs to be changed.

With medium-sized and large properties in which lost keys, new transponder allocations and organisational changes are more frequent, it makes sense to manage and maintain the locking system by means of a network. Not all the doors need to be networked, however. The system can also be configured for mixed operation (networking/standalone).

In a networked system, all of the maintenance and programming functions can be conducted from a central computer, where it is also possible to obtain an overview of the current status of the entire network. For example, locks and door statuses can be requested centrally – such as door open, door closed, door locked, battery warning, access list, break-in alarm. This enables you to respond to events directly from the central control room.

WaveNet is an easily installable 'Plug-and-Play' network for use in building automation. Because it is wireless, it is especially suitable for the online management and control of the SimonsVoss 3060 digital locking and organisation system. It can be used in existing buildings, but also in new buildings (for flexible-use zones, for example).

The transmission of data within a WaveNet network is largely independent of the transmission medium. For instance, data can be transmitted via RS232 interfaces, RS485 ports, TCP/IP, or by radio (868 MHz).

To summarise, networking enables the entire access control system to be configured and monitored from one central computer. This enables the user to respond immediately to critical situations.

2.0 Transmission media

WaveNet supports the following media for the transmission of data inside the system:

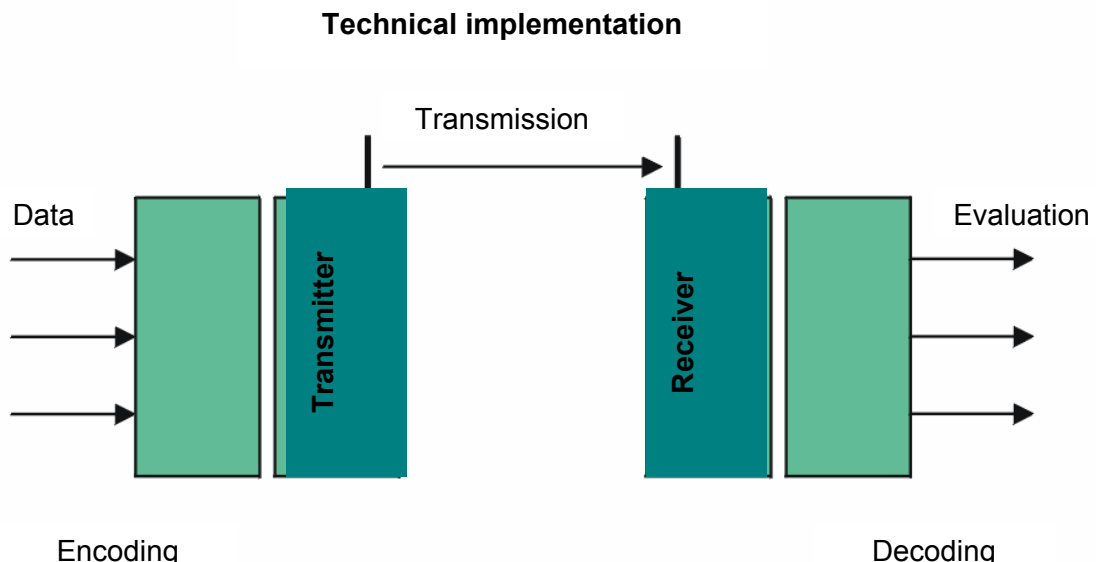
- Internet and Intranet via TCP/IP for transmitting data between different computers within a network.
- RS232, for data transmission between a computer and the WaveNet Central Node (cable length maximum 15 m).
- RS485 bus wiring for connecting individual WaveNet Routers functioning as network backbones (cable type KAT5, shielded, cable length maximum 900 m).
- 868 MHz radio (radio range approx. 20 to 30 m depending on building structure).
- B-field 25 kHz (radio range approx. 30 cm), for transmitting data between the WaveNet Lock Node and a SimonsVoss lock (e.g. locking cylinders, Smart Relays, and so on).

3.0 Usable radio wavelengths

Nowadays, what is referred to as modern radio technology for security engineering should not be confused with the radio systems common in the automotive industry and soon to be widespread in household communications. Radio transmission in access control systems must satisfy the necessary security standards.

In the year 2000, a special SRD (short range device) band in the 868 MHz range was made available for this type of application. The advantage of this new SRD band is that a clear set of regulations governing utilisation periods per time unit has been defined for the sub-bands. This means that a radio device (e.g. Router Node) which utilises a frequency channel in the 868 MHz bandwidth is only permitted to transmit for 36 seconds in every hour. This limitation is defined in what is known as the 'duty cycle conditions'.

This excludes permanent transmitters from the outset – and with them sources of interference in secure radio transmission such as wireless headsets and amateur radio enthusiasts. There are also wavelengths that are exclusively reserved for security applications. With its basic information and specifications relating to system technology such as size of components, minimum range, battery lifespan and so on, the 868 MHz band represents a sufficiently secure transmission method for use in WaveNet.



4.0 What are the factors to look out for?

Regardless of the method, radio transmission is subject to a range of outside factors which can impede it or interfere with it. Equipment characteristics can also influence the range.

Upon what is the range dependent?

- Transmission output power
- Antennas
- Sensitivity of receiver
- Environment (air humidity, temperature)
- Position of installation
- Frequency
- Structural surroundings (walls, ceilings, etc.)

Transmission range can also be limited by obstacles. The following table provides some guidelines:

Material	Energy transmittance
Wood, plaster, plasterboard	90–100 %
Brick, particle board	65–95 %
Reinforced concrete (transmitter on metal)	10–70 %
Metal, metal mesh, aluminium cladding, underfloor heating	0–10 %

5.0 Secure message transmission

The transmission security of a message by radio in the WaveNet depends upon:

- Radio transmission security in the sense of data telegram management.
- Potential coincidental disturbances along the transmission route.
- Intentional interference such as manipulation or sabotage of the transmission route.
- Intelligent methods of avoiding interference and finding alternative routes.

The speed of data transmission and message transfer can be influenced by a range of factors, and these can also cause a certain proportion of the messages to be lost.

These factors can include:

- High data traffic levels within the WaveNet.
- External interference in the WaveNet radio bandwidth.
- Power failure in segments of the WaveNet of the Central Node.
- Transmission failure or transmission interference in an external network (e.g. LAN).

6.0 WaveNet System 3065 Network components

WaveNet network components all have two independent ports. This enables two different network segments to be connected together through a WaveNet network component.

Definition: network segments are characterised on the one hand by a particular transmission medium (e.g. RS485 cable, RS232 cable, radio) and on the other hand by a separate segment address (GID = GroupID).

The following SimonsVoss WaveNet network components are available:

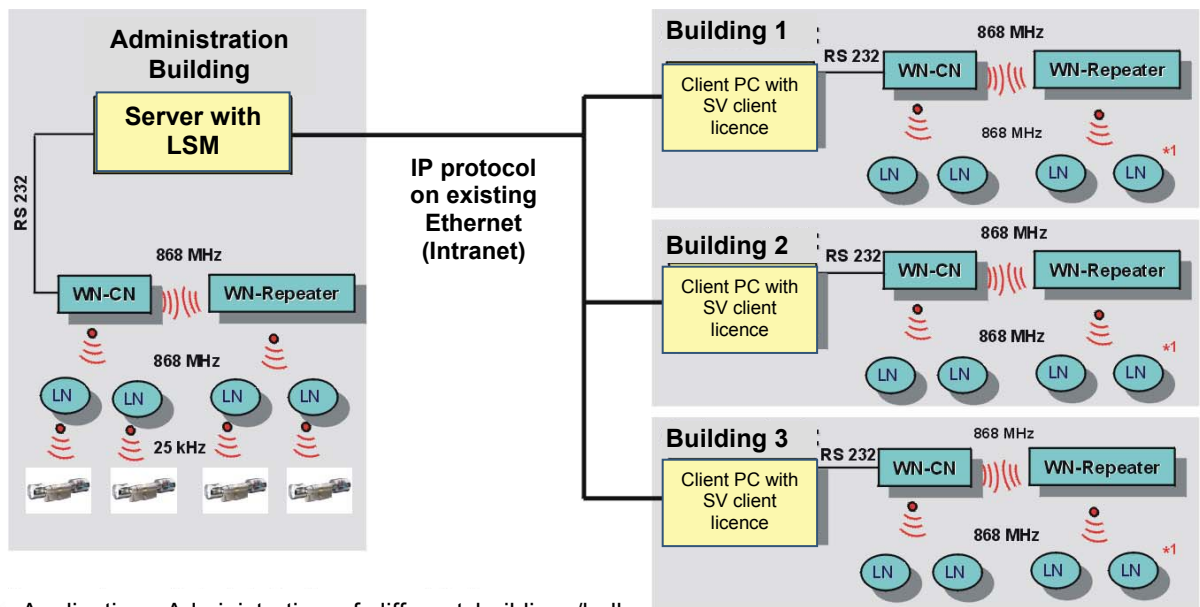
WaveNet Radio Network 3065

Page 8

6.1 Computers

Using special communication node software (CommNode), computers can be integrated into WaveNet:

- between the user interface and RS232 port, and
- between the user interface and TCP/IP (Internet, Intranet), and
- between TCP/IP and the RS232 port.



Application: Administration of different buildings/halls (at one location) via existing Ethernet (Intranet)

***1 = LN communicates with the allocated lock via 25 kHz (see Administration Building)**

6.2 Router Nodes (general)

WaveNet Router Nodes are basically used to connect two different network segments together; these two may use the same transmission medium (e.g. RS485/RS485), or different transmission media (e.g. RS485 cable / 868 MHz radio).

Furthermore, data streams arriving from the segments are filtered by the WaveNet Router Node so that the only data passed on to the segment downstream from the WaveNet Router Node is the data which is supposed to be processed by that

segment. The WaveNet Router Node blocks out all other data from the downstream segment.

WaveNet Router Nodes are currently capable of connecting the following transmission interfaces between the segments: RS485 KAT5 cable, RS232 cable, 868 MHz radio.

6.3 Router Nodes (special versions)

WaveNet Central Nodes are Router Nodes which enable the linking of:

- computers (RS232 port) and 868 MHz radio, and
- computers (RS232 port) and KAT5 wiring (RS485).

WaveNet Repeater Nodes are Router Nodes which link together two different segments that use the same transmission media, thus enabling the range to be extended. This means that if the radio transmission distance to the Lock Node achieved by the Router Node is too small, or if a cable within the network is going to exceed the maximum length, an extension can be created which complies with the system specifications using the WaveNet Repeater Node.

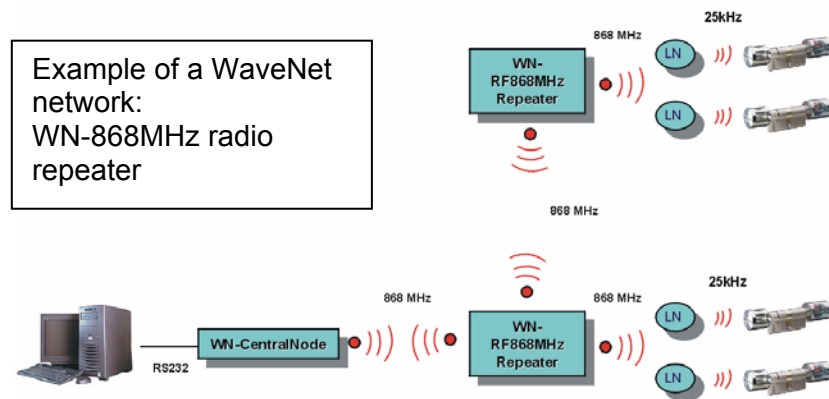
WaveNet Router Nodes as a converter from radio.... to cable....

WaveNet Radio Network 3065

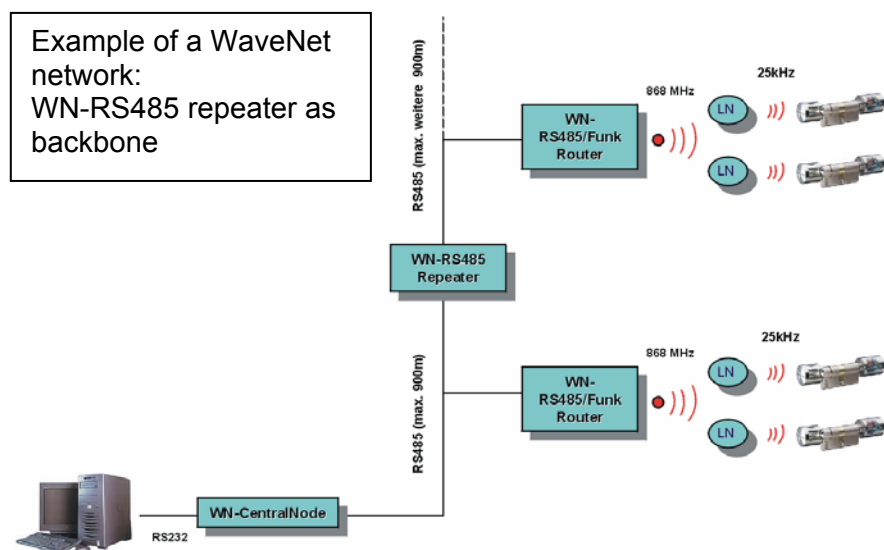
Page 10

WaveNet Repeater Nodes are used in situations such as the following:

- If the radio range to a Lock Node is further than the range of a WaveNet Router Node: the radio signal is sent by the WaveNet Router Node to the WaveNet Repeater Node and from there to the Lock Node (LN).

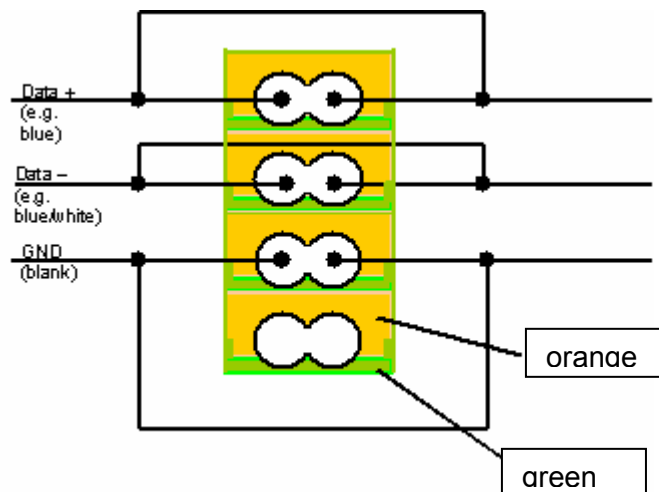


- To extend a network with an existing RS485 segment whose cable length is 900 m (KAT5) by a further segment of maximum 900 m.



Backbone wiring:

An RS485 segment (backbone) is wired using a bus comprising a shielded, standard KAT5 cable. The bus line consists of two data lines (Data+, Data-) and an earth line. This bus line is connected to every RS485 module associated with a WaveNet Router in the segment. The RS485 modules are connected to the bus line using a green and orange 8-pin plug as follows.



6.4 Lock Nodes

WaveNet Lock Nodes form the interface between WaveNet and the locks in the 3060 digital locking and organisation system (locking cylinders and Smart Relays, for example).

All of them have:

- A special B-field port through which they communicate with the SimonsVoss locks (locking cylinders, control units, furniture locks and so on);
- A radio port (868 MHz) for transmitting data to the WaveNet Nodes (WaveNet Router Nodes, WaveNet Repeater Nodes and WaveNet Central Nodes, for instance).

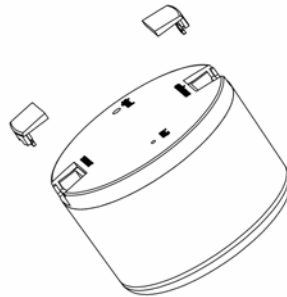
Inside the system, a WaveNet Lock Node can only be allocated to one digital lock (locking cylinder, Smart Relay or furniture lock, for instance). The distance between a WaveNet Lock Node and a digital lock may not exceed 30 cm.

WaveNet Lock Nodes are **always battery-powered** and can therefore be integrated into the SimonsVoss WaveNet without any wiring whatsoever. This means that the system is ideal for installation in an already existing building.

In order to make installation as easy as possible, the casing of the WaveNet Lock Node is designed to fit into a standard flush-type box (40 mm deep, 58 mm Ø) in accordance with **DIN 49073 Part 1** (for installation in a light switch strip, for example).

Note: Some ranges of switch have less space because of the way the cover is attached.

However, you should ensure that there is no excessive interference in or around the light switch strip – insufficiently suppressed ballasts and so on. In extreme cases you may have to fit an additional flush-type box further away in order to house the Lock Node.



Lock Node with casing

Lock Node inputs / output

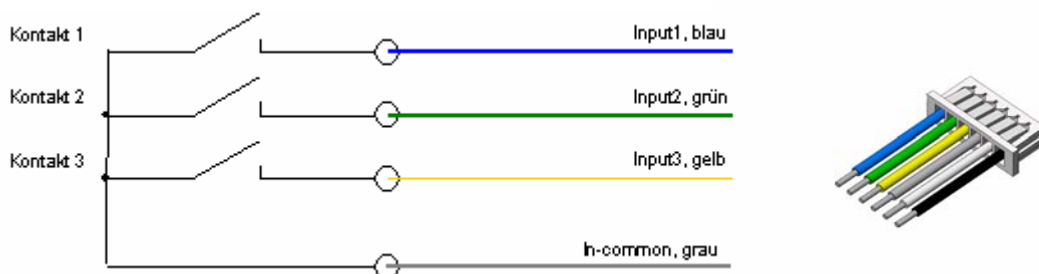
Every WaveNet Lock Node has one output and three inputs (for door monitoring, for example).

The three inputs enable up to three external floating contacts to be connected.

This enables the central monitoring of devices such as door and lock contacts as well as motion sensors, light barriers and so on – via the WaveNet network. The status of each connected contact can be polled by the central computer at any time, and changes to the contacts (events) can (if the Lock Node is configured accordingly) also be automatically registered by the central computer.

The output is used to send signals to external systems such as sensors, heaters, lights and so on. The output is an electronic switch (open drain) which can operate with up to 25 V and 650 mA.

A 6-pin colour-coded cable is available for the optional **connection of the I/Os**. The cable is plugged into the socket market 'sensor' on the Lock Node. For monitoring tasks, up to three floating contacts can be connected between the green In-Common

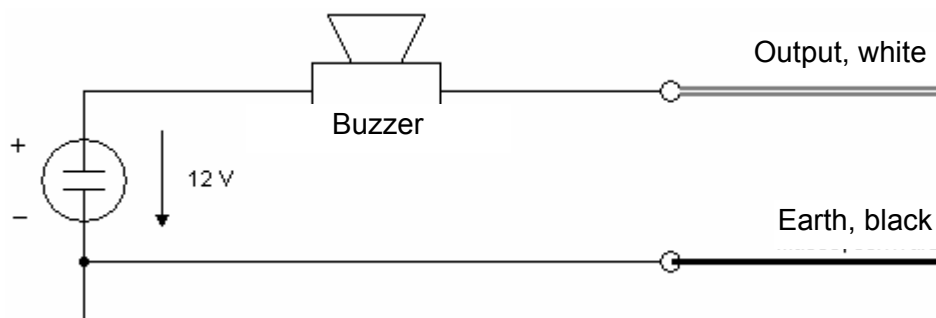


line and one of the coloured (blue, green, yellow) lines (see following diagram):

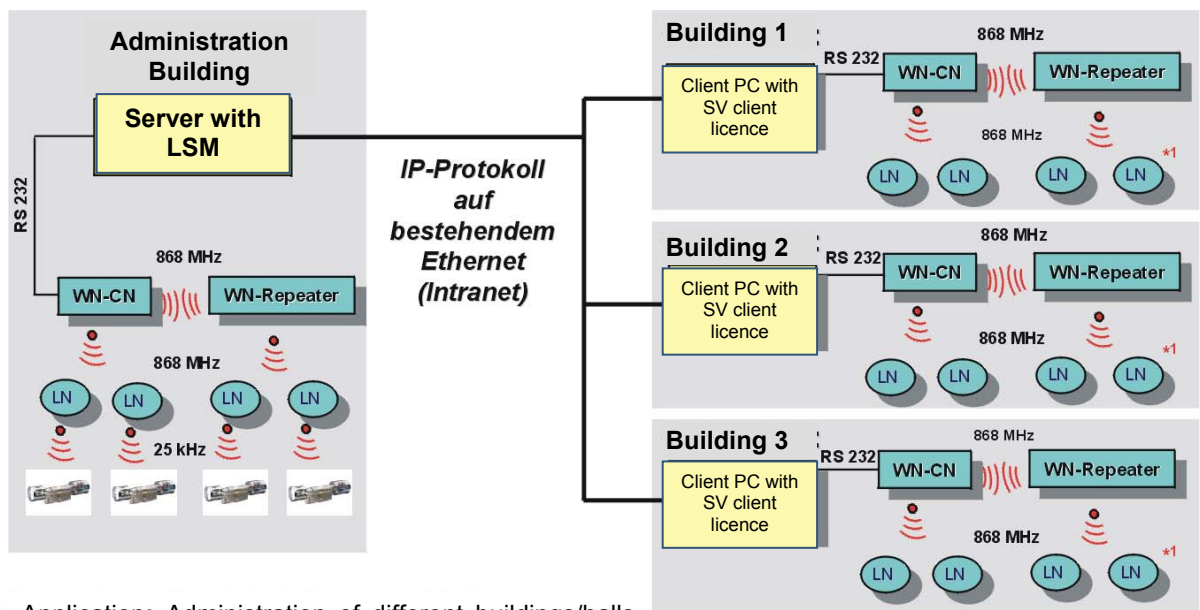
In the LDB and LSM user interfaces, an open contact has the value 0 while a closed contact has the value 1. In the diagram above, for instance, if contact 1 is used for monitoring a door, then when the door opens it will generate an event: 'input 1 transition from 1 to 0' (if contact 1 is closed when the door is closed and open when the door is open).

Internally, the output is formed by a transistor wired as an Open Collector. The white and black wires are available for connecting up external devices (such as buzzers). Note: out = white; earth = black.

Wiring example:



7.0 Network structure



- Application: Administration of different buildings/halls (at one location) via existing Ethernet (Intranet)

In the network structure depicted above, different users with different rights can access a common server using the SimonsVoss WaveNet communication node software (CommNode) and a GUI (Graphical User Interface) via the Internet/Intranet. This server acts as a communication node and is connected to the WaveNet Central Node via an RS232 cable.

In the example shown above, the WaveNet Central Node connected to the server communicates via radio (868 MHz) directly with a Lock Node, which in turn exchanges data with the digital component (locking cylinder), also by radio (25 kHz). In this example, all of the other Lock Nodes are outside the radio range of the WaveNet Central Node, and are therefore contacted indirectly via a WaveNet Repeater Node.

The structure above can be set up nicely using the multi-user and client-compatible database application known as the SimonsVoss LSM locking system management software. However, in the example above there is only one single CommNode, and thus only one single Central Node with a local subnetwork. In reality, almost any

number of CommNodes can be connected via the Intranet or Internet. This enables what is known as 'branch operation'; that means any number of branch offices with local Central Nodes and associated subnetworks can be linked to a central office via the Intranet/Internet.

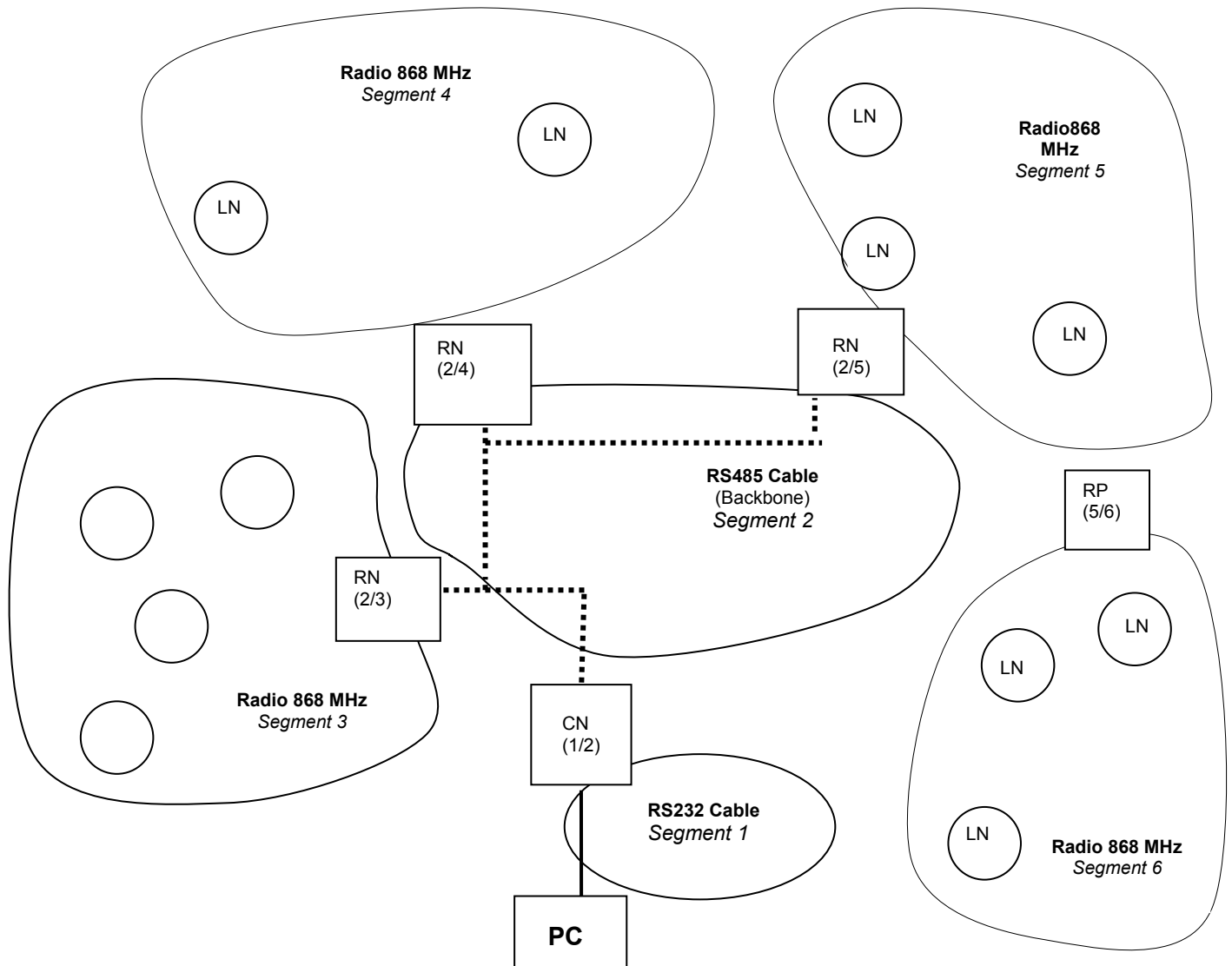
Much easier to install (and correspondingly easier to manage) is the file-based LDB locking system administration software from SimonsVoss, which, unlike LSM, does not allow a direct integration of the Intranet/Internet transmission medium. Instead, a central computer is connected directly to the Central Node of the WaveNet network. There are, however, some interesting solutions which also allow 'branch operation' using devices such as a modem or external software (PC Anywhere, for example). Networks are divided up into segments. A WaveNet Central Node can serve up to 253 segments, while each segment can have up to 253 WaveNet Lock Nodes / WaveNet Router Nodes.

Note: If you are using the LSM software, the network can be divided up between 1021/62 and 253/253 (segments / Lock Nodes per segment). When planning the system, this means you can decide whether each segment should have more segments or more Lock Nodes.

WaveNet Radio Network 3065

Page 17

Examples of a WaveNet network structure:



CN = WaveNet Central Node (RS232 / RS485)

RN = WaveNet Router Node (RS485 / radio 868 MHz)

RP = WaveNet Repeater Node (radio 868 MHz)

LN = WaveNet Lock Node

8.0 Security

Since WaveNet gathers and records critical data, it has to be reliably protected against unauthorised access. This places the highest demands on the system with regard to information and manipulation security.

8.1 Secure communication between the WaveNet network nodes

Network communication is protected against tapping and data-monitoring by means of elaborate cryptography.

8.2 Automatic testing of individual system components

Since individual components may be installed across large areas of a building, functional disturbances, manipulations and break-ins must be automatically detected and reported to the controlling computer.

Important: if a door is to be fitted with a break-in alarm function, then it must be equipped with at least one door contact which can recognise if the door is open or closed.

All of the nodes can report to the controlling computer at configurable intervals of time. These intervals may be variable during particular periods – if, for example, critical doors need to be monitored more frequently at night.

8.3 Alarms

Alarms are messages which require an immediate response (e.g. break-in, fire). If the same type of alarm is sent repeatedly, it is only reported once in order to retain a better overview and not to burden the central alarm office unnecessarily.

9.0 Battery warning

If the voltage of the battery used to supply the Lock Node drops below a certain level, this can cause communication problems between the Lock Node and its associated lock, and also between the Lock Node and a Router Node (WaveNet Repeater Node, WaveNet Router Node, WaveNet Central Node).

If this type of fault occurs, then the 'N' behind the lock concerned is shown in red (communication fault). If after repeated recording the red N does not disappear, then you should check whether the battery requires replacement.

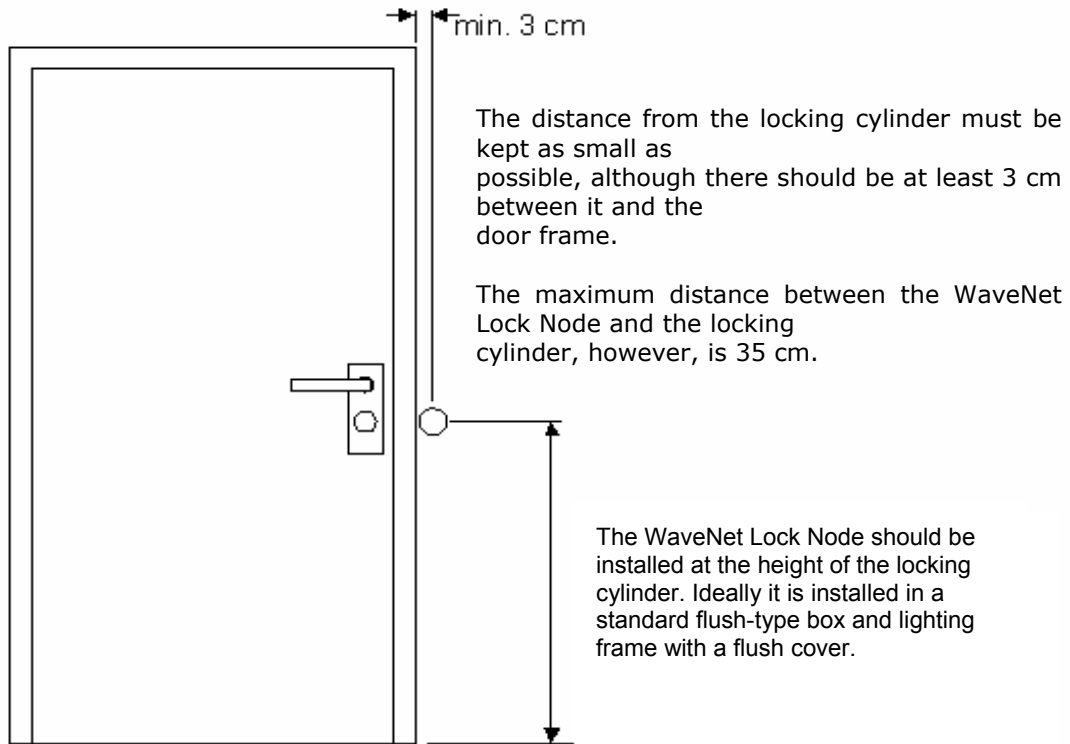
9.1. Changing the Lock Node batteries

To change the batteries of a Lock Node, remove the node from its place of installation (e.g. flush-type box) and remove the cover on the back.

The position of each battery is clearly marked in the battery compartment. You should only use batteries approved by SimonsVoss.

Please watch the LED when inserting the new battery. It should flash (2 times) briefly immediately after you have placed the first new battery into the empty battery compartment. The node is then ready for operation (power-up reset). If the LED does not light up, please take out the battery, short-circuit the battery contacts in the Lock Node, then replace the battery.

10.0 Installing WaveNet Lock Nodes



- The optimum radio signal range of RNs and LNs is generally achieved by fitting the Router Nodes so that their antennas point vertically upwards or downwards, and the Lock Nodes are fitted such that the lettering is horizontal, enabling you to read it normally.

11.0 Technical specifications

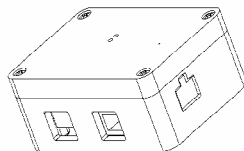
11.1 WaveNet power supply

Order number	WN.POWER.SUPPLY.PPP
Description	Externally regulated 230V AV / 6V DC plug-in power supply for WaveNet Central Nodes, WaveNet Repeaters & WaveNet Routers (PPP = Plug Power Pack).

11.2 WaveNet Central Node RS232 connection cable

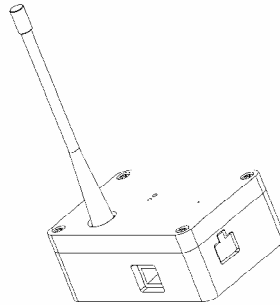
Order number	WN.CN.RS232.CABLE
Description	RS232 connection cable between computer and WaveNet Central Node
Length	2 m

11.3 WaveNet Central Node with integrated RS485 port



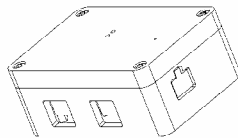
Order number	WN.CN.SC
Description	WaveNet Central Node for connecting to a computer/server. Central Node with integrated RS485 port for backbone.
Dimensions (L*W*H)	100 x 65 x 40 mm (applies to all Routers without antennas)
Voltage supply (for all Routers)	6 V ... 12 V DC
Power (for all Routers)	Min. 3 VA (250 mA at permanent load*) * - current peak if both ends are terminated on the backbone

11.4 WaveNet Central Node with 868 MHz radio module



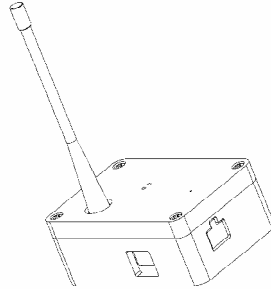
Order number	WN.CN.SR
Description	WaveNet Central Node with 868 MHz radio interface and external antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antennae)
Voltage supply	6 V ... 12 V DC
Power	Min. 3 VA (250 mA at permanent load)
For all routers with radio modules:	
Maximum transmission output	5 dBm (3.16 mW) to antenna socket
Sensitivity	-90 dBm at 19.2 kBaud
Frequency	868.2972 MHz
Current consumption in receive mode	12 mA at 3.3 V

11.5 WaveNet Router Node as RS 485 Repeater



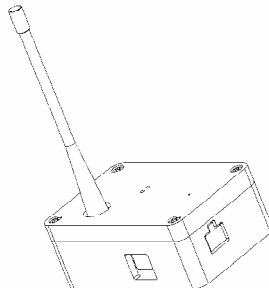
Order number	WN.RN.CC
Description	WaveNet Router Node as RS485 Repeater with two RS485 ports, including connection terminal for external plug-in power supply
Dimensions (L*W*H)	100 x 65 x 40 mm

11.6 WaveNet Router Node as 868 MHz Repeater



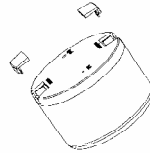
Order number	WN.RN.R
Description	WaveNet Router Node as Repeater with 868 MHz radio module. Includes connection terminals for external plug-in power supply and external send and receive antenna.
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)

11.7 WaveNet Router Node with RS 485 / 868 MHz Converter



Order number	WN.RN.CR
Description	WaveNet Router Node as a converter between 868 MHz and the RS485 port for using the Router Node as a backbone, including connection terminals for an external plug-in power supply and an external send and receive antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)

11.8 WaveNet Lock Node



Order number	WN.LN
Description	Battery-powered WaveNet Lock Node (node for networking computer with digital components) with 3 inputs and 1 output
Dimensions (H x Ø)	37 mm x 53 mm
Voltage supply	Two CR2/3AA batteries, lithium 3.6 V made by Sonnenschein, SL761
Current consumption	Radio transmission: 25 mA; Radio reception: 15 mA; Power consumption with no data traffic: approx. 40 µA Note: dependent on data traffic and HF interference density
Maximum transmission power	approx. 1 mW
Sensitivity	-95 dBm
Frequency	868.2972 MHz
Input (3x)	Floating (current pulse approx. 35 µA for 1ms every 0.5 sec)
Output (Open Drain)	Maximum switching voltage: 25 V DC Maximum switch-on current: 2 A Continuous current: 650 mA Internal resistance (AN): 0.5 Ω
Battery lifespan	approx. 3 years

WaveNet Radio Network 3065

Page 25

Order number	WN.LN.O.I/O
Description	WaveNet Lock Node with integrated battery, without inputs and output (node for PC networking of the digital components)
Dimensions (H x Ø)	37 mm x 53 mm
Voltage supply	2 Batterien CR2/3AA, Lithium 3,6 V Fa. Tadiran, SL761
Current consumption	Radio transmission: 25 mA; Radio reception: 15 mA; Power consumption with no data traffic: approx. 40 µA Note: dependent on data traffic and HF interference density
Maximum transmission power	ca. 1 mW
Sensitivity	-95 dBm
Frequency	868,2972 MHz
Battery lifespan	approx. 3 years

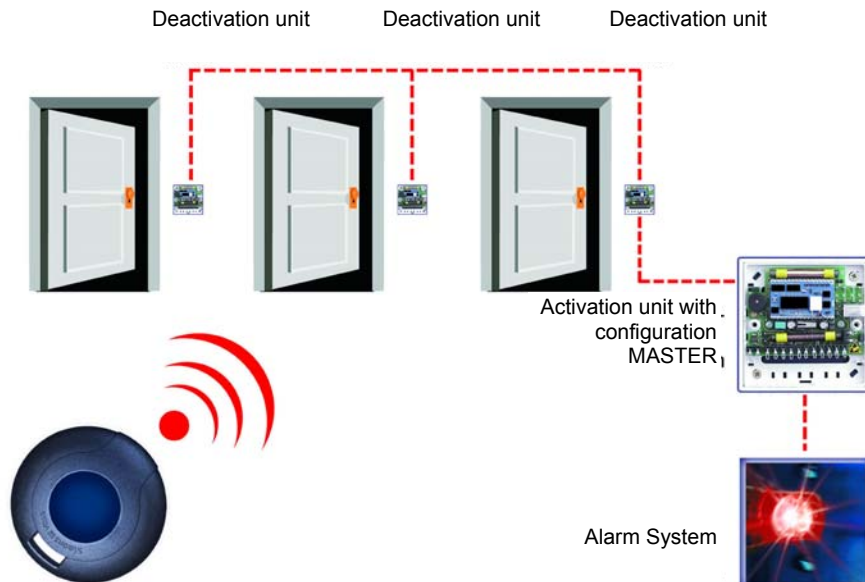
Shunt lock function 3066

Operator Instructions

Version: January 2004

VdS Shunt lock function 3066

Content



1.0	Shunt lock function 3066 System Components	3
2.0	Shunt lock function 3066 Operation	4
3.0	Special Versions of the Shunt lock function 3066	6
3.1	Operating the Activation Unit without a Deactivation Unit	6
3.2	Operating the Deactivation Unit without an Activation Unit	6
4.0	Data Sheet	7

1.0 Shunt lock function 3066 System Components

In objects protected by the alarm, measures must be taken to prevent any unintentional entry of the secured area when the alarm system is activated externally (burglar alarm system, BAS) because this would trigger a false alarm. The Shunt lock function 3066 implements such a feature without extensive work on the door or doorframe.

The following components are needed for this:

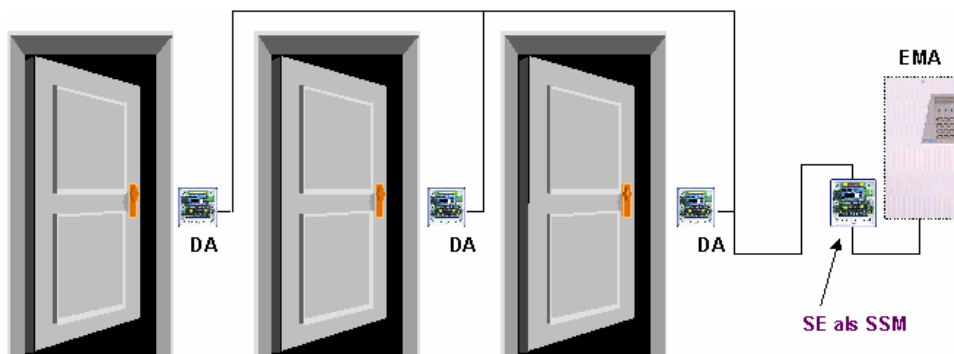
1. Activation unit(s) (MA and SA)

Such a unit is used to switch the alarm system. You need at least one activation unit (AU) to activate and deactivate the system externally. If you want to be able to activate/deactivate from several locations, you need the corresponding number of activation units. With a mouse click in the locking plan, you can issue the authorizations for activating and deactivating the alarm system.

Basically, there is a difference between the master activation unit (MA) and the slave activation units (SA). The SAs are needed only if you want to activate/deactivate from more than one location. It is always the MA that activates/deactivates the alarm system externally over a floating contact. SAs only send the appropriate requests to the MA. You can also activate internally by using SAs that are separately connected to the internal activation connection of the burglar alarm center (BAC).

2. Deactivation units (DA)

These are installed next to the doors of the secured area (and in the immediate vicinity of the digital cylinder). They make sure that even an authorized transponder cannot open these doors accidentally if the alarm system has been activated externally. This reliably prevents false alarms.



2.0 Shunt lock function 3066 Operation

Switching on the alarm system (burglar alarm system, BAS)

The person with switching authorization presses his or her transponder two times in quick succession (within 2 sec.) near an activation unit. This sends a signal to all deactivation units present. If lock contacts are connected to the deactivation units, the DAs first check whether the doors have been correctly locked. The digital locking cylinders or Smart Relays are not deactivated unless this is the case, so that it is no longer possible to enter the secured area. The activation unit does not receive a positive acknowledge until all lockings have been successfully deactivated. It then uses a floating contact to activate the alarm system externally (compelled signaling). The light emitting diodes on the activation units signal this by lighting for 2.5 seconds. The light emitting diode(s) of the deactivation unit(s) go out. The BAS acoustically shows that the activation has occurred - for example, on the activation unit.

Switching off the alarm system

The person with switching authorization again presses his or her transponder twice in quick succession within the transmitting range of the activation unit. The deactivation units signal this to the digital locking cylinders or digital Smart Relays. The BAS acoustically signals the successful deactivation. The LEDs on the activation units signal that the activation has occurred by blinking 1 x short-long. The LEDs on the deactivation unit(s) light again. (The LEDs on the deactivation units are used only for testing purposes, so they do not have to be brought out). Now it is possible to access the doors again with all authorized transponders.

- ☺ In network operation, (not VdS), you can do without deactivation units. In this case, the network nodes take care of activating and deactivating the locking.
- ☺ By simply clicking the transponder button within the transmitting range of activation units, you can determine the activation state of the alarm system if the LEDs on the activation units are brought out.

1 x short-long blinking means "deactivated"
1 x long (2.5 sec.) blinking means "activated"

Activation transponder

For emergencies, you can use the locking plan software to program a transponder that cancels the deactivation of the locking cylinder so that the doors can be opened with an authorized transponder. The alarm system, however, remains activated externally and the alarm will be triggered.

- Special model

If you want to keep a log of who switched the alarm system and when, you need an activation unit with access logging (PLUS version).

- PLUS activation unit

Design is similar to the standard version, but with access logging and time zone control.

Access logging The activation unit stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the programming device or over the network.

Time zone control You can program activation units in such a way that authorized transponders can switch the alarm system at certain times only.

Safety remarks

- Read through the operating manual carefully and thoroughly before putting the shunt lock components into operation. This manual contains important information on operation and programming.
- The components are built in accordance with the latest state of the technology. Use them only as instructed and only when they are in perfect technical condition and are properly installed according to the technical specifications.
- The manufacturer is not liable for damages that are caused by use that does not comply with the directions.
- Keep the documentation that comes with the product and system-specific notices in a safe place.
- Only trained experts are authorized to perform installation, programming and repair work.
- Soldering and connection work within the entire system must be performed only when the system is voltage-free.
- Soldering work must be performed with a temperature-controlled soldering iron that is metallically separated from the power system.
- Observe VDE safety regulations and regulations of the local electric utility.
- Do not use the components in areas subject to explosion hazards or in areas with fumes that dissolve metal or plastic.
- DIN norms and the guidelines of VDS Class C must be adhered to.

3.0 Special Versions of the Shunt lock function 3066

3.1 Operating the Activation Unit without a Deactivation Unit

If you want to activate and deactivate the burglar alarm system externally with the transponder instead of with a key, you only need a master activation unit (MA). In this case, however, you will lose the true purpose of the shunt lock function.

3.2 Operating the Deactivation Unit without an Activation Unit

If you continue to operate the alarm system with a standard key, you can do without the activation unit. In this case, the BAS controls the deactivation units.

VdS Shunt lock function 3066

Page 7

Data Sheet

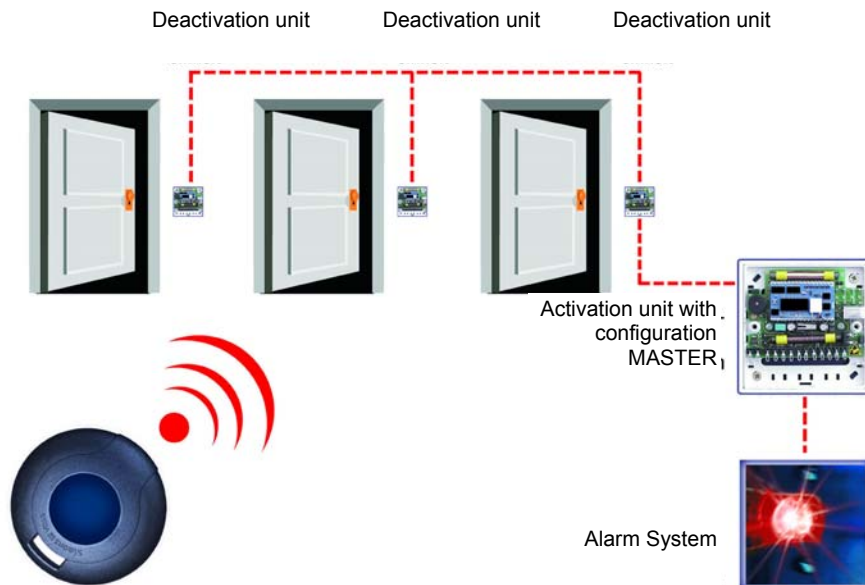
MA, SA and DA	Operating voltage Current consumption	8 to 16 Volts DC < 30 mA
Applied relay for switching output	Max. continuous current Max. switch on current Max. switching voltage Max. switching capacity	1 A 1 A 40 V AC 30 W / 60 VA
Tamper contact	Make contact	1 A / 30 V DC
Transponder range with extended antenna		1 – 3 cm
Temperature range	-10°C to +55°C (14°F to +131°F)	
Degree of protection	VdS environmental class II	
Housing	Material Color Dimensions [L/W/H]	S-B or A-B-S White 85 x 85 x 26 mm
	Article description	_____
	Article number	_____

VdS Shunt lock function 3066

Version: September 2006

VdS Shunt lock function 3066

Content



1.0	Functional Description	4
1.1	General Information	4
1.2	Safety Remarks	6
2.0	Assembly Instructions	7
2.1	General Information on Installing the Components	7
2.2	Installing the Deactivation Unit (DA)	8
2.2.1	Testing the Deactivation Unit (DA)	9
2.2.2	Connecting Power Supply, Lock Contact Evaluation and Sabotage Contacts:	9
2.2.3	Connecting Deactivation Request and eactivation Acknowledgement	10
2.3	Installing the Master Activation Unit (MA)	11
2.3.1	Testing the Master Activation Unit (MA)	12
2.3.2	Connecting Power Supply, Switch Contacts and abotage Contacts:	12
2.3.3	Connecting Deactivation Request, Deactivation Acknowledgement and Activation Request	13

VdS Shunt lock function 3066

Content

2.4	Installing the Slave Activation Unit (SA)	14
2.4.1	Testing the Slave Activation Unit (SA)	15
2.4.2	Connecting Power Supply, Sabotage Contacts and Local	15
	Activation Suppression:	15
2.4.3	Connecting Deactivation Acknowledgement and Activation Request	16
2.5	Wiring the Shunt Lock Components	16
2.6	Functional Principles	17
3.0	Programming	20
3.1	Programming the Activation Units (MA and SA)	20
3.2	Programming the Deactivation Units (DA)	22
4.0	Installation	24
4.1	Installing the Deactivation Unit	24
4.2	Installing the Activation Unit (MA and SA)	25
4.3	VdS-Compliant Installation of the Activation Unit (MA and SA)	26
5.0	Special Versions of the Shunt lock function 3066	28
5.1	Operating the Activation Unit Without a Deactivation Unit	28
5.2	Operating the Deactivation Unit without an Activation Unit	28
6.0	Data Sheet	29

1.0 Functional Description

1.1 General Information

In objects protected by the alarm, measures must be taken to prevent any unintentional entry of the secured area when the alarm system (burglar alarm system, BAS) is activated externally, because this would trigger a false alarm. The Shunt Lock function 3066 implements such a feature without requiring extensive work on the door or doorframe.

The following components are needed for this:

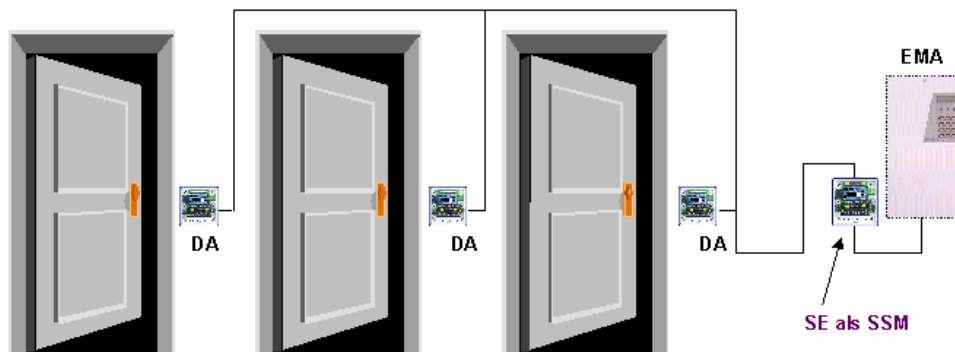
1. Activation unit(s) (MA and SA)

Such a unit is used to switch the alarm system. You need at least one activation unit (AU) to activate and deactivate the system externally. If you want to be able to activate/deactivate from several locations, you need the corresponding number of activation units. You can use a mouse click to issue the authorizations for activating and deactivating the alarm system in the locking plan.

Basically, there is a difference between the master activation unit (MA) and the slave activation units (SA). The SAs are needed only if you want to activate or deactivate from more than one location. It is always the MA that activates or deactivates the alarm system externally using a floating contact. SAs only send the appropriate requests to the MA. You can also activate internally by using SAs that are separately connected to the internal activation connection of the burglar alarm center (BAC).

2. Deactivation units (DA)

These are installed next to the doors of the secured area (and in the immediate vicinity of the digital cylinder). They see to it that these doors cannot be accidentally opened even with an authorized transponder if the alarm system has been activated externally. This reliably prevents false alarms.



Switching on the alarm system (burglar alarm system, BAS)

The person with switching authorization presses his or her transponder near an activation unit two times in quick succession (within 2 sec.). This sends a signal to all deactivation units present. If lock contacts are connected to the deactivation units, the DAs first verifies that the doors have been correctly locked. The digital locking cylinders or Smart Relays are not deactivated unless this is the case, so that it is no longer possible to enter the secured area. The activation unit does not receive a positive acknowledgement until all lockings have been successfully deactivated. It then uses a floating contact to activate the alarm system externally (compelled signaling). The light emitting diodes of the activation units signal this by lighting for 2.5 seconds. The light emitting diode(s) on the deactivation unit(s) go out. **The BAS** acoustically signals – for example, on the activation unit – that the system has been successfully activated.

Switching off the alarm system

The person with switching authorization again presses his or her transponder twice in quick succession within transmitting range of the activation unit. The deactivation units signal this to the digital locking cylinders or the digital Smart Relays. The LEDs on the activation units visually signal that the system has been successfully deactivated by blinking 1x short-long. The LEDs on the deactivation unit(s) light again. (The LEDs on the deactivation units are used only for testing purposes, so they do not have to be brought out where they can be seen). Now it is possible to access the doors again with all authorized transponders.

- ☺ By simply clicking the transponder button within transmitting range of activation units, you can determine the activation state of the alarm system if the LEDs on the activation units are brought out where they can be seen. 1 x short-long blinking means "deactivated", 1 x long (2.5 sec.) blinking means "activated".

Activation transponder

For emergencies, you can use the locking plan software to program a transponder that cancels the deactivation of the locking cylinder so that the doors can be opened with an authorized transponder. However the alarm system remains activated **externally**.

Time zone control und access logging

The activation units (master and slaves) can log activation/deactivation switches (access logging), and you can define time slots during which it is possible to activate/deactivate the system (time zone control):

Access logging	The activation unit stores the last 128 activations/deactivations with date, time and the user name of the transponder. You can read out the data with the programming device or over the network.
Time zone control	You can program activation units in such a way that authorized transponders can only switch the alarm system at certain times.

Refer to the Software Operating Instructions, timezone administration

1.2 Safety Remarks

- Read through the assembly instructions carefully and thoroughly before installing and commissioning the Shunt lock components. They contain important information on the assembly, programming and operation.
- The components are built in accordance with the latest state of the technology. Use them only as instructed and when they are in perfect technical condition and are properly installed according to the technical specifications
- The manufacturer is not liable for damages that are caused by use that does not comply with the directions.
- Keep the documentation that comes with the product and system-specific notices in a safe place.
- Only trained experts are authorized to perform installation, programming and repair work.
- Soldering and connection work anywhere in the entire system must be performed only when the system is voltage-free.
- Soldering work must be performed with a temperature-controlled soldering iron that is electrically insulated from the power system.
- Observe VDE safety regulations and regulations from the local electric utility.
- Do not use the components in areas subject to explosion hazards or in areas with fumes that dissolve metal or plastic.
- DIN norms and the guidelines of VdS Class C must be adhered to.

2.0 Assembly Instructions

2.1 General Information on Installing the Components

Always install in the protected area, for example, in the inside area behind the door, behind brickwork, etc. There are some materials, however, such as stainless steel or aluminum, that can significantly reduce the range. There may also be sources of magnetic interference near the activation or deactivation unit that also very strongly reduce the range. When making the connections, please observe the technical specifications for the activation unit and the relay (refer to Chap. 6). Failing to comply with these values can lead to interference with the function of the components or even to destruction of the components. **Make absolutely sure that the polarity is correct.** You can attach the components (deactivation and activation units) on the wall surface with two countersunk head screws, 3.5 x 30 mm, and two S5 plastic plugs (not included in the delivery).

The two enclosed VdS adhesive labels guarantee permanent evidence if the housing is opened without authorization (sealing of the cover screws).

Programming the components

Program the Shunt lock components and accompanying lockings before installation. When doing this, please keep the following points in mind:

- Program activation units, deactivation units and locking cylinders in the same locking plan
- Select type *Control unit* for the shunt lock components
- During programming, supply only one component with power at a time and do not connect the cables to one another.
- After programming, read out the components and verify that they report correctly.

Refer to Chapter 3 for more detailed information.

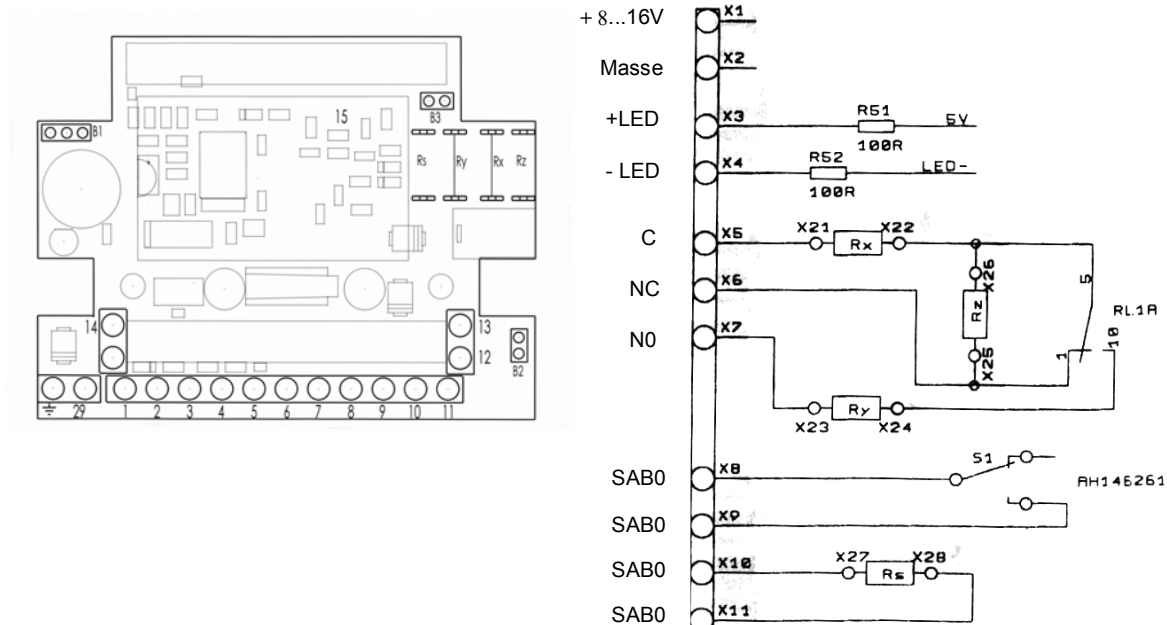
Installing a locking that should be deactivated with the Shunt lock function

Install the digital locking (Smart Relay or locking cylinder) that should be deactivated by the Shunt lock function. **Follow the installation guidelines. These are under the relevant heading in the system manual.**

VdS Shunt lock function 3066

Page 8

2.2 Installing the Deactivation Unit (DA)



Soldering terminal assignments:

- 1 Supply voltage positive pole
- 2 Supply voltage negative pole (ground)
- 3 + 4 Connection for LED (5 volts) in outside area
- 5 - 7 Not used
- 8 - 11 Sabotage contacts
- 12 Optional lock monitoring contact for activation suppression
- 13 Deactivation request (input)
- 14 Deactivation acknowledgement (output)
- 15 Ground (identical to soldering terminal 2)
- 29 Acoustic BAC acknowledgement (**not for DA**)
- 30 Solder terminal for cable screen

Jumper settings:

Jumper B1 can be inserted any way
 Insert jumper B2 for maximum transmitting range
Do not insert jumper B3

2.2.1 Testing the Deactivation Unit (DA):

To test, connect the deactivation unit to a 9-volt compound battery. Make sure that the polarity is correct. Position the deactivation unit within radio range of the digital locking:

Deactivation unit → digital locking cylinder max. 40 cm (16 inches)

Deactivation unit → digital Smart Relay min. 20 cm, max. 1 m (8 till 40 inches)

The ranges depend on the structural circumstances and so will vary.

Make sure that both the deactivation unit and cylinder are correctly programmed (refer to Chapter 3). Then connect soldering terminals 13 and 15 (ground) to one another. This deactivates the cylinder/Smart Relay (signal tone for cylinder) and the LED on the deactivation unit goes out. The cylinder no longer responds to transponders. When you remove the connection, the cylinder or Smart Relay is activated. The LED lights again. Repeat the tests several times until the radio link works perfectly.

- ☺ You can increase the range between the cylinder and deactivation unit by using FH version locking cylinders (with plastic inside knob).

Once the deactivation unit successfully passes the test, you can carry out the actual permanent installation.

2.2.2 Connecting Power Supply, Lock Contact Evaluation and Sabotage Contacts:

- Power supply

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to

exceed a value of +16 V under any circumstances.

Connect soldering terminal 2 to ground.

- Optional lock contact evaluation (global activation suppression)

If you want the alarm system to remain inactivated until all doors of the security area are closed, meaning the bolts have been driven out, you can connect the lock switch contact to soldering terminals 12 and 15. The lock contact must be a floating electric strike.

- ☺ If there is no lock contact (not VdS-compliant), it is, of course, impossible to check whether all doors have been locked, which means that it is also possible to activate the alarm system if some doors are not locked. In any case, however, all cylinders must have been successfully deactivated. If there is no lock contact, simply do not connect soldering terminals 12 and 15.

Test the shunt lock function again after you have connected the lock switch contact. Try to deactivate the locking cylinder or Smart Relay even when the bolts have not been driven out.

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 so that you have a visual display in the outside area showing whether the cylinder or Smart Relay is activated or deactivated. Maximum length of the line: 10 m (33 feet).

- Switch contacts (not used)

Soldering terminals 5 to 7 are not needed for the deactivation unit.

- Sabotage contacts

Connect these to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

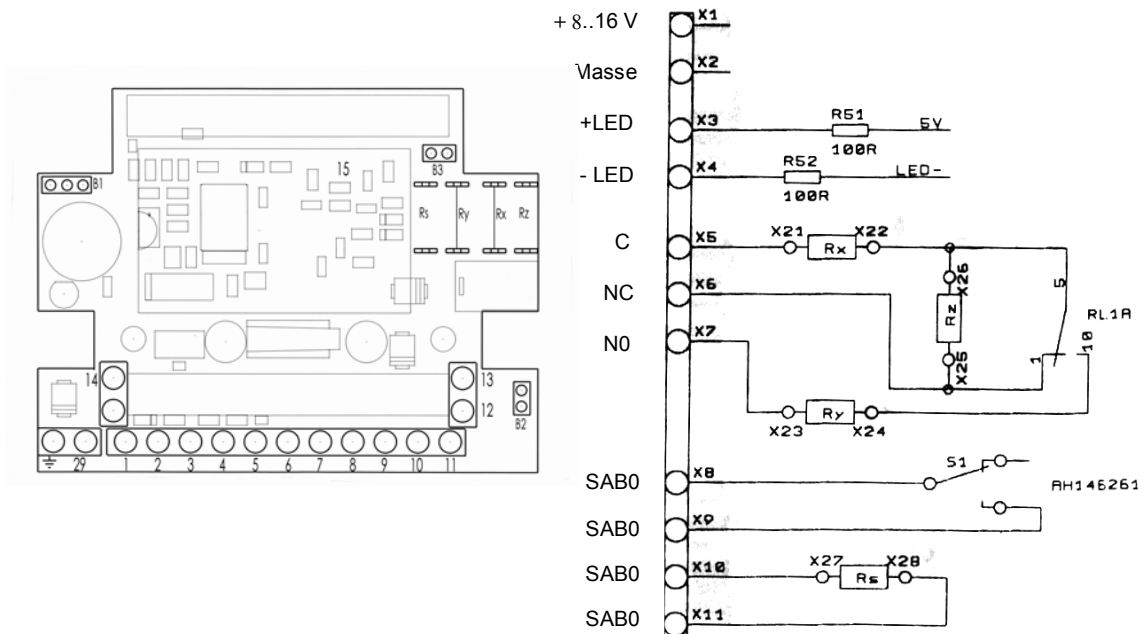
Install other deactivation units, if any, according to the same plan.

2.2.3 Connecting Deactivation Request and Deactivation Acknowledgement Refer to Chapter 2.5

VdS Shunt lock function 3066

Page 11

2.3 Installing the Master Activation Unit (MA)



Soldering terminal assignments:

- 1 Supply voltage positive pole
- 2 Supply voltage negative pole (ground)
- 3 + 4 Connection for LED (5 volts) in outside area
- 5 - 7 Floating contacts for switching the alarm system
- 8 - 11 Sabotage contacts
- 12 Activation request from slave activation units (SAs) (optional)
- 13 Deactivation acknowledgement (input) → Activation suppression when ground is applied
- 14 Deactivation request (output)
- 15 Ground (identical to soldering terminal 2)
- 29 Acoustic activation acknowledgement by BAC (not for DA)
- 30 Solder terminal for cable screen

Jumper settings:

Jumper connects right and middle contacts of B1:

⇒ Acoustic acknowledgement after activation release by activation unit

Jumper connects left and middle contacts of B1:

⇒ Acoustic acknowledgement after final activation is done by the BAC (this is the VdS-compliant configuration).

The BAC must draw pin 29 to ground for the acoustic acknowledgement.

Jumper B2 is inserted:

⇒ Maximum transmitting range. For VdS-compliant installation, however, you must then work with external keys to differentiate between outside and inside. (refer to 4.3 VdS-Compliant Installation of the Activation Unit).

⇒ In VdS-compliant installation, the range of the antenna extender is reduced solely by the correct use of the aluminum sleeve. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

Install the activation unit so that the distance between its antenna and other digital components is **at least 1 m (40 inches)**.

2.3.1 Testing the Master Activation Unit (MA):

Before final installation, apply voltage to contacts 1 and 2 of the activation unit (compound battery). Make sure that the polarity is correct. Do not wire the other contacts for this test.

Transponder → master activation unit **1 cm to max. 3 cm (.4 to 1.2 inches)**

- ① This corresponds to the strongly reduced range when the screening sleeve is inserted on the antenna extender (refer to Chap. 4.3).

Make sure that all components are correctly programmed (refer to Chap. 3). Insert jumper B1 on the right. Then test whether the relay on the activation unit switches (soldering terminals 5 and 7) by operating the transponder two times in quick succession (within 0.5 ... 2 sec.).

An acoustic signal indicates the switching state of the alarm system. A 2.5-second long continuous tone signals that the activation contact was closed and a two-part signal tone (short – long) means that the activation contact is open again (de-activated).

Then you must convert the acoustic activation acknowledgement to BAC operation (insert jumper B1 to the left) and test it by attempting to activate the system. Once the master activation unit has successfully passed the test, you can carry out the actual permanent installation.

2.3.2 Connecting Power Supply, Switch Contacts and Sabotage Contacts:

- Power supply

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to

exceed a value of

+16 V under any circumstances

Connect soldering terminal 2 to ground

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 for visual signaling. When the transponder is operated successfully, the LED blinks. Maximum length of the line: 10 m (33 feet).

- Switch contacts

Connect them to the alarm system. Soldering terminal 5 is the common contact, 6 is for the electric strike and 7 for the make contact. Refer to the BAS installer instructions for the wiring and values for the terminating resistor(s).

Rx: wire jumper; Ry: wire jumper; Rz: terminating resistor

- Sabotage contacts

Connect them to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

- Global activation suppression (optional)

Applies ground (such as pin 15 or pin 2) to pin 13 over a floating contact so that the system cannot be activated.

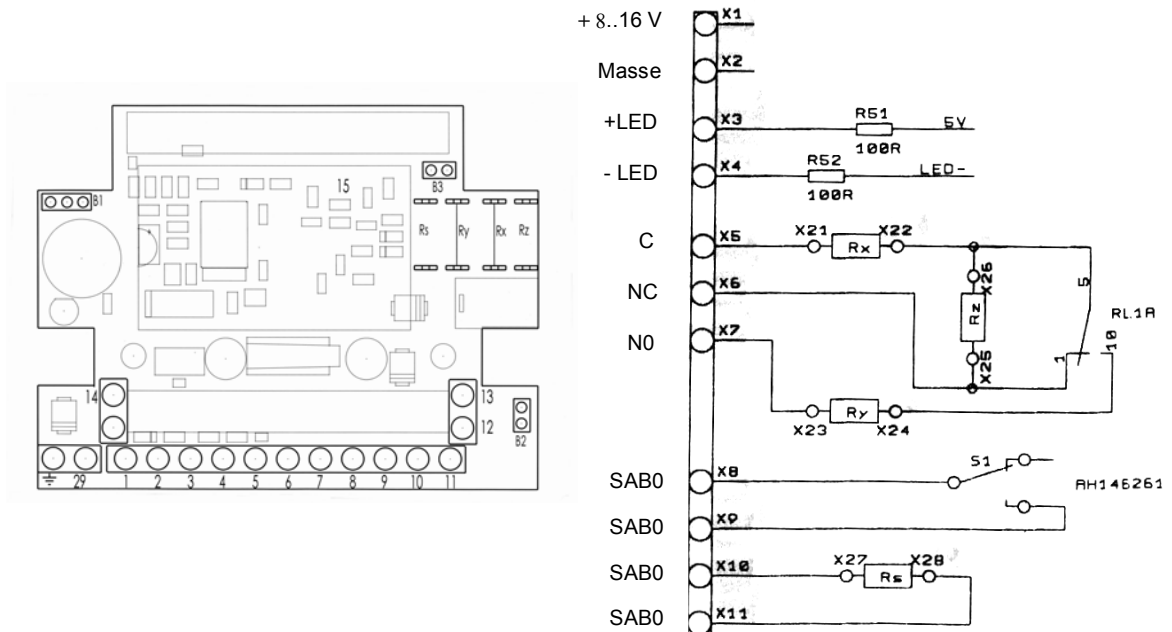
2.3.3 Connecting Deactivation Request, Deactivation Acknowledgement and Activation Request

Refer to Chapter 2.5.

VdS Shunt lock function 3066

Page 14

2.4 Installing the Slave Activation Unit (SA)



Soldering terminal assignments:

- 1 Supply voltage positive pole
- 2 Supply voltage negative pole (ground)
- 3 + 4 Connection for LED (5 volts) in outside area
- 5 - 7 Not used
- 8 - 11 Sabotage contacts
- 12 Optional activation suppression when ground is applied (for example, lock contact evaluation)
- 13 Deactivation acknowledgement (input)
- 14 Activation request to the master activation unit MA (output)
- 15 Ground (identical to soldering terminal 2)
- 29 Acoustic activation acknowledgement by BAC (not for DA)
- 30 Solder terminal for cable screen

Jumper settings:

Jumper connects right and middle contacts of B1:

⇒ Acoustic acknowledgement after activation release by activation unit

Jumper connects left and middle contacts of B1:

⇒ Acoustic acknowledgement after final activation is done by the BAC. The BAC must draw pin 29 to ground (VdS-compliant configuration).

Jumper B2 is inserted:

⇒ Maximum transmitting range. For VdS-compliant installation, however, you must then work with external keys to differentiate between outside and inside. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

⇒ In VdS-compliant installation, the range of the antenna extender is reduced solely by the correct use of the aluminum sleeve. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

2.4.1 Testing the Slave Activation Unit (SA):

Before final installation, apply voltage to contacts 1 and 2 of the activation unit (compound battery). Make sure that the polarity is correct. Do not wire the other contacts for this test.

Transponder → slave activation unit **1 cm to max. 3 cm (.4 to 1.2 inches)**

- ① This corresponds to the strongly reduced range when the screening sleeve is inserted on the antenna extender (refer to Chap. 4.3).

Make sure that all components are correctly programmed (refer to Chap. 3). Insert jumper B1 on the right. Then test whether the relay on the activation unit switches (soldering terminals 5 and 7) by operating the transponder two times in quick succession (within 0.5 ... 2 sec.).

Then you must convert the acoustic activation acknowledgement to BAC operation (insert jumper B1 on the left) and test it by attempting to activate the system. Once the slave activation unit successfully passes the test, you can carry out the actual permanent installation.

2.4.2 Connecting Power Supply, Sabotage Contacts and Local Activation Suppression:

- Power supply

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to

exceed a value of +16 V under any circumstances.

Connect soldering terminal 2 to ground.

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 for visual signaling. When the transponder is operated successfully, the LED blinks. Maximum length of the line: 10 m (33 feet).

- Switch contacts

Soldering terminal 5 to 7 are not needed for the slave activation unit unless you want to use the SA for internal activation. In this case, wire the SA separately from other activation units. Connect soldering terminals 5 to 7 to the internal activation connection of the BAC. Refer to the BAS installer instructions for wiring information.

- Sabotage contacts

Connect them to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

- Optional local activation suppression

If you want to use activation suppression, connect a floating contact between soldering terminals 12 and 15. When the contact is closed, it is impossible to activate or deactivate the system locally (from this SA). This has no effect on the activation behavior of other activation units.

2.4.3 Connecting Deactivation Acknowledgement and Activation Request

Refer to Chapter 2.5.

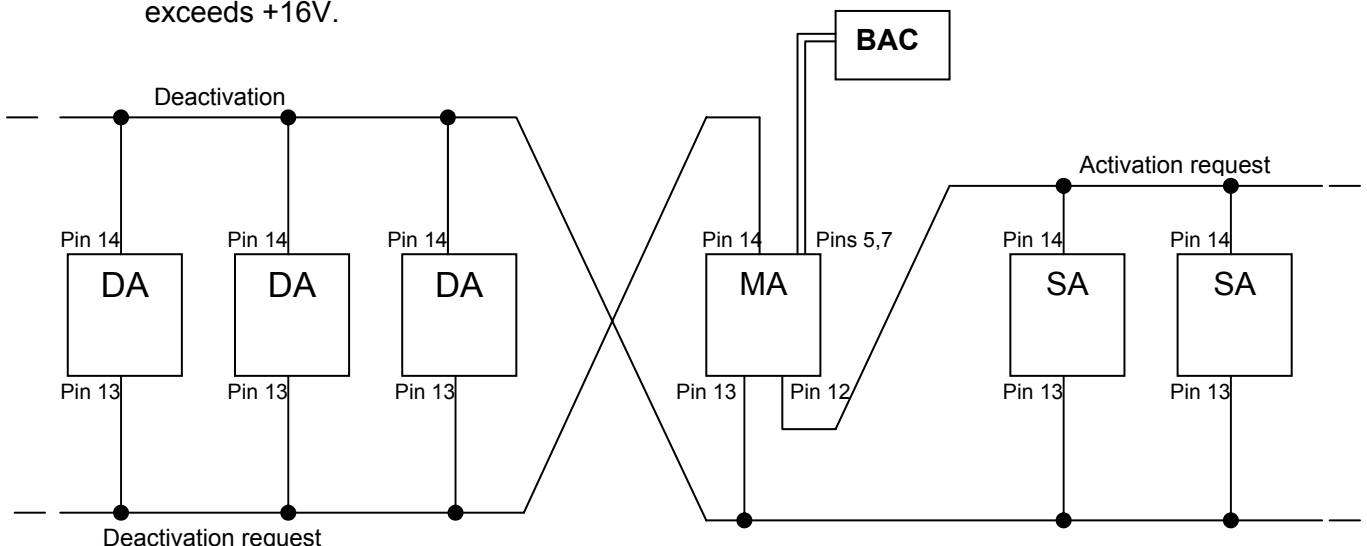
2.5 Wiring the Shunt Lock Components

We recommend that you use the following types of lines: J-Y(ST)Y 6 or 8 pin, Ø 0.6 mm. The diameter should be fit to the length of the line so that the minimum voltage for the components never falls below +8 volt (voltage drop on the line).

ATTENTION: You should always shield longer lines.

Connect the deactivation request, deactivation acknowledgement and activation request to one another according to the drawing below.

Also connect the supply voltage everywhere (pins 1 and 2, with the positive on 1 and ground on 2). Make sure that the polarity is correct. Then measure the voltage on all units and make sure that the voltage never falls below a value of +8v and never exceeds +16V.



VdS Shunt lock function 3066

	DA	MA	SA
Deactivation request	Solder pin 13	Solder pin 14	-
Deactivation acknowledgement	Solder pin 14	Solder pin 13	Solder pin 13
Activation request	-	Solder pin 12	Solder pin 14
Activation suppression	Solder pin 12	-	Solder pin 12
Supply voltage positive	Solder pin 1	Solder pin 1	Solder pin 1
Supply voltage ground	Solder pin 2	Solder pin 2	Solder pin 2

DA = Deactivation unit
MA = Master activation unit
SA = Slave activation unit

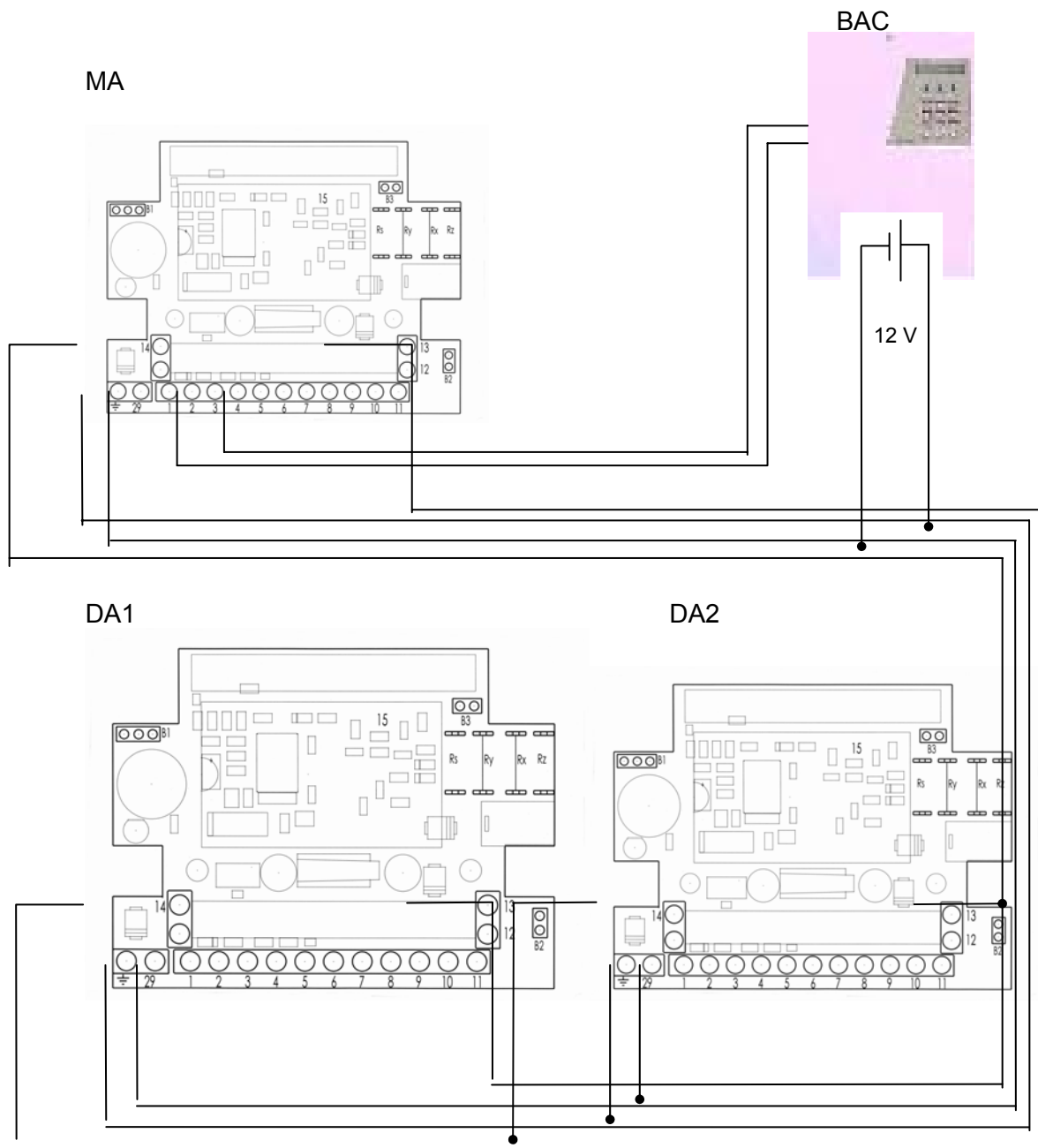
2.6 Functional Principles

1. A DA deactivates a neighboring cylinder if the deactivation request line (pin 13) is drawn to ground potential by the MA **or** the BAC.
2. A DA reactivates a neighboring cylinder as soon as the deactivation request line (pin 13) is high-impedance, which means that the MA output (pin 14) and the corresponding BAC output must **both** be high-impedance.
3. A DA draws the deactivation acknowledgement line (pin 14) to ground as long as its neighboring cylinder is activated or as long as the lock monitoring input (pin 12) is connected to ground. Therefore, a lock contact must be an electric strike between ground and pin 12 that opens when the bolt is pushed forward.
4. Consequently, the deactivation acknowledgement line does not go to high-impedance until each deactivation unit has successfully deactivated its neighboring cylinder and, if there is lock contact evaluation, all bolts have been pushed forward.
5. An MA draws the deactivation request line (pin 14) to ground potential after someone authorized to activate the system operates the transponder. This causes each DA to start to deactivate its cylinder.
If the MA receives a positive deactivation acknowledgement within no more than 10 sec. (deactivation acknowledgement line goes high-impedance), a floating contact is closed between pin 5 and pin 7. This requests the BAC to activate the system.
6. When someone authorized to activate the system operates the transponder again, the floating contact between pins 5 and 7 is separated immediately, so that the BAC is requested to deactivate.
Then the deactivation request line (pin 14) is set to high-impedance. The DAs then start to reactivate unless the BAC continues to draw the deactivation request line to ground potential in order to prevent the cylinders from reactivating (for example, until the system deactivation is complete).

VdS Shunt lock function 3066

7. Instead of operating the transponder at the MA, the slave activation units (after transponder activation at the SA by someone authorized to activate the system) can trigger an activation or deactivation process with a "high-impedance – ground potential – high-impedance" pulse on the activation request line (pin 14).

Connecting plan (example with one MA and 2 DAs)



After you have completed the installation work, carry out a function test.

Do this by operating an authorized transponder near the activation unit twice in quick succession. The light emitting diodes on the activation unit and the deactivation unit(s) go out and you receive the acoustic acknowledgement signal from the BAC or (if jumper B1 is inserted on the right) the signal lasting 2.5 seconds from the activation unit indicating that the alarm system has been activated.

Check whether the cylinder(s) or Smart Relay(s) have been deactivated.

Operate the transponder near the activation unit two times again. This unit signals the activation of the lockings only visually on the LED with 1 x short-long blinking or (if jumper B1 is inserted on the right) with a double signal tone from the activation unit. The LEDs on the shunt lock components light again.

The locking cylinder or Smart Relay is now active and can be switched if you operate an authorized transponder one time.

Please set the acoustic activation acknowledgement to BAC operation (insert jumper B1 on the left) if you have not done this yet.

Test the Shunt lock function several times.

VdS Shunt lock function 3066

Page 20

3.0 Programming

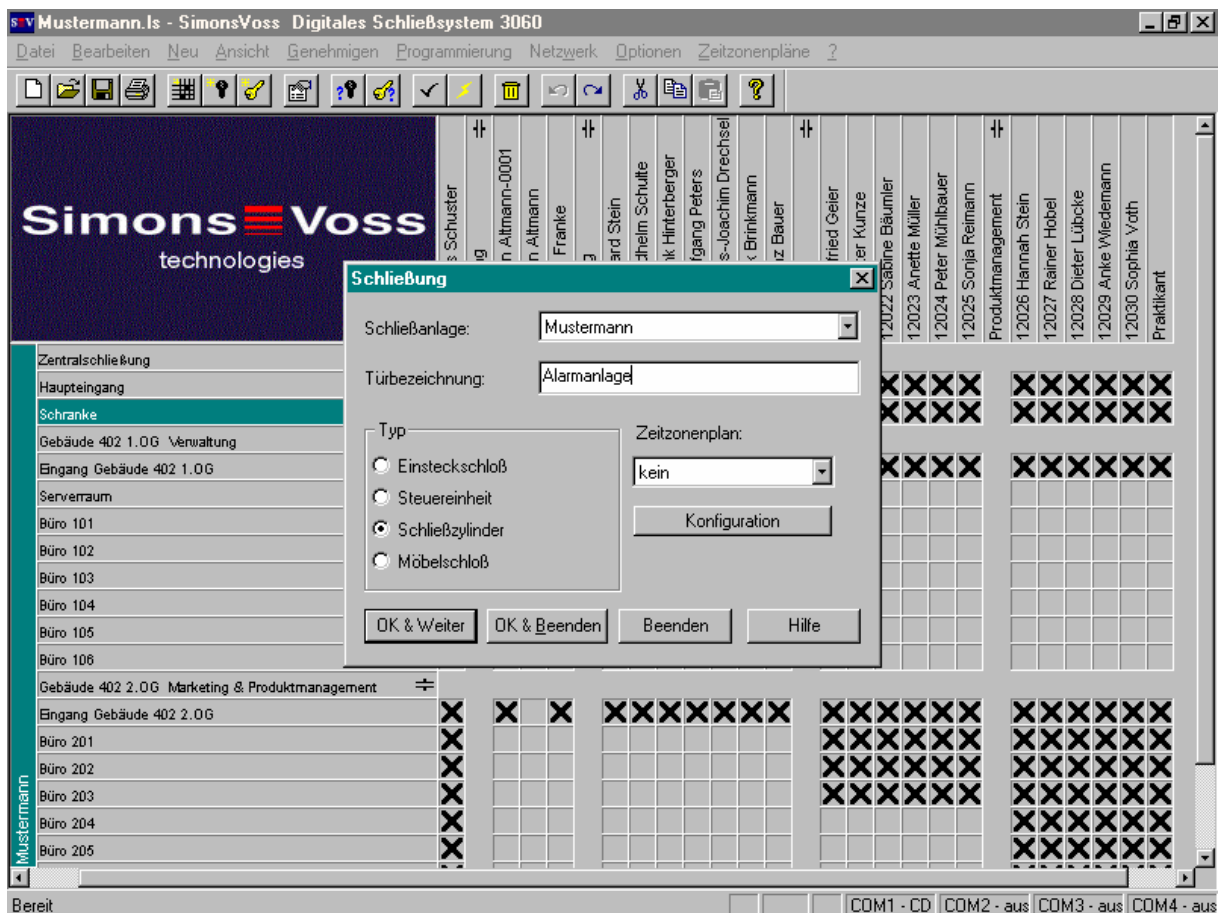
3.1 Programming the Activation Units (MA and SA)

If you want to add the shunt lock components at some time after the initial installation, open your locking plan with the password. If this is the initial installation, create a new locking plan.

Click the locking above which you want to add an activation unit. Select **New → Locking**. Then give the activation unit a name:

➡ For example, Alarm system

In the field **Type**, select *Control unit*. Click **OK & Exit** or **OK & Next**, if you want to set up additional activation units (slaves).



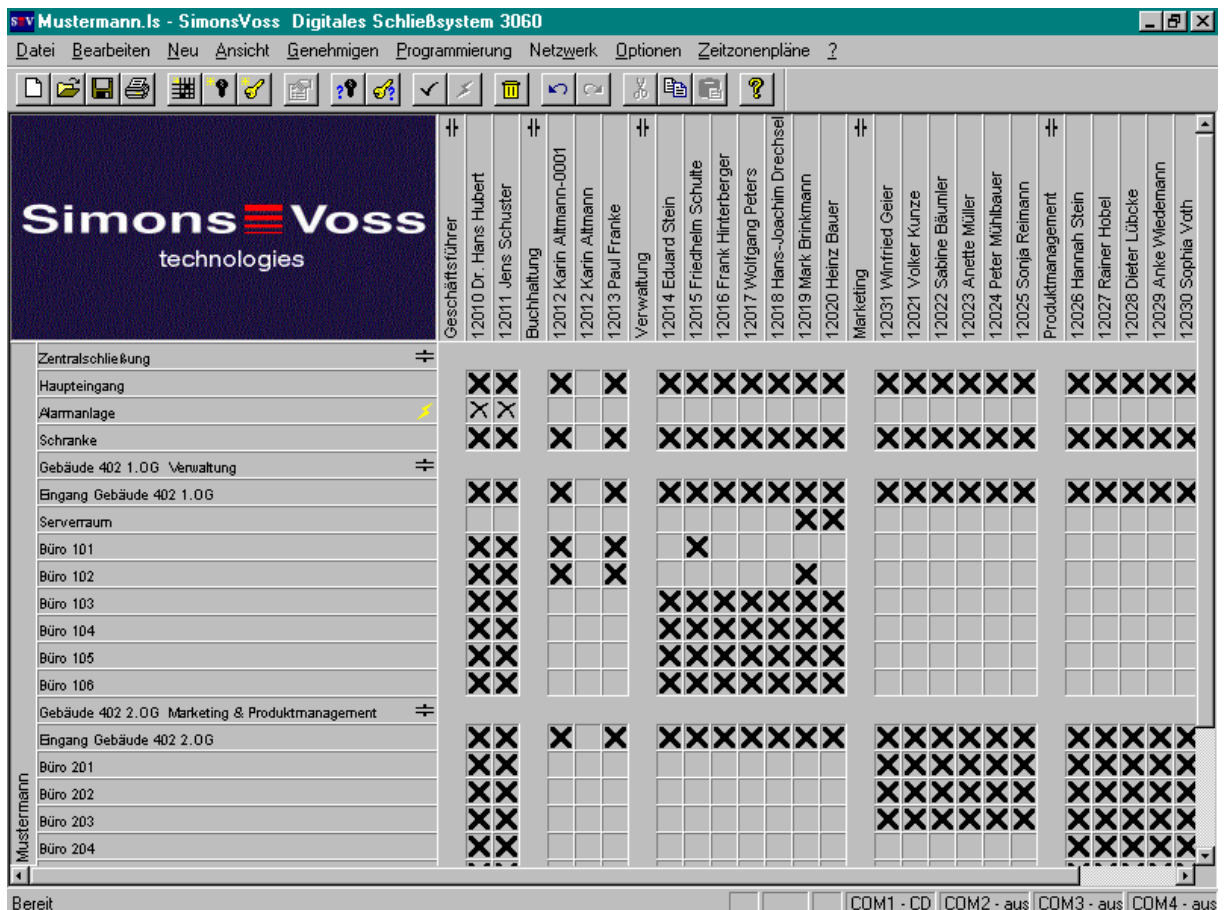
VdS Shunt lock function 3066

In the locking plan, make a cross by the employees who are authorized to turn the alarm system on and off.

☺ You do not have to reprogram the transponders in this case.

Approve your locking system and program the activation unit under **Programming** → **Locking**.

👉 The activation unit needs supply voltage during the programming. You can provide this with a 9-volt compound battery, for example. Program activation unit(s) and deactivation units separately from one another. Do not wire the two components until after you have programmed them successfully.



VdS Shunt lock function 3066

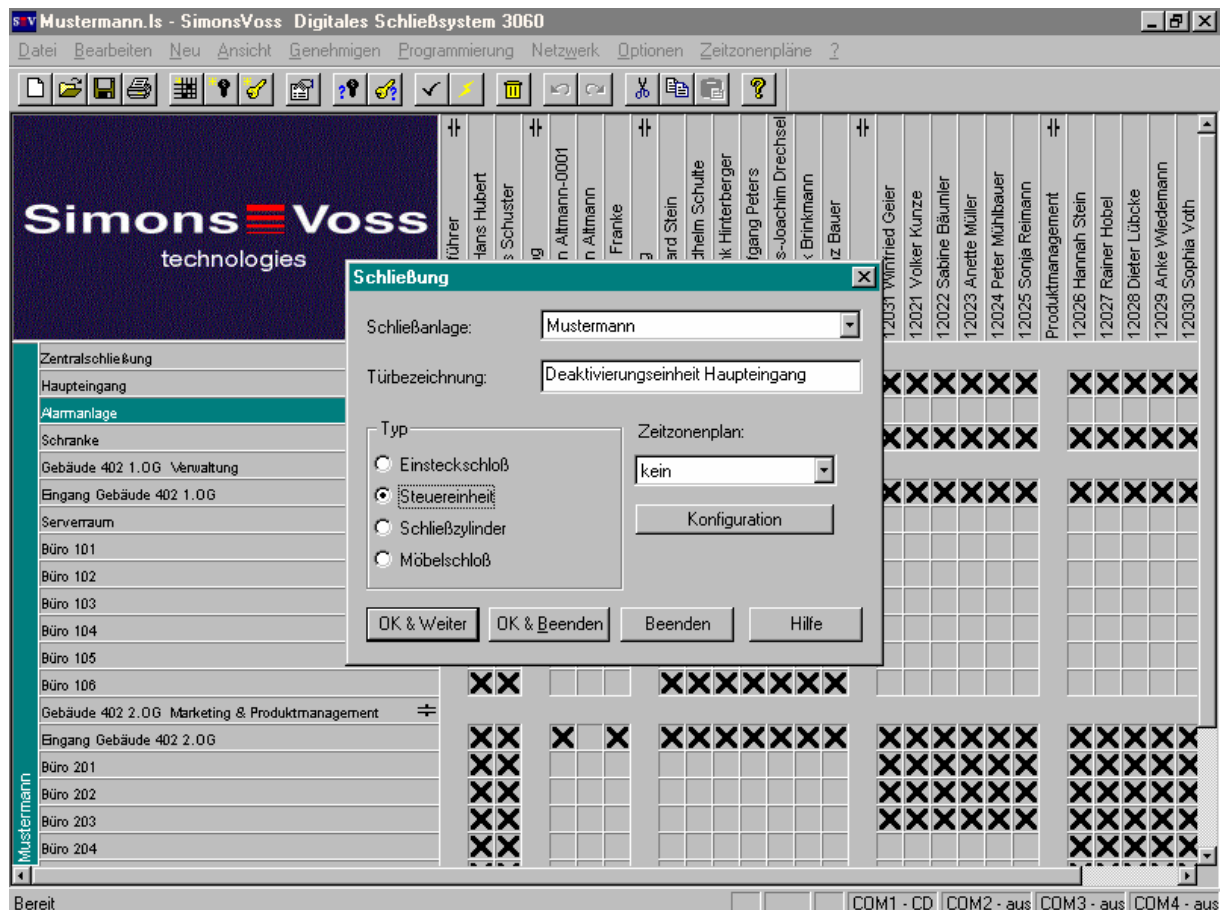
3.2 Programming the Deactivation Units (DA)

Click the line in the locking plan above the one where you want to add a deactivation unit. Select **New** → **Locking**. Then give the deactivation unit a name:

➡ Such as Deactivation unit, main entrance

In the field **Type**, select *Control unit*. Click **OK & Exit**. If you want to set up additional deactivation units, repeat these steps.

😊 If you always add the deactivation units above the accompanying digital locking cylinder, you will have a better overview of the system.



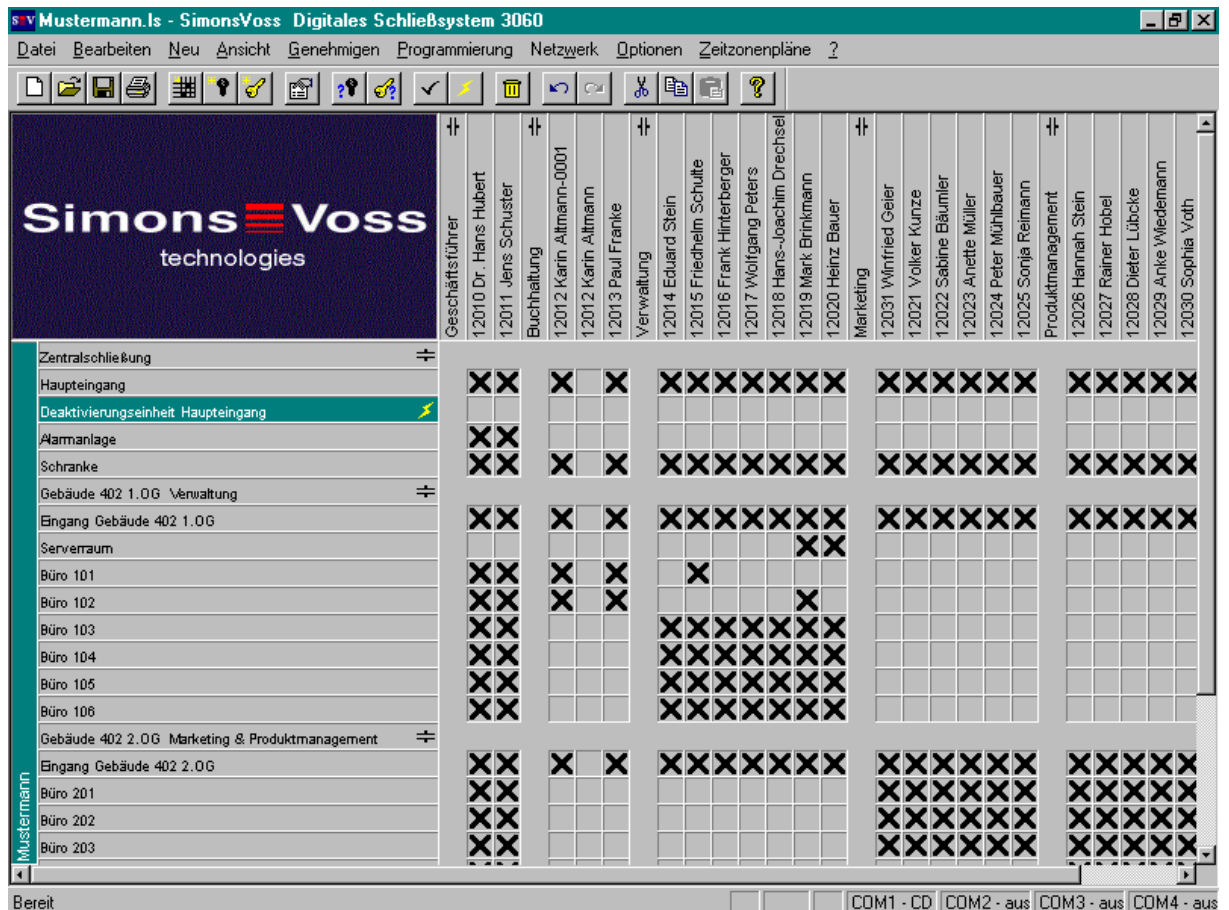
Deactivation units do not need any authorizations which means that you do not have to insert any crosses. Approve your locking system and program the deactivation units under **Programming** → **Locking**.

👉 The deactivation unit needs supply voltage during the programming. You can provide this with a 9-volt compound battery, for example. Program activation unit(s) and deactivation units separately from one another. Do not wire the two components until after you have programmed them successfully.

VdS Shunt lock function 3066

Read out the shunt lock components: **Programming** → **Read unknown locking**. The type of the component (deactivation unit or activation unit) is displayed.

Attention: The display treats slave activation units as normal control unit.

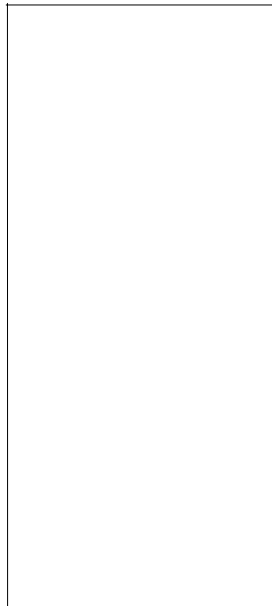


4.0 Installation

4.1 Installing the Deactivation Unit

Install the deactivation unit DA in the immediate vicinity of the digital locking cylinder (no farther than approximately 30 cm or 12 inches). This guarantees optimum transmission traffic. Align the deactivation unit so that both fastening screws lie in a horizontal line. Then the antennas point directly to the locking cylinder (refer to the drawing below).

😊 You can always achieve better ranges if you use FH cylinders (plastic knob instead of stainless steel).



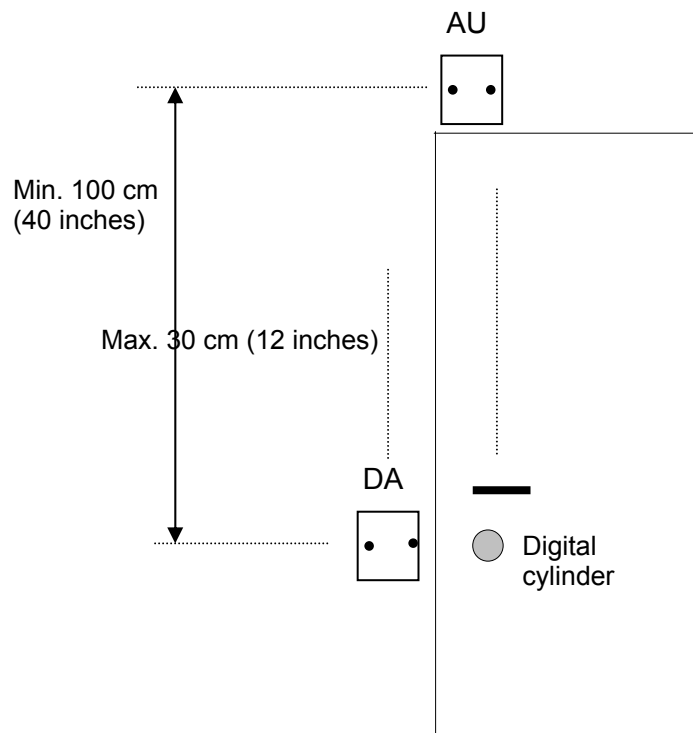
4.2 Installing the Activation Unit (MA and SA)

You should install the activation unit (AU), no matter whether it is a master activation unit MA or slave activation unit (SA), above the door case and above the locking cylinder. In any case, the distance to other SimonsVoss components **must** be at least 1 m or approximately 40 inches (refer to the drawing).

Only in this way can you rule out mutual interference influences.

If you install it above the door case, align the activation unit so that the two fastening screws lie in a horizontal line. This eliminates interference when the door is used in the normal way. (Refer to the drawing below.)

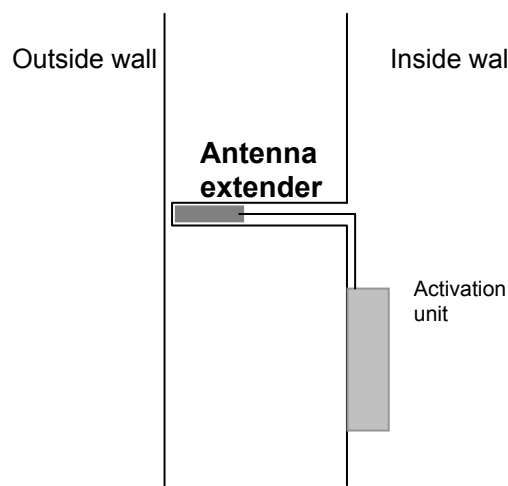
This installation is done without the antenna extender and with jumper B2 is inserted (max. range). Because this (simple) installation method allows the system t



4.3 VdS-Compliant Installation of the Activation Unit (MA and SA)

VdS-compliant installation must guarantee that the system can be activated from the outside, but not from the inside. This requires the following measures:

3. Use **activation units with antenna extender**. Shorten the color-coded cable on the antenna extender to the required length, pull the cable through the bore hole in the aluminum screening sleeve and connect the cable to soldering connections 16 to 20 as follows:
16 - green, 17 - blue, 18 - screening, 19 - red, 20 - yellow.
4. **Insert jumper B2!** The range of the antennas is reduced if you use the aluminum sleeve correctly.
Bore a blind hole (\varnothing 23 mm) in the outside wall, insert the antenna extender in the blind hole and fix in position. (See drawing below). While doing this, make sure that you get within at least 2 cm (approximately 3/4 inch) of the front side of the antenna extender from the outside and that you guarantee a minimum distance of at least 12 cm (4 3/4 inches) to the front side of the antenna extender from the inside. This is approximately the thickness of the wall.
The distance between the antenna and activation unit must be at least 30 cm (12 inches) and the distance from the locking cylinder to the antenna must be at least 1 m (40 inches).
5. We recommend that you mark the position of the blind hole on the outside wall with a red point or similar marking. The person authorized to activate the system must hold the transponder at this point in order to be able to communicate with the antenna extender.



6. Install the deactivation unit according to the description in Chapter 4.1.

VdS Shunt lock function 3066

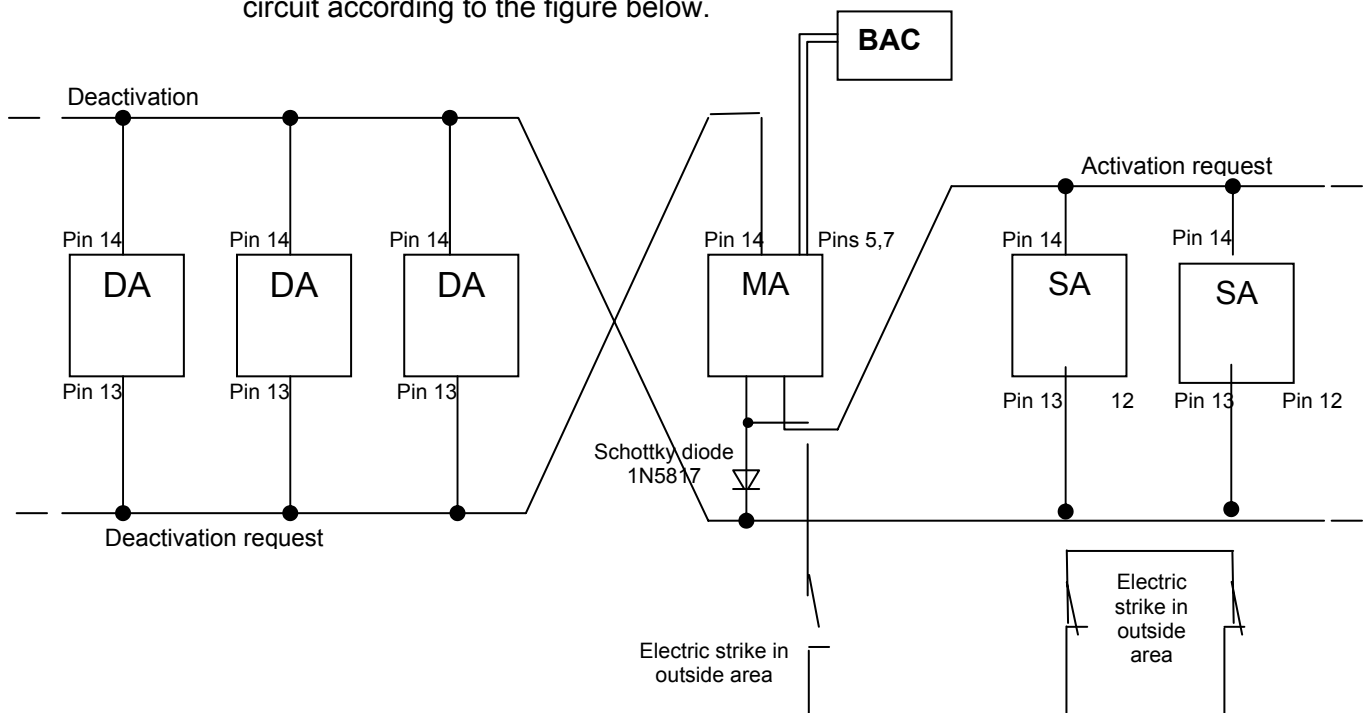
7. You can also **optionally** use an **activation unit without antenna extender**. Install it as described in Chapter 4.2.

In order to guarantee that the system can be **externally activated** from the outside only, you must then install a **button in the outside area**. You cannot externally activate or deactivate the system by operating a transponder until this button is pushed.

The deactivation acknowledgement input (pin 13) is suppressed on master activation units (MAs) as long as it is connected to ground (normally closed button in outside area).

A Schottky diode decouples the deactivation acknowledgement line (see below). This diode is needed, however, only if there are slave activation units.

With slave activation units (SAs), you can apply the activation suppression (pin 12) to ground over a normally-closed button that is in the outside area. If there is also an activation suppression button on the master, you should use a circuit according to the figure below.



5.0 Special Versions of the Shunt lock function 3066

5.1 Operating the Activation Unit without a Deactivation Unit

If you want to activate and deactivate the burglar alarm system externally with the transponder instead of with a key, you only need a master activation unit (MA). In this case, however, you will lose the true purpose of the Shunt lock function.

- 👉 You need to connect only pins 1 and 2 for the power supply, the floating switch contact (pins 5, 6, 7) and the sabotage contacts (pins 8 to 11). Do not connect the other lines of the activation unit (refer to Chapter 2.3).

5.2 Operating the Deactivation Unit without an Activation Unit

If you continue to operate the alarm system with a standard key, you can do without the activation unit.

Connection assignment

Connect the supply voltage (separate power supply) to soldering terminals 1 and 2. Connect terminals 13 and 15 over a relay contact of the alarm system (floating make contact). If there is a lock switch contact, wire this to soldering terminals 12 and 15 (Refer to Chapter 2.2).

- 😊 As long as soldering terminals 13 and 15 are connected to one another, for example, by a relay point of the alarm system, all digital locking cylinders equipped with a deactivation unit are deactivated. This means it is not possible to accidentally go through these doors when the alarm system is activated.

VdS Shunt lock function 3066

Page 29

6.0 Data Sheet

MA, SA and DA	Operating voltage Current consumption	8 to 16 volts DC < 30 mA
Applied relay for switching output	Max. continuous current Max. switch on current Max. switching voltage Max. switching capacity	1 A 1 A 40 V AC 30 W / 60 VA
Tamper contact	Make contact	1 A / 30 V DC
Transponder range with extended antenna		1 - 3 cm (.4 to 1.2 inches)
Extended antenna Dimensions Cabel length		64 x 18 mm 5 m
Temperature range	-10°C to +55°C (14°F to +131°F)	
Degree of protection	VdS environmental class II	
Housing	Material Color Dimensions [L/W/H]	S-B or A-B-S White 85 x 85 x 26 mm
	Article description	_____
	Article number	_____
	VdS no.	G 101 160

Programming Transponder 3067

State of: June 2006

Programming Transponder 3067

Content



1.0	Introduction	3
2.0	Backup Card	3
3.0	Programming Notes	4
3.1	Error Messages	4
3.2	Initial Programming	4
3.3	Reading Out a Transponder	5
3.4	Adding a New Transponder	5
3.5	Emergency Opening	6
3.6	Blocking a Lost Transponder	6
4.0	Loss of the Programming Transponder	7
5.0	Data Sheet	7

1.0 Introduction

The Programming Transponder 3067 is used for programming Digital Locking Cylinder 3061 and Transponder 3064 devices. You can use it to perform the following actions:

- Program the system for the first time
- Make changes to the authorisations
- Block lost transponders
- Determine the ID number of a transponder

It is not possible to read out the locking cylinder with the Programming Transponder. Each transponder receives its own ID number and secret password when the system is programmed for the first time. This allows the locking cylinders to distinguish between the different transponders.

The Programming Transponder takes care of this job. It assigns a consecutive ID number to the transponders, beginning with 1. The next transponder receives the number 2, and so on. You can program a maximum of 99 transponders and a maximum of 250 lockings with a program transponder.

While the Programming Transponder is carrying out the programming, the locking cylinders are also learning the secret password, as well as which transponders will be authorised in the future.

2.0 Backup Card

The entire system is protected by a secret password that is saved at the factory on the Programmer Transponder 3067. The system password is stored on the backup card. The password is covered by a scratch panel and does not have to be scratched free for programming. Keep this backup card in a safe place and make sure it is not accessible to third parties. If the backup card is lost, it may be necessary to replace the entire locking system.

3.0 Programming Notes

Always position only one locking cylinder in the immediate vicinity of the Programming Transponder during programming. All other components must be at a distance of at least 1 m (3.3 feet).

3.1 Error Messages

If you receive one of the following signals when not expected during the programming, there has been an error.

- Light emitting diode (LED) blinks red 1x:
Action: Correct the distance to the cylinder or transponder and try again.
- LED flickers and then blinks red 2x.
You have tried to authorise a transponder in more than 3 different locking systems. (A transponder can be authorised for a maximum of 3 different locking systems).
- LED flickers and then blinks red 3x:
You have tried to program more than the maximum allowable number of transponders or cylinders.
- LED flickers and then blinks red 4x.
You have tried to authorise a transponder for a cylinder that does not belong to your locking system.
or
The programming transponder button was pressed too long.

3.2 Initial Programming

The following programming steps must be done very quickly, because otherwise the Programming Transponder automatically shuts down, which interrupts the programming.

Be absolutely sure to maintain a minimum distance of 1 meter (3.3 feet) from the locking cylinder to the Programming Transponder when carrying out steps 1 and 2.

1. Briefly press the Programming Transponder button once. The light emitting diode then blinks green.
2. Operate the transponder that you want to program at a distance of from approximately 10 to 20 cm (4 to 8 in.) to the Programming Transponder and wait until the light emitting diode on the Programming Transponder lights green for three seconds. If you want to authorise another transponder, repeat step 2.
3. Once you have authorised all transponders, hold the Programming Transponder near the inner knob of the cylinder (long knob) and briefly press

its

button one time. Attention: you must press the button during the LED's blinking phase. The data is then transferred. The locking cylinder makes several signal tones during this part of the programming. If the programming was successful, the cylinder couples and the LED on the Programming Transponder lights green.

4. Perform a test to see whether all of the transponders that you have programmed function perfectly.
5. Follow the same procedure to program additional locking cylinders.

3.3 Reading Out a Transponder

In order to be able to block a lost transponder for a specific locking cylinder, you need its ID number. We recommend that you create a list containing the name of the owner and the accompanying ID number of the transponder. You can determine this with the Programming Transponder:

1. Briefly operate the Programming Transponder until it blinks green.
2. Hold the transponder whose ID number you want to read out near the Programming Transponder. Briefly operate the transponder. The LED on the Programming Transponder lights green for approximately 3 seconds.
3. Press the transponder button again. The LED lights yellowish for approximately 2 seconds.
4. The ID number of the transponder is shown by the different coloured blinking of the LED.
Red blinking indicates the tens and green blinking indicates the ones.

Example: If the ID number of the transponder is 25, the LED blinks red 2x and then green 5x. If the ID number has only one digit, only the green LED blinks.

5. Once the ID number has been determined, the LED on the Programming Transponder lights yellowish again.

3.4 Adding a New Transponder

If you want to authorise a new transponder, proceed in the same way as for the initial programming. You do not have to repeat the procedure for reading in transponders that were already authorised for locking.

3.5 Emergency Opening

It is possible to perform an emergency opening with the Programming Transponder. Proceed as follows:

1. Press the Programming Transponder button briefly one time. Then the LED blinks green.
2. Hold the Programming Transponder at a distance of approximately 10 to 20 cm (approximately 4 to 8 inches) from the locking cylinder and briefly press the button.
Attention: you must press the button during the LED's blinking phase.

3.6 Blocking a Lost Transponder

The procedure depends on whether or not you know the ID number of the lost transponder. If you do not know it, proceed as follows:

1. Press the Programming Transponder button until the light emitting diode blinks red.
2. Hold the Programming Transponder near the inner knob of the cylinder (long knob) until the LED lights green for approximately 3 seconds and the cylinder couples.
3. You have now deleted all authorised transponders and must reprogram then as described in Chapter 3.2.

If you know the ID number, you can block this specific transponder with the following steps:

Note: It is important that the steps be executed quickly for this procedure, too. Memorise the ID number of the transponder so that you can enter it immediately in the following steps. Like when reading out the number, the input is done in tens (red) and ones (green).

1. Press the Programming Transponder button until the light emitting diode blinks red. Then release the button.
2. Then repeat the procedure and wait until the LED lights red. Immediately (red LED must still be lit) press the Programming Transponder button the appropriate number of times to enter the number of tens (only if there are more than nine transponders).
3. The LED now begins to light green. Now enter the number of ones in the same way (now the green LED must still be lit).

Programming Transponder 3067

Page 7

4. The Programming Transponder repeats the ID number that you enter as a check. First the LED briefly lights yellowish. Then the Programming Transponder outputs the ID number with red and green blinking. The color then changes back to yellow and finally the LED blinks green.
5. If the displayed number is correct, hold the Programming Transponder near the inner knob of the cylinder (long knob) and press its button.
6. Then the data transfer takes place (signal tones on the cylinder). Wait until the LED has lit green for 3 seconds and the cylinder has coupled. The data transfer is not completed until this happens.

4.0 Loss of the Programming Transponder

Get your backup card and contact your dealer. You will receive a new Programming Transponder, which you first must reauthorize for your cylinders.

To do this, proceed as follows:

1. Hold your new Programming Transponder in front of a cylinder and press its button twice. The LED lights green for approximately 3 seconds and the cylinder couples.
2. Then hold your new Programming Transponder in front of the same cylinder, but this time press its button only once.
3. The light emitting diode blinks yellowish and goes out. The cylinder couples and the LED lights green for approximately 3 seconds.
4. Repeat steps 2 and 3 for all other cylinders in your locking system.
5. Once you have authorised the new Programming Transponder on all cylinders, press its button until the LED stops blinking.
6. The new Programming Transponder is now ready to use.

5.0 Data Sheet

Housing	Material	Plastic
	Colour	Grey
	Dimensions	58 x 38 x 12.3 mm

PalmCD2 Programming Device

State of : September 2004

PalmCD2 Programming Device

Content



1.0	Introduction	3
2.0	Commissioning	3
3.0	Programming with the PC or Laptop	3
4.0	Programming with the Palm Organizer	4
5.0	Setting Up the PalmCD2 With Transponder Function	4
6.0	Data Sheet	4

1.0 Introduction

The PalmCD2 is a programming device that was developed especially for operation on a PC/Laptop or in combination with a Palm m5xx or Palm Tungsten W, or T3 Organiser. It makes it very easy to program and read out all digital components of the 3060 system. You can also use the Palm to match up your personal data (addresses, calendar, etc.)

2.0 Commissioning

Insert the two batteries into the battery compartment. Make sure that the polarity is correct. Do not use storage batteries.

ATTENTION:

The battery fitted in the cylinder can, in the case of inappropriate treatment, represent a fire or bums hazard! Do not recharge, open, heat to more than 100°C or incinerate! Replace battery only with type AAA 1.5 V. Use of a different type battery can present a fire and explosion risk!

Install the PalmLDB on the Palm m5xx or Palm Tungsten W, or T3 Organiser and transmit the locking plan data from the PC to the Palm (see the PalmLDB operating instructions). Insert your Palm Organiser onto the PalmCD2 at an angle and carefully let it snap into place. Start the PalmLDB and test the PalmCD2 (Config-Device → Test).


The PalmCD2 is now ready for operation. To remove the Palm Organiser from the PalmCD2 again, you must press the slide on the back of the PalmCD2 in the direction of the arrow. Then carefully click out the Palm and slide it up.

- 👉 The PalmCD2 does not have a low battery warning with firmware versions 9.1 or earlier. If it stops answering or if there are problems with the radio link, check the batteries or replace them. Dispose of used batteries immediately, keep them out of reach of children, do not open them and do not throw them into a fire.
- 👉 For firmware version 9.3 and later and PalmLDB 1.26, a battery warning has been implemented. When a battery warning is issued, please change the batteries as soon as possible.
- 👉 Avoid direct exposure to the sun and keep the PalmCD2 away from sources of magnetic interference.

3.0 Programming with the PC or Laptop

You can use the cable enclosed with the PalmCD2 to connect it directly to a free COM interface on a PC or laptop. If no COM interface is available, you can optionally acquire a special serial USB converter cable from SimonsVoss. (Only this cable has

been tested and approved by SimonsVoss). In this configuration, you can program all digital components directly on the PC.

If you use the same interface (such as COM1) for both the docking station and the PalmCD2, you need to end the HotSync manager first in order to free the serial interface for the PalmCD2. You can set this up so that it happens automatically by selecting the appropriate settings in the Palm user dialog box. You can also click the  symbol in the lower right of the Windows task bar and then click **End**.



You can also match up your personal data with the PalmCD2 by placing your Palm on the PalmCD2, connecting the PalmCD2 to the PC/Laptop and then performing the HotSync process.

4.0 Programming with the Palm Organiser

Create the locking plan with the LDB locking plan software. Program the components on the PC or laptop. When you make changes to the locking plan, the data is transmitted to the Palm Organiser via the docking station (or PalmCD2) so that both computers have the same data stock. Then go to each of the lockings affected by the changes and either read them out or reprogram them from the Palm Organiser with docked PalmCD2. Finally, transmit the new locking system status back to the PC with a new synchronisation process. Refer to the PalmLDB operating instructions for more detailed information.

5.0 Setting Up the PalmCD2 with Transponder Function

You can also use the PalmCD2 as a transponder in your locking system. In this case, the HotSync key functions as the pushbutton. Refer to the chapter on special transponders in the software operating instructions for more details.

6.0 Data Sheet

Battery type	AAA 1.5 V (2x)
Dimensions	120 mm x 70 mm x 20 mm
Degree of protection	IP 20

Caption

State of: June 2006

Explanation of technical terms

Access logging	Additional function of the digital components in the TC version: The digital lockings store the last 128 accesses with date, time of day and user name. The stored accesses can be read out with the help of the <i>Config-Device</i> or PalmCD2 or over the network.
Activation transponder	Can be inserted within the scope of the <i>shunt lock function</i> , so that, in case of an emergency, the deactivation of the lockings can be released when the alarm system is activated. The door can then be opened with an authorised transponder.
Activation unit	See <i>shunt lock function</i>
Central node	Component of the network installation: is connected to the PC using the RS232 interface and represents the central unit of the <i>network</i> .
Deactivation unit	See <i>shunt lock function</i>
Higher priority locking level	If a transponder should lock in more than three different locking systems, one sets up a higher priority transponder.
Locking	General term for digital locking cylinders, digital Smart Relays and shunt lock components.
LockNode	Component of the network installation: LockNodes are installed in the vicinity of a digital locking and are connected to the CentralNode over the network wiring. The data transmission from the LockNode to the digital locking takes place over radio without wires. Using the locking plan software, the lockings can be programmed or read out.
Network	All digital components can be connected to a network and configured and administered from a central PC. A physical approach to the lockings with the SmartCD is then no longer necessary.
Overlay mode	Locking systems with up to 1000 transponders can be operated in the so-called overlay mode. If a transponder should be lost in this case, you simply set up a replacement transponder in the locking plan and program it. Then go to all lockings to which this transponder has authorisation. After the activation of the transponder, the locking recognises that this is a replacement transponder. The old, lost transponder is automatically blocked.

SmartCD	The SmartCD is a programming device that was developed especially for wireless operation with a PDA. It makes it very easy to program and read out all digital components of the System 3060. You can also use the PDA to match up your personal data (addresses, calendar, etc.).
Password transponder	Instead of manually entering the password for the locking plan software, you can also transmit it over radio with the password transponder.
Programming transponder	Use the programming transponder to program Digital Locking Cylinder 3061 and Transponder 3064 devices. You do not need a PC or special system software – simply press a button. For example, you can grant or change access authorisation if you lose a key or make changes to the locking plan in small systems.
Repeater (LON)	The repeater (LON) is used to extend the specified cable length of 900 m (984 m) (BUS) in a segment. This requires that an additional LPI10 also be used.
Router (LON)	The router (LON) is used to separate individual segments, such as floors or buildings, for example, from one another in large networks. Likewise, routers are used as intermediary switches in long network lines.
Shunt lock function	Serves the integration of an alarm system into the System 3060. A deactivation unit must be installed on every door that leads to a security area. The activation unit is installed at a central location and connected to the deactivation units. The alarm system can then be activated and deactivated via the activation unit using an authorised transponder. The signals are forwarded to the deactivation units, which prevent a door from being accidentally opened when the alarm system has been activated.
Switching transponder	This transponder has a two-wire cable connected to the switch contacts of the button. This cable is led to the outside of the device.
Time zone control	Additional function of the digital components in the TC Version: Transponders can be programmed such that they are authorised for the lockings only at predetermined times.
Twisted-Pair	Double wire, twisted cable, used for the network cabling.

Special symbols used in the text

😊 Remark, tip

🔄 Example

👉 Attention

Subject to technical modifications.