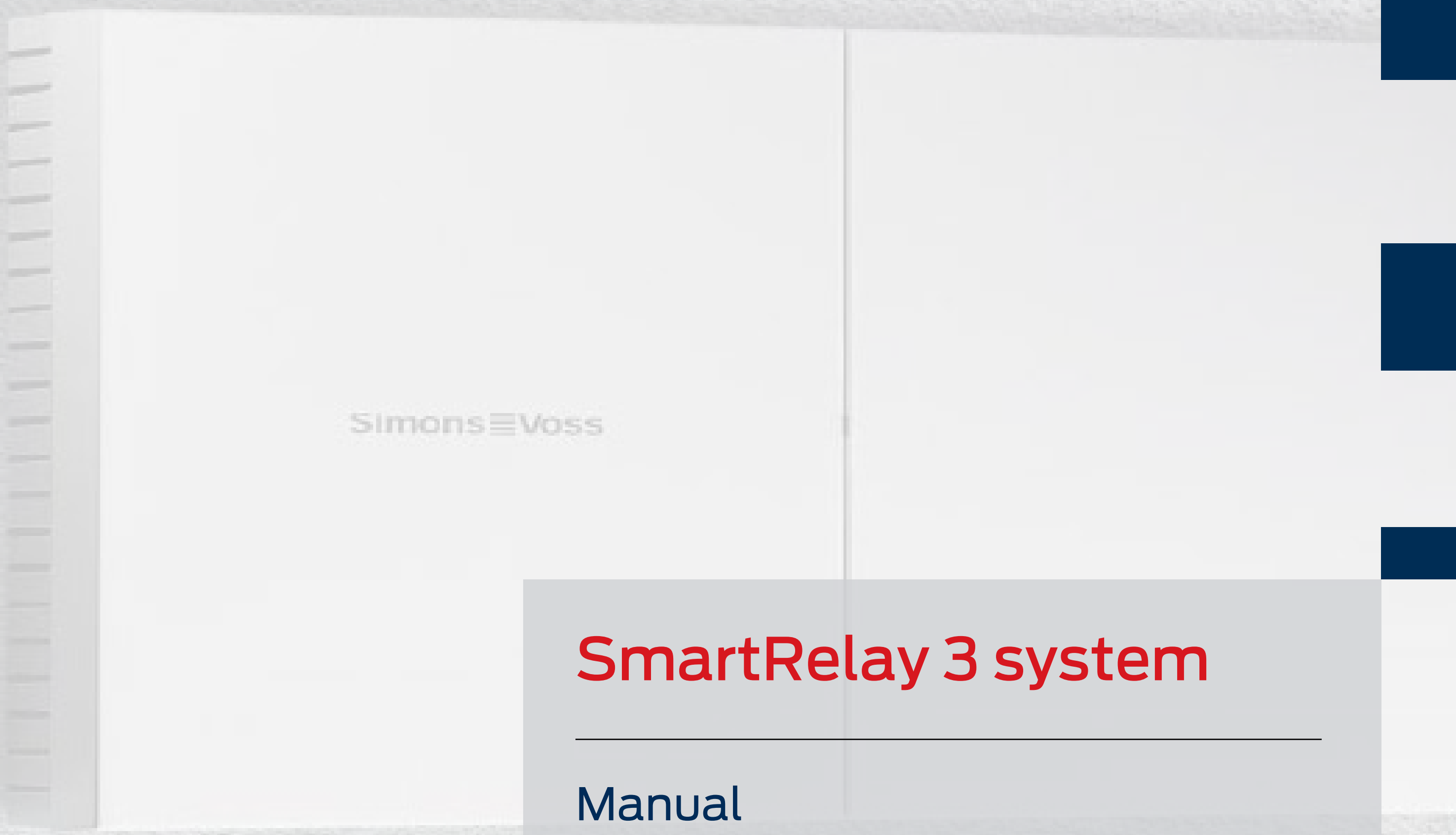


SmartRelay 3 system

Manual

25.03.2025

SimonsVoss technologies

Contents

1. Intended use

In its third generation, the SimonsVoss SmartRelay system (SREL 3 ADV) is a system consisting of several networked components which provide intelligent control of locking devices and third-party systems. The system consists of a controller, at least one external reader and an optional SmartOutput module.

The controller is the main component. A service communicates with the LSM database and provides the controller with the latest information from the database when it is used as a gateway. No manual updates or time-consuming reprogramming are required.

The controller can use information retrieved from the LSM database and identification data transmitted by the reader to verify identification data with the database. Different actions are possible, depending on the settings programmed in the controller, including:

- Assigning authorisations
- Withdrawing authorisations
- Loading time budgets
- Updating identification media configurations
- Switching relay outputs
- Reading lists

Identification media are read by up to three external readers, which may be physically separate from one another and the controller. In the third-generation SmartRelay system, the reader can read active and passive identification media and transmit the information to the controller for evaluation.

The controller features a built-in relay output which can be freely programmed. The system can be extended with SmartOutput modules in a daisy chain featuring up to 116 relay outputs, which are also freely programmable.

2. General safety instructions

Signal word: Possible immediate effects of non-compliance
DANGER: Death or serious injury (likely)
WARNING: Death or serious injury (possible, but unlikely)
CAUTION: Minor injury
IMPORTANT: Property damage or malfunction
NOTE: Low or none

WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

Do not swallow battery. Danger of burns from hazardous substances

This product contains lithium button cell batteries. Swallowing the button cell battery, in can result in severe internal burns leading to death in as little as two hours.

1. Keep new and used batteries away from children.
2. If the battery compartment does not close securely, cease using the product and keep it away from children.
3. If you think batteries have been swallowed or are in any part of the body, seek medical attention immediately.

Risk of explosion due to incorrect battery type

Inserting the wrong type of battery can cause an explosion.

- Only use the batteries specified in the technical data.

CAUTION

Fire hazard posed by batteries

The batteries used may pose a fire or burn hazard if handled incorrectly.

1. Do not try to charge, open, heat or burn the batteries.
2. Do not short-circuit the batteries.

IMPORTANT

Damage resulting from electrostatic discharge (ESD) when enclosure is open

This product contains electronic components that may be damaged by electrostatic discharges.

1. Use ESD-compliant working materials (e.g. Grounding strap).
2. Ground yourself before carrying out any work that could bring you into contact with the electronics. For this purpose, touch earthed metallic surfaces (e.g. door frames, water pipes or heating valves).

Damage resulting from liquids

This product contains electronic and/or mechanic components that may be damaged by liquids of any kind.

- Keep liquids away from the electronics.

Damage resulting from aggressive cleaning agents

The surface of this product may be damaged as a result of the use of unsuitable cleaning agents.

- Only use cleaning agents that are suitable for plastic surfaces.

Damage as a result of mechanical impact

This product contains electronic components that may be damaged by mechanical impacts of any kind.

1. Avoid touching the electronics.
2. Avoid other mechanical influences on the electronics.

Damage as a result of overcurrent or overvoltage

This product contains electronic components that may be damaged by excessive current or voltage.

- Do not exceed the maximum permissible voltages and/or currents.

Damage due to polarity reversal

This product contains electronic components that may be damaged by reverse polarity of the power source.

- Do not reverse the polarity of the voltage source (batteries or mains adapters).

Communication interference due to metallic surfaces

This product communicates wirelessly. Metallic surfaces can greatly reduce the range of the product.

- Do not mount or place the product on or near metallic surfaces.

NOTE

Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SimonsVoss products for any other purposes.

Malfunctions due to poor contact or different discharge

Contact surfaces that are too small/contaminated or different discharged batteries can lead to malfunctions.

1. Only use batteries that are approved by SimonsVoss.
2. Do not touch the contacts of the new batteries with your hands.
3. Use clean and grease-free gloves.
4. Always replace all batteries at the same time.

Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to ± 15 minutes per year.

- Regularly reprogram time-critical locking devices.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

Incorrect installation

SimonsVoss Technologies GmbH accepts no liability for damage caused to doors or components due to incorrect fitting or installation.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

3. Product specific safety notices

DANGER

Risk of injury due to incorrect programming

The SREL3 ADV system is not suitable to replace existing security installations.

1. Ensure that the SREL3 ADV system is used as an additional securing measure only.
2. Do not replace existing security installations with the SREL3 ADV system.

CAUTION

Risk of burns due to hot circuit board

The circuit board can become very hot if PoE is used (power supply over Ethernet).

- Let the controller cool down before you open the housing.

IMPORTANT

Unauthorised access

The relay in the controller can be short-circuited by unauthorised persons.

- Mount the controller with the relay in an environment that is protected against unauthorised access.

Unauthorised switching of the relay by magnet

The relay can switch unintentionally due to strong magnets nearby.

1. Mount the controller with the relay in an environment that is inaccessible to unauthorised persons with magnets.
2. Alternatively, operate the relay permanently activated (invert output and use NC+COM instead of NO+COM).

4. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

Example	button
☑ Example ☐ Example	checkbox
◉ Example	Option
[Example]	Tab
"Example"	Name of a displayed window
| Example |	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
Example	Field
Example	Name of a (Windows) service
Example	Commands (e.g. Windows CMD commands)
`Example`	Database entry
[Example]	MobileKey type selection

5. System description

5.1 Controller

The SREL3 ADV system is connected to the network via Ethernet. The Ethernet connection is PoE-capable, so an external power supply unit is not essential.

It is possible to use the system as a gateway in the virtual network. The controller establishes a connection to the VN host server to do so. The VN host server forwards changed authorisations (programming requirement) and data from the LSM database to the controller. This means that complete, time-consuming loading of the database is no longer required; instead, the controller collects the provided data when an identification medium is detected (pull principle). The entire system is programmed via a single interface – the controller.

The SREL3 ADV is also available in a ZK variant, which extends the system's functions to include time zone control and event logging (access lists).

Three available screw terminal inputs ensure that the controller is flexible in its use.

- Forwarding to LSM (Inputs 1 and 2)
- Push-to-open contact (Input 3)

The built-in screw terminal relay output can activate any system and open an electric door, for example.

An IP address needs to be issued using USB when the controller is programmed for the first time. Once the IP address is issued, a USB connection is no longer needed. The controller's configuration can be modified over the network instead.

The built-in backup battery ensures that the programmed settings are maintained after a power failure and guarantees that the controller continues to function without any limitations once power is restored.

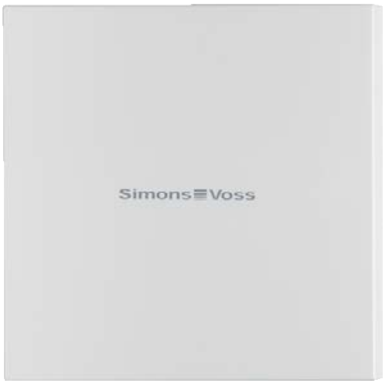
NOTE

Follow the switch-on sequence

After a power-on reset (power outage followed by restoration of power supply), the controller automatically searches for connected system components one time on restarting. System components which are not supplied power until the controller restarts are thus unable to respond to the controller's query and are not recognised.

The controller must therefore be supplied power with the other system components at the same time or must be the last system component to receive power.

5.2 Reader



At least one external reader is required to use the SREL3 ADV system. SmartRelay 3 readers are ordered separately from the controller.

The controller is unable to read identification media. Up to three readers can be connected via an RS-485 interface for this purpose. They can read both active and passive identification media. After reading media, the readers transmit the data to the controller, which checks the identification medium's authorisation and triggers relevant actions as programmed. The reader itself is unable to trigger actions and can thus be installed in less protected areas. In the WP variant, the housing is sealed and protected against splashing water.

Readers can either be powered through the controller or equipped with their own power supply unit.

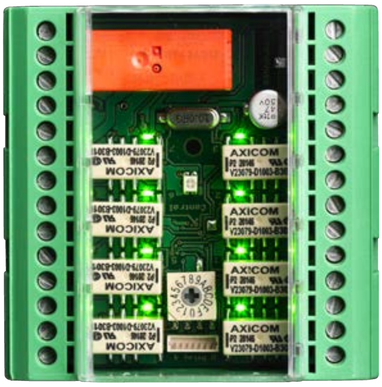
NOTE

Too low operating voltage

When selecting the power supply, please allow for a voltage drop occurring in conductors. A voltage drop can cause the operating voltage in the reader to fall below the required level and malfunctions may occur. In such a case, either the operating voltage on the controller needs to be increased or the reader equipped with its own power supply unit.

A multi-coloured LED signals the different operating modes.

5.3 SmartOutput module



SmartOutput modules are ideal complements to controllers if more than one relay output is required. Every SmartOutput module is equipped with eight relays, which each feature a change-over contact. SmartOutput modules can be connected in parallel to one another and fitted on a DIN rail (35 mm x 7.5 mm).

Up to 15 modules can be connected. Only four outputs are available on module 15 (up to 116 additional outputs in total).

A multi-coloured LED signals the different operating modes.

NOTE

Follow the switch-on sequence

After a power-on reset (power outage followed by restoration of power supply), the controller automatically searches for connected system components one time on restarting. System components which are not supplied power until the controller restarts are thus unable to respond to the controller's query and are not recognised.

The controller must therefore be supplied power with the other system components at the same time or must be the last system component to receive power.

5.4 Versions

Several improvements have been made for the newly launched SREL 3 ADV compared to its predecessor:

Comparison between SmartRelay 2 and SmartRelay 3

	SmartRelay 2	SmartRelay 3 Advanced
Duration of data transmission to the gateway	Depending on the data volume (push principle)	Immediate (pull principle)
Interfaces	Wiegand, 33 bit Wiegand, 26 bit Primion Siemens Cerpass Kaba Benzing Gantner Legic Isgus	Wiegand, 33 bit Wiegand, 26 bit Primion Siemens Cerpass Kaba Benzing Gantner Legic Isgus
Components required for networking	Controller Reader LockNode Router	Controller Reader
Networking	LockNode	Ethernet (integrated)
Power supply	9–24 VDC	9-32 VDC PoE
Number of relay contacts	1	Up to 116+1 (with SmartOutput modules)
Number of external readers	Max. 2	Max. 3
Programming	SmartCD	Ethernet USB (with power adapter)

5.5 Accessories

You can adapt the SREL3 ADV system to different purposes with optional accessories. The following accessories can be ordered:

Order code	Name	Purpose
MOD.SOM8	SmartOutput module	The SmartOutput module increases the number of switchable relay outputs to up to 116+1 outputs.
POWER.SUPPLY.2	Power supply unit (12 V_{DC}, 500 mA)	This power supply unit can be used to power the controller.
SREL2.COVER1	Anti-vandalism housing	Fastened with special screws, this housing is also suitable for the SREL3 ADV system. It protects the SREL3 ADV system reader against the weather and vandalism.

6. System requirements

LSM 3.3 SP2 or higher (Basic Online, Business or Professional) is required to programme SmartRelay 3.

The VN host must be installed and running, so that the controller can retrieve data and programming requirements from the database via the VN host in gateway mode.

The controller requires a TCP/IP connection to the server for operation:

- 10/100 MB/s
- Latency typ. < 10 ms

Connection to faster networks is possible provided they are backwards-compatible.

.NET-Framework Version 4.0 or higher must be installed to use the CommNode or VN host server.

If LSM Basic Online is used with a virtual network, then LSM Basic Online must be run in administrator mode.

7. Connections

NOTE

Fault through electromagnetic fields

Signals on the connection cable between reader and controller are influenced externally by electromagnetic fields. A shielded cable reduces the influence of disruptive signals from outside.

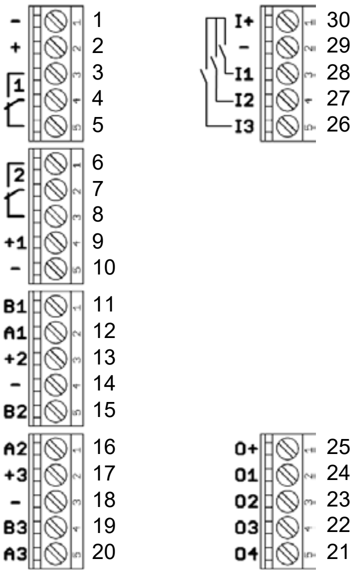
- Use a shielded cable.

Ground loop through shielding

Remote devices may have a slightly different ground potential. A shield connected on both sides represents a second ground connection through which this potential difference is compensated. The resulting current flow can interfere with the data transfer.

- Only connect the screen on one side to the common ground potential, e.g. on the reader (WP variant: Shield is led out on reader side together with ground).

7.1 Controller

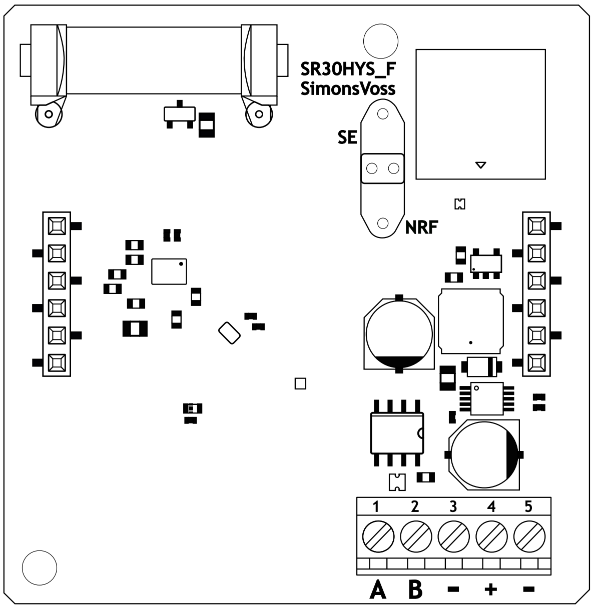


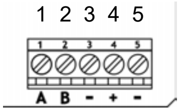
No.	Circuit board	Explanation
1	–	GND Optional connection of an external power supply (ground).
2	+	V_{IN}. Connection of an external power supply (positive pole).
3		Relay 1: NO (Normally Open). This contact is connected to C when the relay switches.

No.	Circuit board	Explanation
4		Relay 1: C (Common). Common connection of the changeover contacts.
5		Relay 1: NC (Normally Closed). This contact is disconnected from C when the relay switches.
6		Relay 2: NO (Normally Open). This contact is connected to C when the relay switches. Availability in the controller depends on the firmware.
7		Relay 2: C (Common). Common connection of the changeover contacts. Availability in the controller depends on the firmware.
8		Relay 2: NC (Normally Closed). This contact is disconnected from C when the relay switches. Availability in the controller depends on the firmware.
9	+1	Reader 1: Power supply. Voltage corresponds to V_{IN} - 1 V or 12 V - 1 V (PoE).
10	-	Reader 1: GND
11	B1	Reader 1: Data line B.
12	A1	Reader 1: Data line A.
13	+2	Reader 2: Power supply. Voltage corresponds to V_{IN} - 1 V or 12 V - 1 V (PoE).
14	-	Reader 2: GND
15	B2	Reader 2: Data line B.
16	A2	Reader 2: Data line A.
17	+3	Reader 3: Power supply. Voltage corresponds to V_{IN} - 1 V or 12 V - 1 V (PoE).
18	-	Reader 3: GND
19	B3	Reader 3 / SmartOutput module: Data line B.
20	A3	Reader 3 / SmartOutput module: Data line A.
21	04	Serial interface: Open drain, data line 4.
22	03	Serial interface: Open drain, data line 3.
23	02	Serial interface: Open drain, data line 2.
24	01	Serial interface: Open drain, data line 1.
25	0+	Serial interface: Power supply. Voltage corresponds to V_{IN} - 1 V or 12 V - 1 V (PoE).

No.	Circuit board	Explanation
26	I3	Input 3: Push to open. The relay switches as soon as this contact is connected to I+ (contact 30).
27	I2	Input 2: Connection of external components.
28	I1	Input 1: Connection of external components.
29	–	Output: GND
30	I+	Output: Power supply. Voltage corresponds to V_{IN} - 1 V or 12 V - 1 V (PoE).

7.2 Reader





Reader connection	SREL3 controller connection	Signal
A	A1/A2/A3	RS-485: Data line A
B	B1/B2/B3	RS-485: Data line B
–	–	GND. Used to establish the common ground reference potential for the data lines. Any ground connection to the SREL3 controller.

Reader connection	SREL3 controller connection	Signal
+	+	V_{IN}. Connection for power supply (external or via controller).
-	- (optional)	GND. Connection for external power supply. Electrically connected to reader port 3. Only required with external power supply.

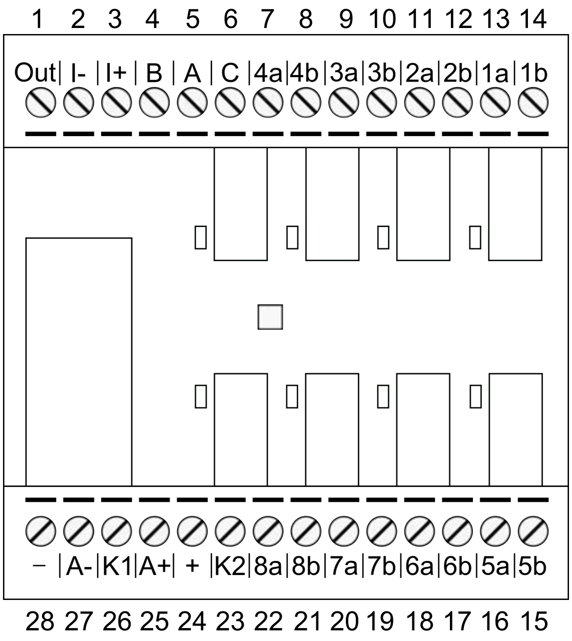
WP version

The weatherproof WP version of the reader is supplied with a 2 m long, pre-assembled cable.

Reader connection	Wire colour in cable	SREL3 controller connection	Signal
A	yellow	A1/A2/A3	RS-485: Data line A
B	brown	B1/B2/B3	RS-485: Data line B
-	green	-	GND. Used to establish the common ground reference potential for the data lines. Any ground connection to the SREL3 controller.
	black (brought out only on the reader's end)	-	GND. Connection of the cable shielding to the common ground reference potential of reader and controller.
+	white	+	V_{IN}. Connection for power supply (external or via controller).

Reader connection	Wire colour in cable	SREL3 controller connection	Signal
-		- (optional)	GND. Connection for external power supply. Electrically connected to reader port 3. Only required with external power supply.

7.3 SmartOutput module


1 2 3 4 5 6 7 8 9 10 11 12 13 14
Out | I- | I+ | B | A | C | 4a | 4b | 3a | 3b | 2a | 2b | 1a | 1b
– | A- | K1 | A+ | + | K2 | 8a | 8b | 7a | 7b | 6a | 6b | 5a | 5b
28 27 26 25 24 23 22 21 20 19 18 17 16 15

No.	Circuit board	Explanation
1	Out	Brownout detection: Open collector, connected to GND if supply voltage is sufficient. This output activates if the supply voltage at V_{IN} falls below 10.0 V_{DC} (±0.5 V_{DC}). The earth connection is usually connected to the AUX relay's coil. If the supply voltage falls at V_{IN}, the AUX relay activates before the other relay contacts activate unchecked due to the decreasing voltage. When the supply voltage is applied, the output does not activate until the module has fully initialised and relay contacts can no longer switch unchecked.

No.	Circuit board	Explanation
2	I-	Isolated digital input. Currently not in use.
3	I+	Isolated digital input. Currently not in use.
4	B	Controller connection: Data Line B; connected to contact for Reader 3.
5	A	Controller connection: Data Line A; connected to contact for Reader 3.
6	C	Controller connection: Earth; connected to contact for Reader 3.
7	4a	Relay 4: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
8	4b	Relay 4: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
9	3a	Relay 3: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
10	3b	Relay 3: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
11	2a	Relay 2: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
12	2b	Relay 2: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
13	1a	Relay 1: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
14	1b	Relay 1: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
15	5b	Relay 5: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
16	5a	Relay 5: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
17	6b	Relay 6: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
18	6a	Relay 6: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
19	7b	Relay 7: Potential-free contact (NC treated as NO in software); activated depending on authorisations.

No.	Circuit board	Explanation
20	7a	Relay 7: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
21	8b	Relay 8: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
22	8a	Relay 8: Potential-free contact (NC treated as NO in software); activated depending on authorisations.
23	K2	AUX relay: Potential-free contact (NO). Contact is connected with K1 (number 26) if coil is connected to power. Equipped with a detachable bridge to + (number 24) ex works.
24	+	V_{IN}. Connection for power supply. Equipped with a detachable bridge to K2 (number 23) ex works.
25	A+	AUX relay: Coil's plus connection. AUX relay activates if coil is connected to power. Equipped with a detachable bridge to K1 (number 26) ex works.
26	K1	AUX relay: Potential-free contact (normally open contact). Contact is connected with K2 (number 23) if coil is connected to power. Equipped with a detachable bridge to A+ (number 25) ex works.
27	A-	AUX relay: Coil's minus connection. AUX relay activates if coil is connected to power.
28	-	GND. Connection for power supply.

8. Setting up

8.1 Unpacking and system test

Scope of delivery

Check to ensure the supply package is complete after receiving it. Unless agreed otherwise, the supply package contains the following components:

Controller

Controller	1x
Instruction leaflet	1x

Reader

Reader	1x
Instruction leaflet	1x

SmartOutput module

SmartOutput module	1x
Jumpers (pre-assembled)	2x
Instruction leaflet	1x

System test

You can check the supplied components to ensure they function correctly before installation and programming. Proceed as follows:

1. Wire the components (see *wiring [▸ 58]*).
2. Connect the components to the power supply (connect the controller last).
3. Wait a few seconds until all components are ready for operation.
   ↳ Controller flashes all colours first and then green.
   ↳ Reader flashes all colours first, beeps and then no longer flashes.
   ↳ Optional SmartOutput module: Relay contacts are open (indicated by LEDs and a tick-tack sound), then flashes green.
4. Use an identification medium on the reader (empty transponders or empty DESFIRE card).

↳ Reader flashes green twice and beeps.
↳ The relay built into controller actuates (Contacts 3, 4 and 5).

8.2 Configuration

You can use the LSM software to programme and configure the controller and the SREL3 ADV system. Other SREL3 ADV system components do not need to be programmed.

NOTE

Initial programming via USB

The controller can be addressed via TCP/IP. However, no IP address is configured in storage mode. That is why initial programming, during which an IP address is assigned, must be carried out with a USB connection.

- ✓ Components connected to power.
- ✓ Controller connected to computer with USB cable.
- ✓ Reader connected to the controller (see *wiring [▸ 58]*).
- ✓ LSM installed and launched as administrator.
- ✓ System requirements met.
- ✓ Communication nodes set up (VN Host and CommNode; see LSM manual).

1. Create a new G2 locking system.
2. Click on the ... button to open the locking system settings.
3. Change to the [G2 card management] tab.
4. Open the ▼ **Card type** drop-down menu.
5. Select your card type.
6. Open the ▼ **Configuration** drop-down menu.
7. Select a configuration.

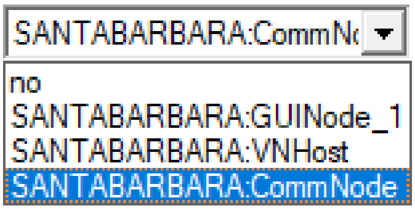
NOTE

Suitable configurations

AV configurations are the only suitable ones for use in a locking system with an SREL3 ADV system.

8. Click on the Apply button.
9. Click on the Exit button.
   ↳ Matrix screen is visible again.
10. Create a new G2 Smart Relay 3 locking device.
11. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
12. Select the [IP settings] tab (see *Establishing IP settings [▸ 28]* for help on IP settings).
13. Enter an IPv4 address.
14. Enter an IPv4 subnet mask.
15. Open the ▼ **Communication nodes** drop-down menu.

16. Select a suitable communication node. If you haven't yet created a communication node for the service, you need to add one first. See *Creating a communication node [▸ 29]*.



NOTE

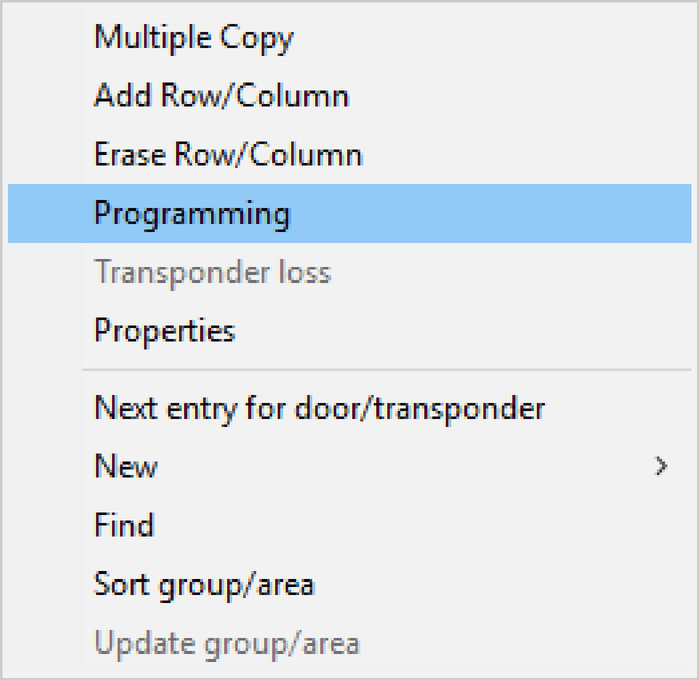
Selecting the communication node

If you are using a CommNode server and a VN host server (use of tasks or events in addition to the virtual network), then choose the CommNode server entry here.

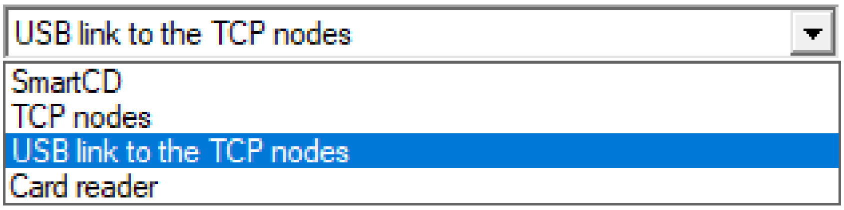
If you want to use a VN host server (use of the virtual network), then select the VN host entry here.

If you do not wish to use either, then select the GUI node entry here.

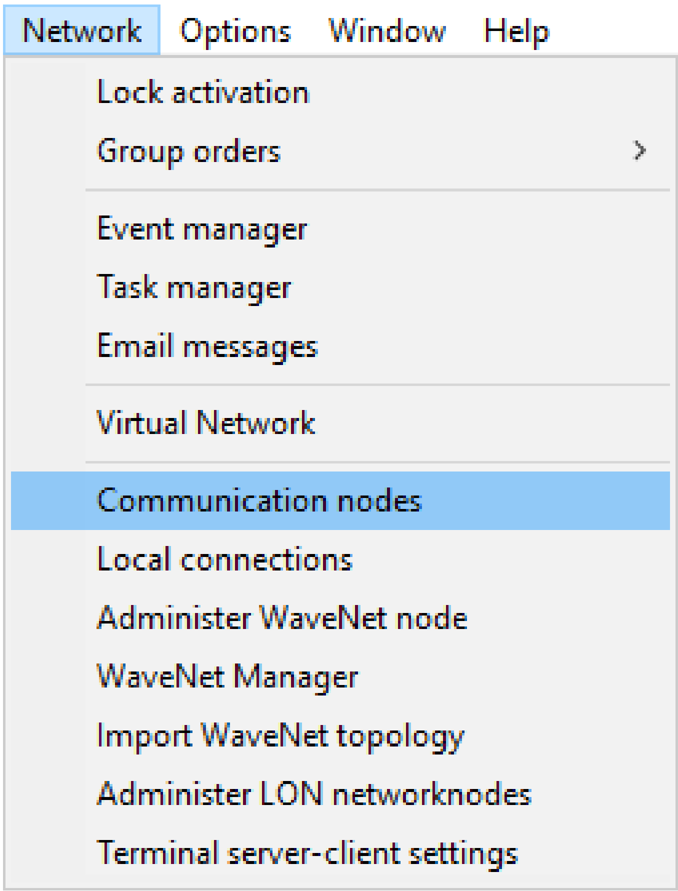
17. Click on the Apply button.
18. Click on the Exit button.
19. Right-click on the SmartRelay 3 entry in the matrix to open the context menu.
20. Select the Programming entry.



21. Select "USB link to the TCP nodes" in the programming window.



22. Click on the Programming button.
    ↳ Programming launches.
23. Wait for programming.
24. Use | Network | to select the Communication nodes entry.



25. If you have created more than one communication node, change to the communication node you have just created. Use the ▸ or ⏭ and ◂ or ⏮ buttons.
26. Terminate the *SimonsVoss VNHost Server* or *SimonsVoss CommNode Server* service.
27. Click on the Config files button.
28. Open Windows services.
29. Save the service's configuration files locally on your computer.

30. Copy the configuration files saved locally and add them to the service's installation folder (default: C:\Programme (x86)\SimonsVoss\VNHost or C:\Program Files (x86)\SimonsVoss\CommNodeSvr_3_4).

NOTE

All three XML files must be copied directly to the installation folder, not to a sub-folder.

31. Launch the *SimonsVoss VNHost Server* or *SimonsVoss CommNode Server* service again.

NOTE

Click on the Ping button to check whether the service is running and responding. If the service responds, you can continue. If it does not, try to launch the service again.

32. Click on the Transmit button in LSM.
    ↳ Controller can be reached via network.
33. Terminate the *SimonsVoss VNHost Server* and *SimonsVoss CommNode Server* services.
34. Create your backup again (see LSM manual).
35. Launch the *SimonsVoss VNHost Server* and *SimonsVoss CommNode Server* services again.

↳ Controller can be reached via network and flashes blue.

8.2.1 Establishing IP settings

The SREL3 ADV system controller needs a static IPv4 address to operate in the network. Ask your IT Department or your network administrator to assign you a free static IPv4 address and provide you with the following information:

- IPv4 address
- Associated subnet mask
- Default gateway (only if not all LSM or System 3060 devices are in the same network)

Alternatively, you can also use DHCP with LSM Version 3.4 SP1 and above. To do so you need to open the [IP settings] tab and enable the ☑ DHCP activated checkbox.

8.2.2 Creating a communication node

✓ LSM launched.

1. Use | Network | to select the Communication nodes item.
2. Enter the communication node name (freely selectable; recommended: VN host or CommNode).
3. Enter the host name of the computer on which *SimonsVoss VNHost Server* has been installed.

NOTE

You can verify the host name as follows:

1. Press the Windows key.
2. Enter cmd.
3. Press the Enter key to confirm.
   ↳ The "Command" window will open.
4. Enter *hostname*.
5. Press the Enter key to confirm.

↳ The computer's host name is displayed.

4. Enter the full computer name (fully qualified domain name).

NOTE

It only needs to be entered if the system is working with LSM clients or database servers in different domains. The FQDN comprises the local computer name and the domain, e.g. COMPUTER.NETWORK.LOCAL. You can verify the domain yourself:

1. Press the Windows key.
2. Enter cmd.
3. Press the Enter key to confirm.
   ↳ The "Command" window will open.
4. Enter *echo %userDNSdomain%*.
5. Press the Enter key to confirm.

↳ The computer's domain is displayed.

5. Click on the Apply button.

↳ The communication node is created.

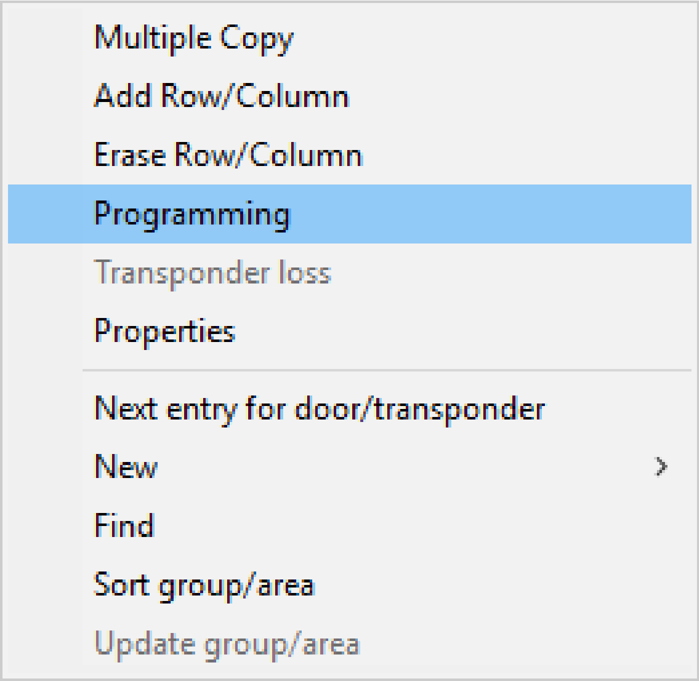
8.3 Programming

Programming does not differ from programming for other locking devices. The SREL3 ADV system can be programmed using either a USB cable or a network connection (except initial programming).

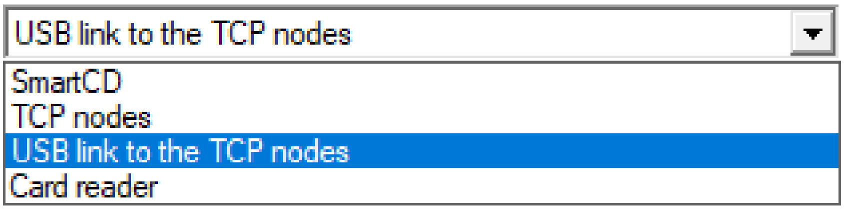
USB programming

- ✓ Controller connected to computer with USB cable.
- ✓ Components connected to power.

1. Right-click on the SmartRelay 3 entry in the matrix to open the context menu.
2. Select the Programming item.



3. Open the ▼ **Type** drop-down menu.
4. Select the "USB link to the TCP nodes" item.



5. Click on the Programming button.

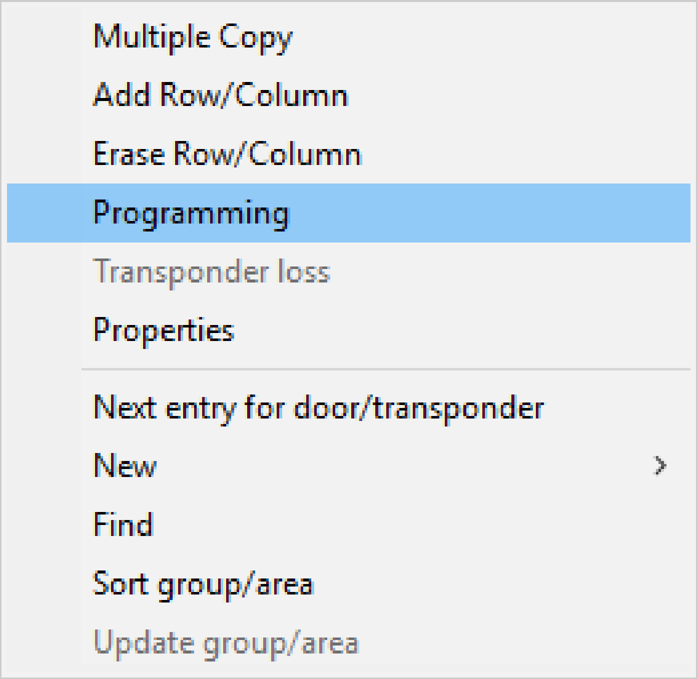
↳ Programming launches.

Network programming

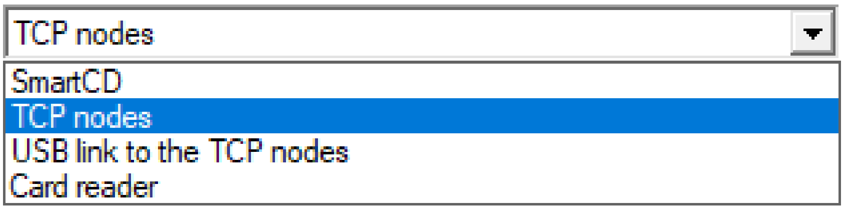
- ✓ Controller has already been programmed.
- ✓ Controller connected to computer via network.
- ✓ Components connected to power.

1. Right-click on the SmartRelay 3 entry in the matrix to open the context menu.

2. Select the Programming item.



3. Open the ▼ **Type** drop-down menu.
4. Select the "TCP nodes" item.



5. Click on the Programming button.

↳ Programming launches.

8.3.1 Adding SmartOutput modules

The SREL3 ADV system controller searches for SmartOutput modules after a power supply has been connected. The controller detects connected SmartOutput modules when they are supplied electricity.

Programming requires that the number of SmartOutput modules detected match the number indicated in LSM. You can add SmartOutput modules as follows.

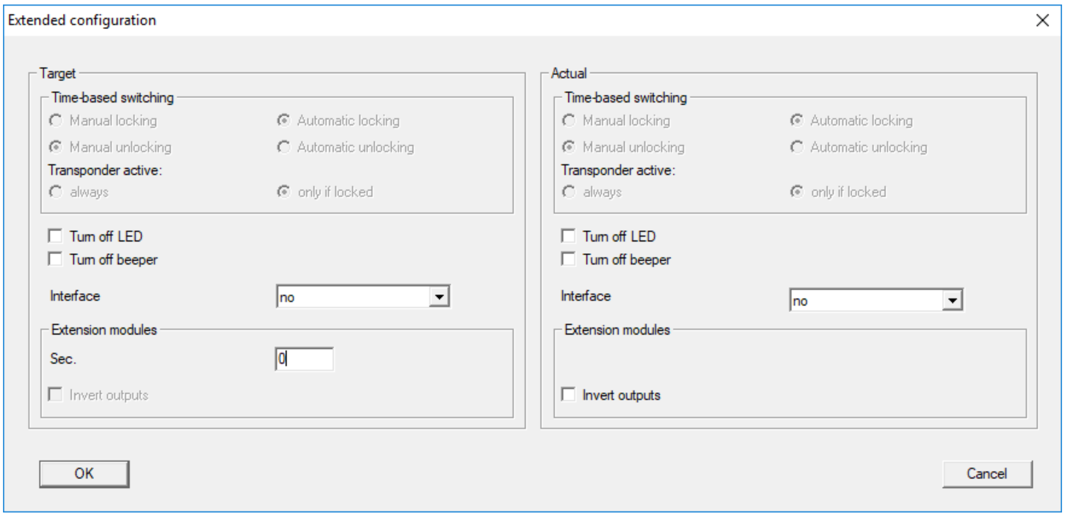
✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

✓ Controller reset (see *Resetting the controller [▸ 33]*).

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.

2. Change to the [Configuration/Data] tab.
3. Click on the Extended configuration button.
   ↳ "Extended configuration" window will open.



Extended configuration

Target

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

Sec.: 0

□ Invert outputs

Actual

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

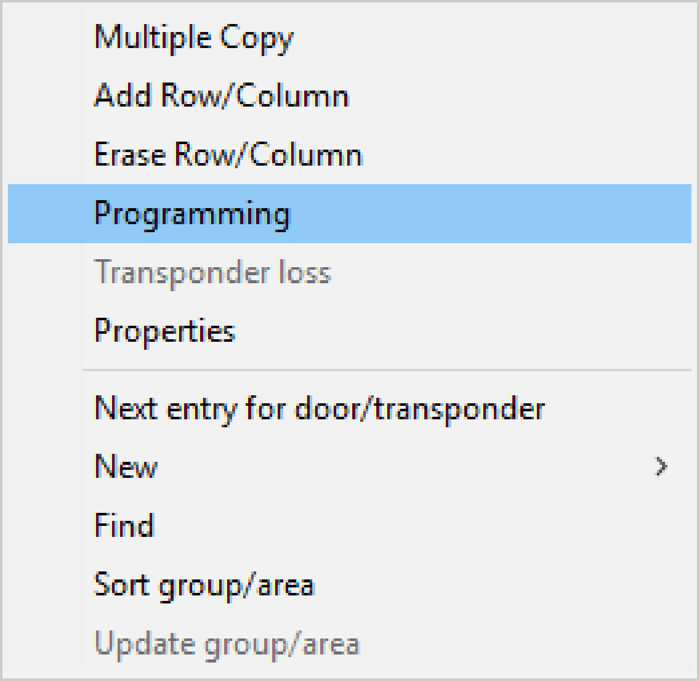
Interface: no

Extension modules

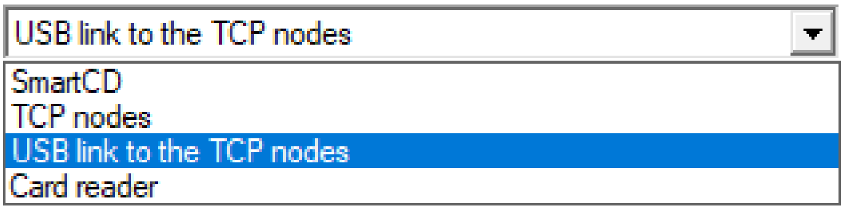
□ Invert outputs

OK Cancel

4. Enter the number of connected SmartOutput modules in the "Extension modules" area.
5. Click on the OK button.
   ↳ Window closes.
6. Click on the Apply button.
7. Click on the Exit button.
   ↳ LSM returns to the matrix.
8. Right-click on the SmartRelay 3 entry in the matrix to open the context menu.
9. Select the Programming item.



10. Open the ▼ **Type** drop-down menu.
11. Select the "USB link to the TCP nodes" item.



12. Click on the Programming button.

↳ Programming launches.

8.3.2 Resetting the controller

You need to reset the controller when changes are made to the connected components. These include:

- SmartOutput modules added
- SmartOutput modules removed
- Readers added
- Readers removed

A reset deletes the programmed settings.

NOTE

Only the hardware settings and access lists on the controller are reset. The IP setting remains unchanged

except for the IP settings made during initial programming. The controller can still be reached using the saved IP address. This means you do not necessarily need to establish a connection with a USB cable.

8.3.2.1 Resetting controller with a USB cable

The controller can be reset with a USB cable. This option is ideal if the controller has not yet been installed and can simply be reached physically.

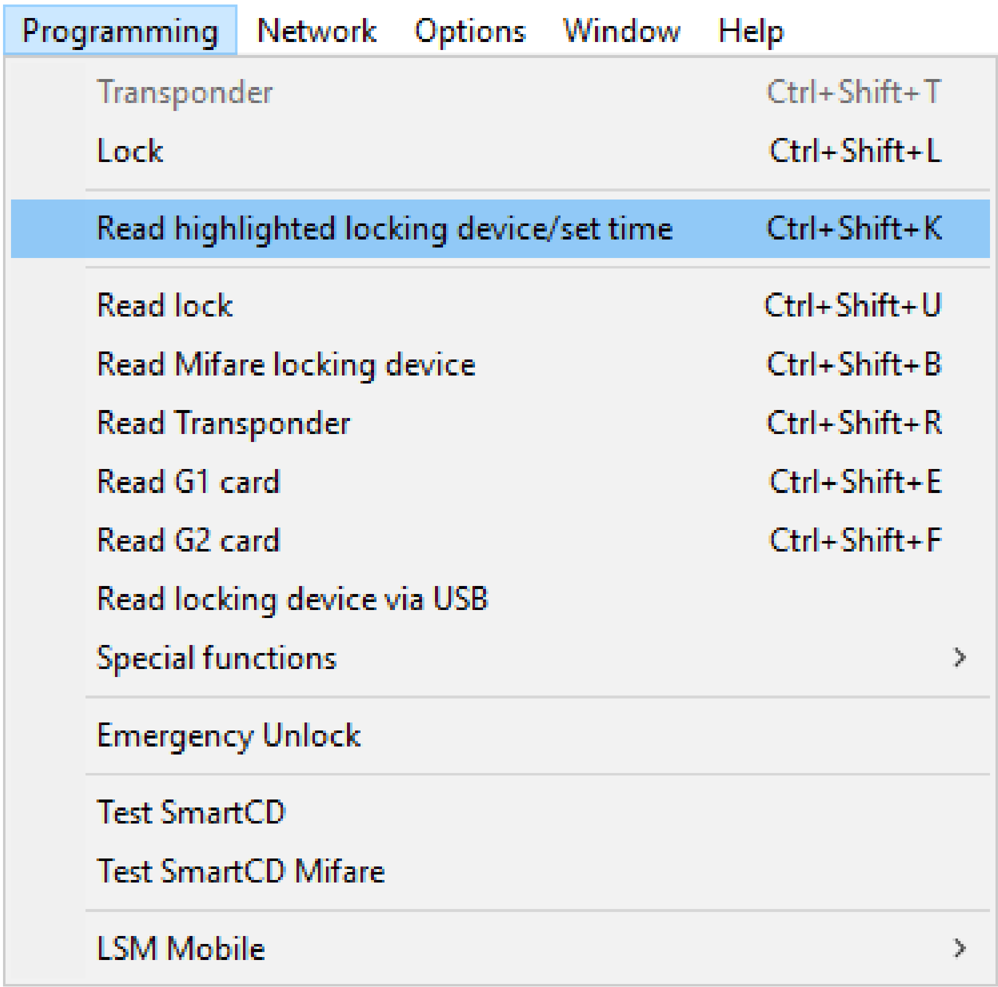
✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

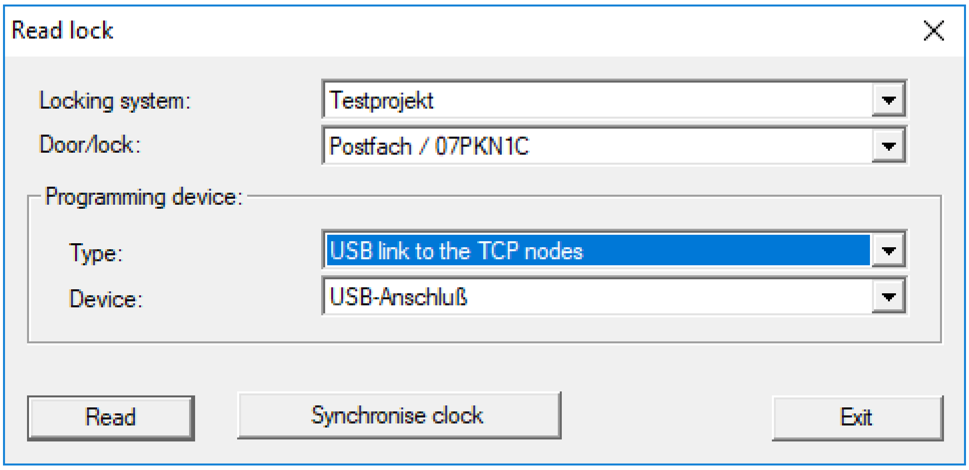
✓ Controller connected to computer with USB cable.

1. Mark the entry on the SmartRelay 3 controller in the matrix.

2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile

↳ The "Read lock" window will open.



Read lock

Locking system: Testprojekt

Door/lock: Postfach / 07PKN1C

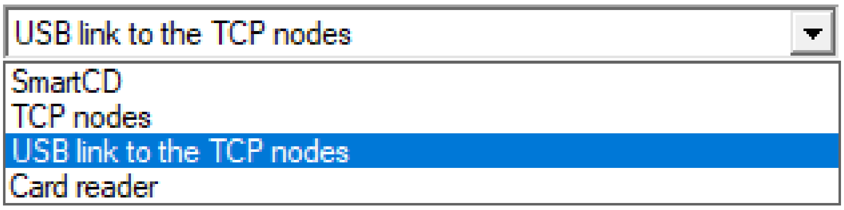
Programming device:

Type: USB link to the TCP nodes

Device: USB-Anschluß

3. Open the ▼ **Type** drop-down menu.

4. Select the "USB link to the TCP nodes" item.



5. Click on the Read button.
   ↳ Locking device is read.
   ↳ The "G2 Smart Relay 3" window will open.
6. Click on the Reset button.
   ↳ The "Reset lock" window will open.
7. Enter the locking system password or apply it from the database.
8. Click on the Reset button.
   ↳ Locking device is reset.

↳ Locking device reset.

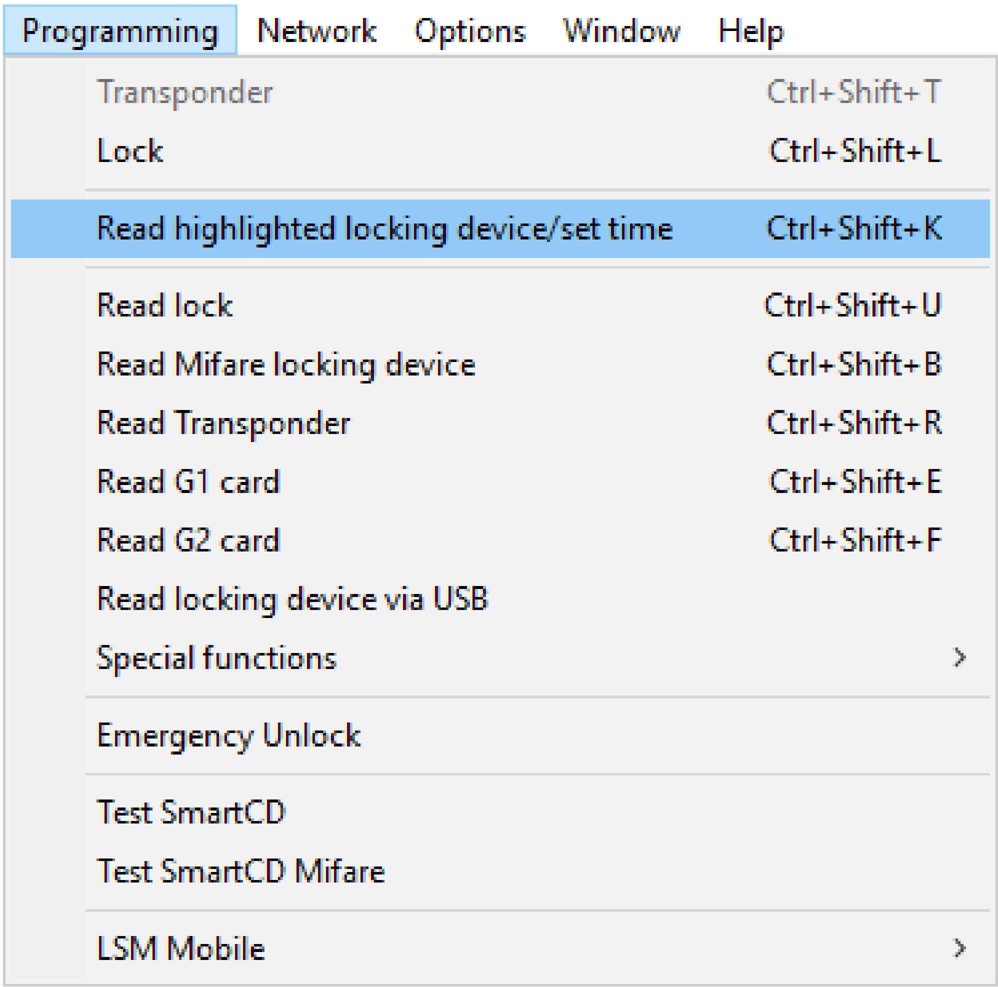
8.3.2.2 Resetting controller over the network

Alternatively, the controller can also be reset over the network after initial programming. This option is ideal if the controller has already been installed and cannot be reached physically.

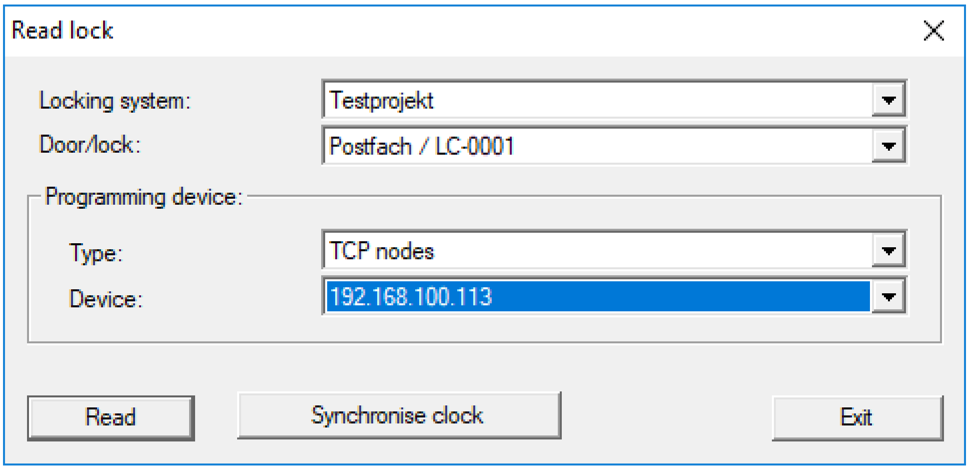
✓ Components wired correctly (see *wiring [▸ 58]*).
✓ Components connected to power.
✓ Controller has already been programmed.
✓ Controller connected to computer via network.

1. Mark the entry on the SmartRelay 3 controller in the matrix.

2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions ›
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile ›

↳ The "Read lock" window will open.


Read lock

Locking system: Testprojekt

Door/lock: Postfach / LC-0001

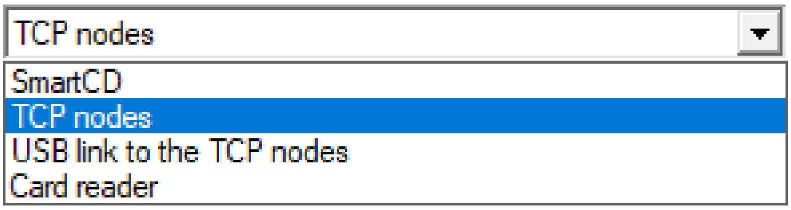
Programming device:

Type: TCP nodes

Device: 192.168.100.113

3. Open the ▼ **Type** drop-down menu.

4. Select the "TCP nodes" item.



5. Click on the Read button.
   ↳ Locking device is read.
   ↳ The "G2 Smart Relay 3" window will open.
6. Click on the Reset button.
   ↳ The "Reset lock" window will open.
7. Enter the locking system password or apply it from the database.
8. Click on the Reset button.
   ↳ Locking device is reset.

↳ Locking device reset.

8.4 Application examples

This section explains the interplay between components in the SREL3 ADV system and shows a few use cases as an example.

IMPORTANT

Overload in a fitted relay

The permitted current and permitted voltage must not be exceeded.

1. Observe the specifications (see *Properties [▸ 166]*).
2. Ensure that the load on the relay is not plugged into a different element or has been increased in some other way.

8.4.1 Basic principle

The SmartRelay 3 system always comprises of a controller, at least one reader and optional SmartOutput modules.

The reader is not able to evaluate detected identification media for security reasons. The communication between the reader and controller is secured. The reader can thus also be installed in unsecured areas without any problems.

8.4.2 Gateway function

The SREL3 ADV system can also be used as a gateway for the virtual network, no matter whether a relay contact is used or not. Any identification medium which is logged onto one of up to three readers is updated. In doing so, a difference must be made between network-dependent and network-independent functions.

Network-independent

- Loading time budgets: Users are able to re-upload their time budgets at any time without the network.
- Automatic blacklist distribution: IDs which have already been flagged for blocking in the controller are also distributed in the virtual network without a network connection.

Partially network-independent

When the network connection is re-established, the controller transmits information which was collected during the outage:

- Feedback signals from blacklist broadcasts: Locking devices which have received authorisation changes for transponders emit a feedback signal. This feedback signal is transmitted to the controller via the virtual network.
- Battery warnings: Locking devices which have low batteries transmit a battery warning to the controller via the identification media in the virtual network.
- Physical access lists: The smart card physical access list are read and saved by the controller independently of the network.

Network-dependent

If there is a network connection, other virtual network functions are available on the gateway:

- Issuing of individual authorisations: When an identification medium has logged on, the controller retrieves the latest authorisation information for the transponder concerned from the VN host server via the network. The authorisation changes are updated on the transponder via the reader if necessary.
- Configuration changes: The controller retrieves configuration changes to identification media, such as a time group change, from the VN host server.
- Issuing of individual blacklist IDs: Up to two IDs to be blocked can also be added to selected identification media in the virtual network. To do so, the controller retrieves the IDs to be blocked from the VN host server when such an identification medium logs on.

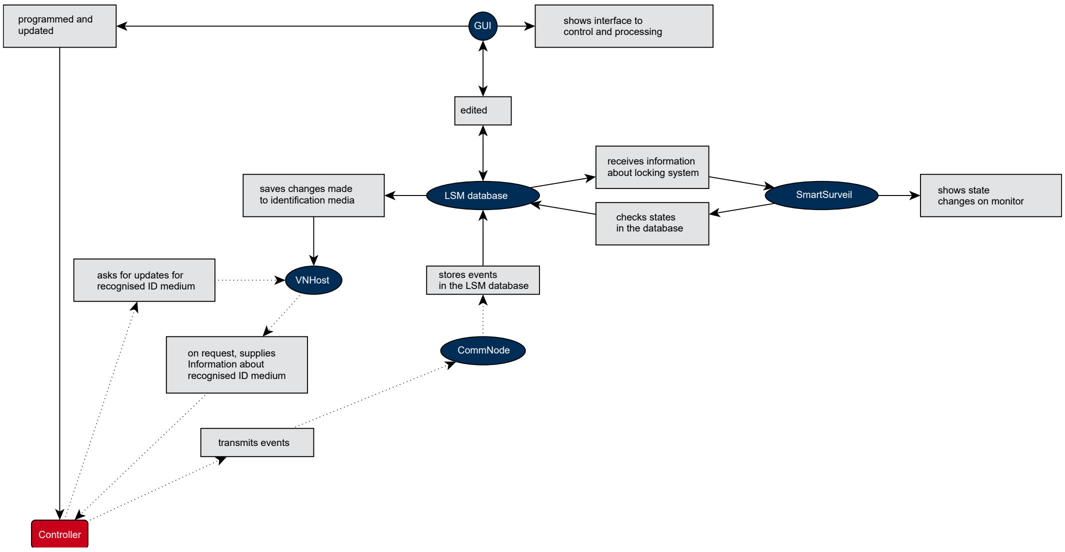
8.4.3 General overview

Controller communication with LSM

The controller does not communicate directly with the database. A distinction must be made with communication between the controller and the database:

- Use in the virtual network: The controller is programmed by LSM and also requests information itself from the VN host using the detected ID medium.
- Use without virtual network: The controller does not request information itself on its own. Changes need to be programmed.

Events on the controller such as a pressed button are transmitted to the LSM database via the CommNode.


programmed and updated
GUI
shows interface to control and processing
edited
receives information about locking system
saves changes made to identification media
LSM database
SmartSurveil
shows state changes on monitor
checks states in the database
asks for updates for recognised ID medium
VNHost
stores events in the LSM database
CommNode
on request, supplies Information about recognised ID medium
transmits events
Controller

Controller communication with the components

A user can log onto up to three readers with an ID medium. The reader forwards encrypted information to the controller, which is located within a protected area. The controller evaluates the information:

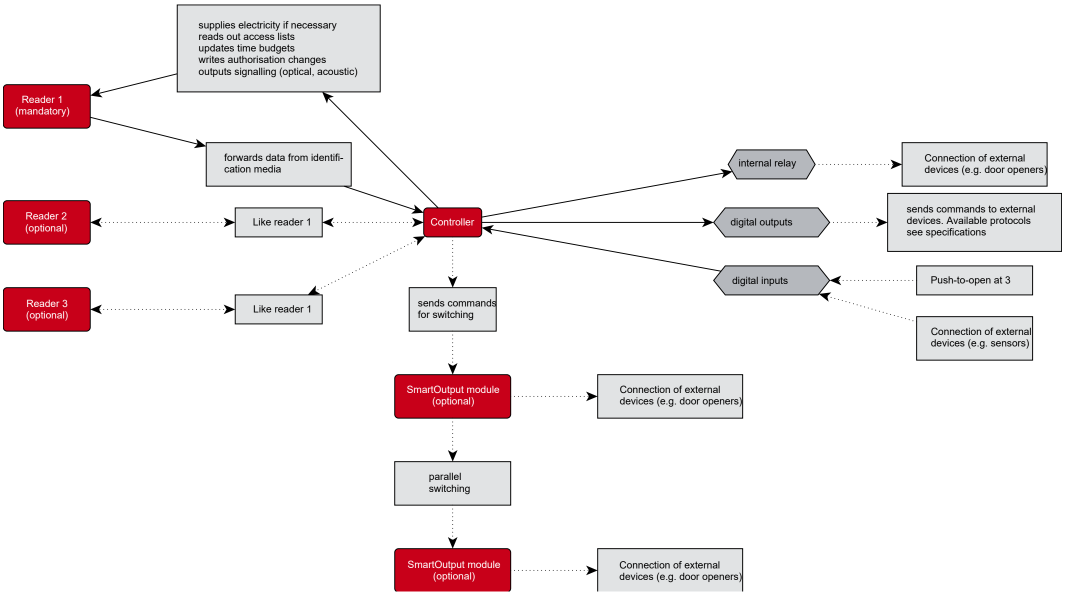
- Use in the virtual network: The controller verifies the information with the VN host.
- Use without virtual network: The controller draws on information stored locally when it was last programmed.

If the authorisation was checked successfully, the controller can:

- Actuate an internal relay, which can then be used to activate external devices.
- Transmit a recognised identification medium to an external device via the serial interface.

- Switch one or several outputs via an optional SmartOutput module chain.

The controller can also respond to a digital entry and, consequently, a connected button or similar as an alternative to successful identification.


supplies electricity if necessary
reads out access lists
updates time budgets
writes authorisation changes
outputs signalling (optical, acoustic)
Reader 1 (mandatory)
forwards data from identification media
Reader 2 (optional)
Like reader 1
Controller
Reader 3 (optional)
Like reader 1
sends commands for switching
SmartOutput module (optional)
Connection of external devices (e.g. door openers)
parallel switching
SmartOutput module (optional)
Connection of external devices (e.g. door openers)
internal relay
Connection of external devices (e.g. door openers)
digital outputs
sends commands to external devices. Available protocols see specifications
digital inputs
Push-to-open at 3
Connection of external devices (e.g. sensors)

8.4.4 Solutions for scenarios

The SREL3 ADV system is the time-tested solution for a large number of use cases. This section presents a few of them and shows how the SREL3 ADV system is used. The wiring is basically always as described in terms of electrics (see *wiring [▸ 58]*). However, line lengths, cable types and wiring installation options vary, depending on the use case.

NOTE

Protected areas are areas which can only be accessed with an authorised identification media or are secured against unauthorised access in some other way.

DANGER

Risk of injury due to incorrect programming

The SREL3 ADV system is not suitable to replace existing security installations.

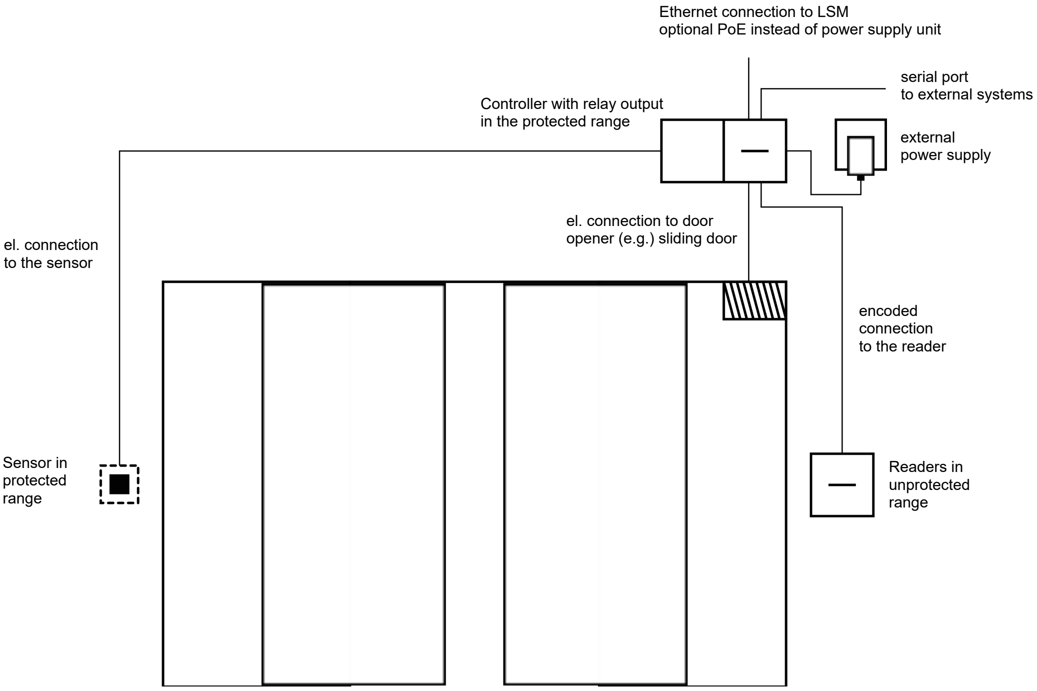
1. Ensure that the SREL3 ADV system is used as an additional securing measure only.
2. Do not replace existing security installations with the SREL3 ADV system.

In the following section, the term *unprotected area* refers to an area or place which anyone can access. The *protected area* refers to an area or place which only persons who have previously identified themselves at least once as access-authorised with an authorised identification media may access.

8.4.4.1 Doors

The SREL3 ADV system can be used to secure doors.

Door with a reader and a button



In this use case, the controller is installed in a protected area, such as the building interior. An external reader is mounted on the unprotected side of the door and can read identification media.

No-one can manipulate the data since communication is secured from the reader to the controller and to LSM. When the data reach the controller, the controller evaluates them. If there is a virtual network and connection to LSM (Ethernet), the latest information is retrieved using the identification medium; if not, the system used the last status saved internally. Depending on the result of the evaluation, the controller triggers the required action, such as actuate a relay.

The controller also features a pre-configured, non-reprogrammable push-to-open function. The relay actuates if the relevant contacts (see *Controller [▸ 17]*) are interconnected with one another. The relay integrated into the controller can be operated with an authorised identification medium or by connecting the relevant contacts. One or more buttons can be installed on the contacts. Users can press these buttons instead of using an identification medium in a secured area. This improves user convenience without losing control over the door status.

If the reader needs to be protected against vandalism, sabotage or the effects of the weather, a protective housing can be fitted to the reader (SREL2.COVER1).

Building entrance doors are a special case:

- All users need to pass through one of the building entrance doors on a daily basis.
- Building entrance doors are exposed to the weather on one side.
- Building entrance doors are in an unsecured area on one side.
- It must also be possible to open building entrance doors without an identification medium in an emergency at times.

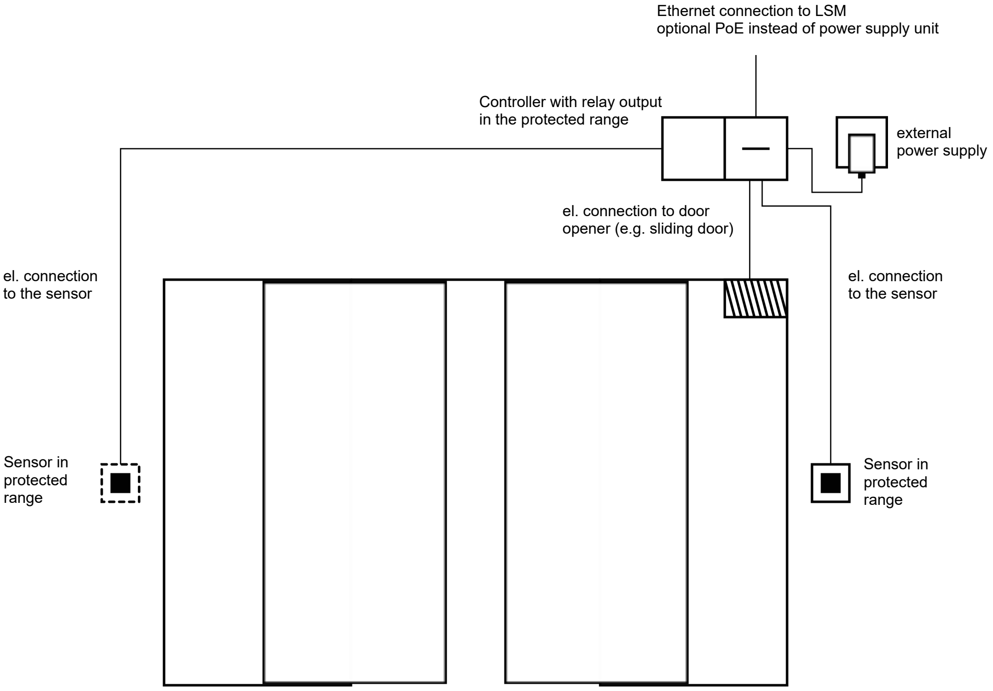
If a virtual network is used, building entrance doors are ideal for use as a gateway. The building entrance is a door which many users pass through on a daily basis. This means that each identification medium used here is verified on the reader and, consequently, in the LSM database via the controller. Authorisation changes, IDs to be blocked and time budgets are thus efficiently managed.

Access events can be forwarded to a third-party system via the serial interface.

The controller can be powered either via an external power supply unit or via the network line. The controller, in turn, can power the reader. If the voltage drop is too great, the reader can also be supplied by an external power supply unit (see *External power supply [▸ 59]*).

See *Connecting one or more readers [▸ 58]* and *Connecting one or more buttons [▸ 61]* on wiring.

Use with two buttons



IMPORTANT

No check on authorisation

Any person who has physical access can operate the relay by using the two buttons.

- Ensure that no unauthorised persons can access this locking device.

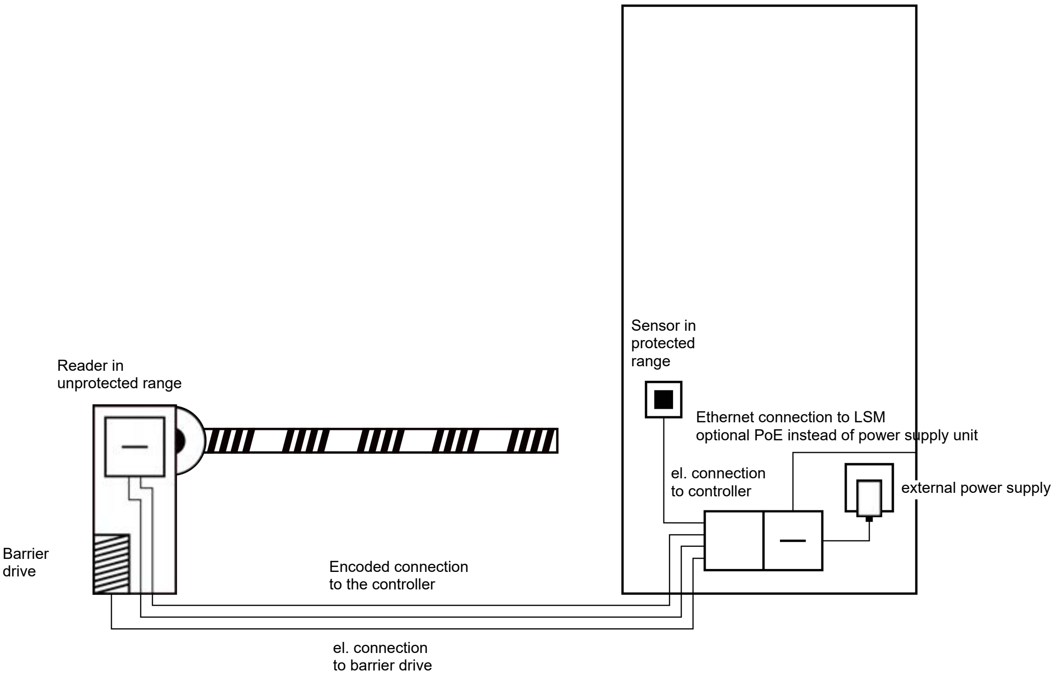
There is no longer a need to use an identification medium. Users only need to press a button to operate the relay (and open the sliding door in this example). Compared to a purely electrical connection, this approach brings the advantage of providing an overview when the relay was actuated and what its current status is (see *SmartSurveil [▸ 147]*).

The relay is not protected against unauthorised operation. This type of connection is thus only suitable for installing in areas which are already secured.

See *Connecting one or more buttons [▸ 61]* on wiring.

8.4.4.2 Entrance barrier

People who want to drive into a segregated area, such as a company car park, need to pass through an entrance barrier. Not everyone can have an authorised identification medium as this would involve considerable organisation. An entrance barrier is also normally installed outdoors and is thus exposed to the weather, vandalism and sabotage.



The SREL3 ADV system offers an intelligent solution for such situations. The controller is installed in a protected area, such as the engineering room. A reader needs to be installed close to the barrier. There are two solutions:

- The reader is fitted into the barrier housing. This variant discreetly blends in. It provides excellent protection against the weather, vandalism and sabotage.
- The reader is fitted on the barrier housing. This variant is visible on the outside and makes it easier for users to place their identification medium onto the reader. The read range is better compared to a reader fitted inside the barrier housing. The protective housing (SREL2.COVER1) ensures protection against the weather, vandalism and sabotage.

The user can use their identification media to check authorisation while in the car. If the user does not have an identification medium, but is expected, they can still announce their arrival, using an intercom, for example. Another person who is in the protected area can then let the user in by pressing the connected button. The button can be installed in a gatehouse, for example, which only allows external customers to enter during business hours while users with identification media can come in at any time.

No-one can manipulate the data since communication is secured from the reader to the controller and to LSM. When the data reach the controller, the controller evaluates them. If there is a virtual network and connection to LSM (Ethernet), the latest information is retrieved using the identification medium; if not, the system used the last status saved internally. Depending on the result of the evaluation, the controller triggers the required action, such as actuate a relay.

If a virtual network is used, the system is ideal for use as a gateway. The barrier is a locking device which is very heavily used. This means that many identification media are already synchronised with the LSM database before they reach the building entrance. As a result, there is less load on the gateway on the building door. In this case, the reader should be installed where it is visible for users to ensure that they can hear or see the reader feedback signals.

The controller can be powered either via an external power supply unit or via the network line. The controller, in turn, can power the reader. If the voltage drop is too great, the reader can also be supplied by an external power supply unit (see *External power supply [▸ 59]*).

Since a feed line needs to be installed for the barrier motor, the power supply for the reader can be easily connected to this line. Power is reliably supplied to the reader with a power supply unit, so the reader is not affected by any voltage drops due to line length.

See *Connecting one or more readers [▸ 58]* and *Connecting one or more buttons [▸ 61]* on wiring.

8.4.4.3 Lift

A lift is a special case. Lift cabs are usually connected to their environment through a trailing cable. However, the number of lines within the trailing cable is limited. The SREL3 ADV system requires a varying large number of lines, depending on the configuration.

It is highly recommended to use one or several SmartOutput modules in a lift to provide sufficient relay contacts. We also need to consider that the controller should be mounted on top of the lift cab or a network connection must be laid through the trailing cable.

If one or several SmartOutput modules are used, effective access management can be implemented in the lift itself with authorisation required for buttons for specific floors.

The reader and the SmartOutput module are installed in the lift. Users identify themselves with their identification medium in the lift.

No-one can manipulate the data since communication is secured from the reader to the controller and to LSM. When the data reach the controller, the controller evaluates them. If there is a virtual network and connection to LSM (Ethernet), the latest information is retrieved using the identification medium; if not, the system used the last status saved internally. Depending on the result of the evaluation, the controller triggers the required action, such as actuate a relay.

IMPORTANT

Interferences in the trailing cable

Lines in the trailing cable through which data is to be transmitted must be shielded (also see *Information on cabling [▸ 176]*).

Power supply from cab

This connection option requires the fewest free lines in the trailing cable and avoids voltage drops due to excessively long lines. The controller can be installed outside the lift where it is protected in a place, such as the engineering room.

The reader is **not** powered via the controller. Instead, it is connected to the existing power supply in the lift cab, which provides electricity for lighting, doors and other elements. The voltage may need to be converted with a power supply unit, so that it is within the specified voltage range for the SmartOutput module and reader (see *Properties [▸ 166]*). The voltages supplied to the individual components do not need to be identical. It is thus possible to operate the controller with 12 V while the reader in the lift is operated with 24 V.

Common earth connection

In this specific case, four lines are also needed to supply power to the cab.

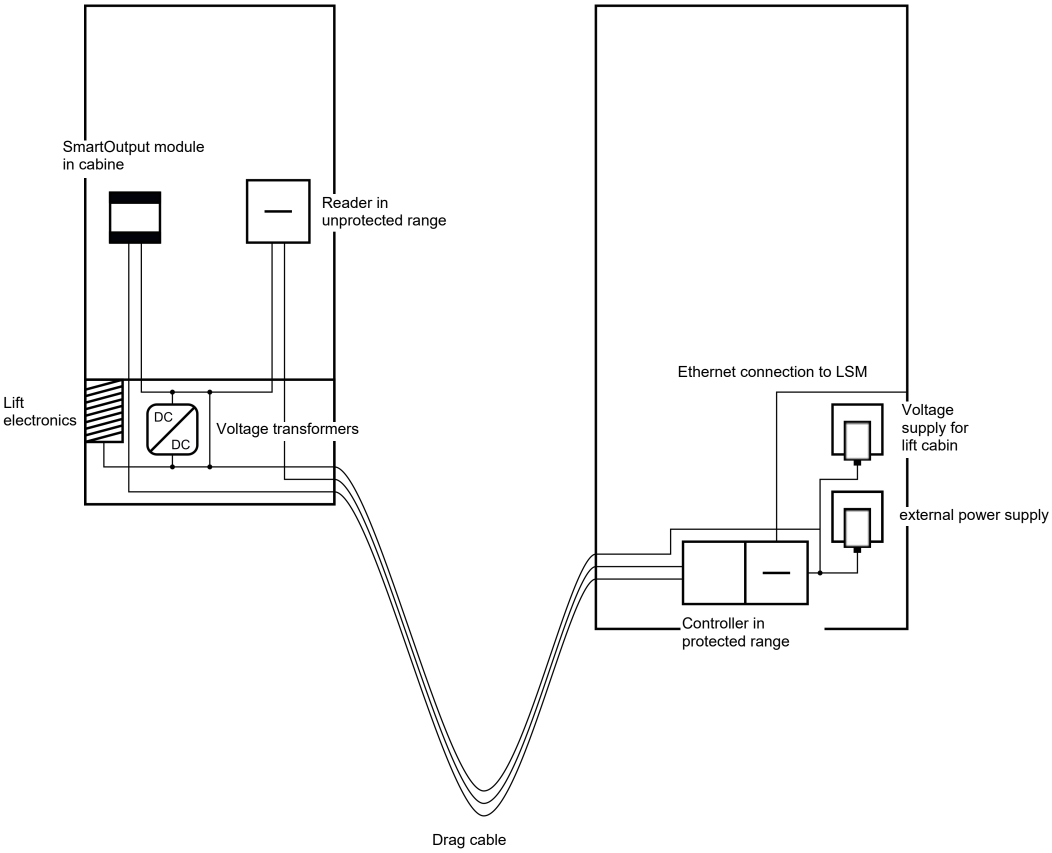
Line	Use
1	Controller – reader: Data line A
2	Controller – reader: Data line B
3	Controller – SmartOutput module: Data line A
4	Controller – SmartOutput module: Data line B

DANGER

Electric shock due to mains voltage

An electric shock may be caused when connecting the non-hazardous earth (low voltage) to a conductor which carries the mains voltage.

1. Only use conductors with a low-voltage potential (< 42 V) as a common earth cable!
2. Protect live cables, so people do not touch them accidentally!



NOTE

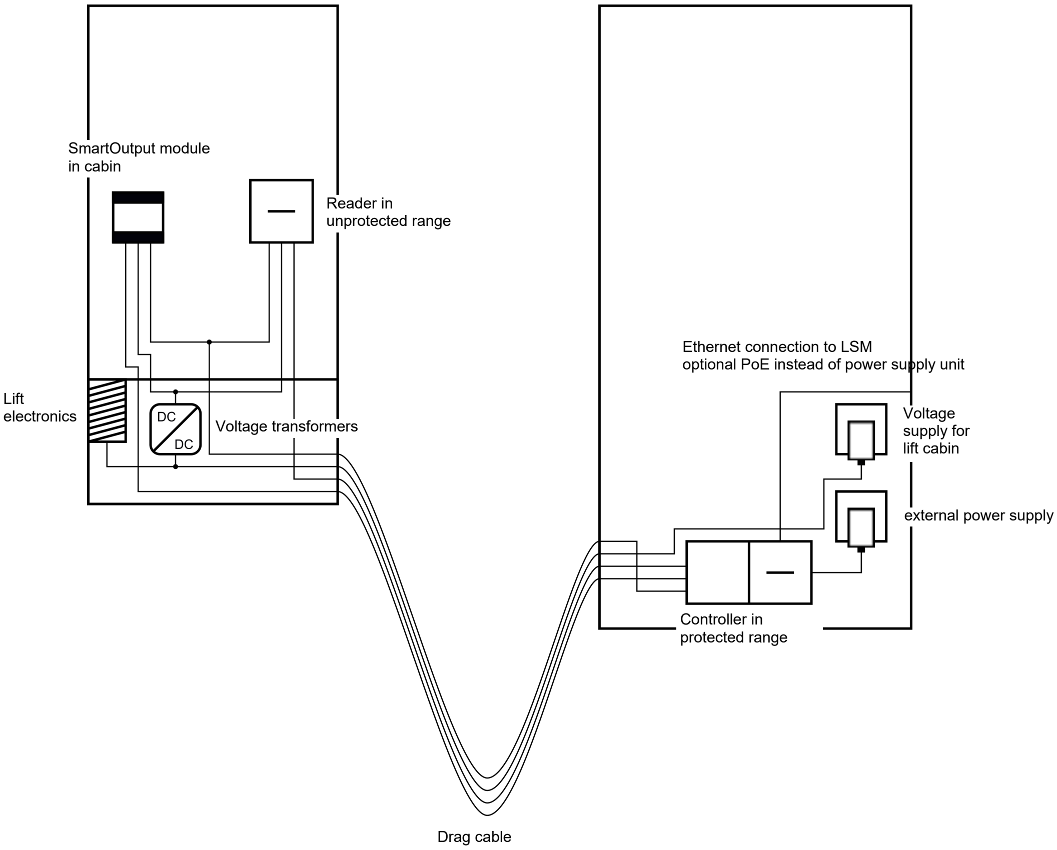
A common earth connection is required between the controller, reader and SmartOutput modules. The cab power supply earth connection can be used to save on lines in the trailing cable. The controller's earth connection needs to be connected to the cab power supply earth connection in this case.

See *Common earth with power supply [▸ 85]* on wiring.

Separate earth connection

If a common earth cable cannot be used for the cab power supply and the components, an additional line needs to be assigned in the trailing cable. In this specific case, five lines are also needed to supply power to the cab.

Line	Use
1	Earth connection between controller, reader and SmartOutput modules
2	Controller – reader: Data line A
3	Controller – reader: Data line B
4	Controller – SmartOutput module: Data line A
5	Controller – SmartOutput module: Data line B


SmartOutput module in cabin
Reader in unprotected range
Ethernet connection to LSM optional PoE instead of power supply unit
Lift electronics
DC
DC
Voltage transformers
Voltage supply for lift cabin
external power supply
Controller in protected range
Drag cable

The earth cables in the power supplies are separated from the common earth cable in this case.

See *Common earth with SREL3 components [▸ 86]* and *Connecting one or more readers [▸ 58]* on wiring.

Power supply via trailing cable

This connection option does not access existing lift electronics. This means the lift electronics remain intact and a new inspection may be avoided.

The components are powered via the trailing cable only. The required power supply unit is at the other end of the trailing cable. Depending on the length of the trailing cable, a possible voltage drop must be taken into account to meet specifications (see *Properties [▸ 166]*).

IMPORTANT

Malfunctions due to voltage drop

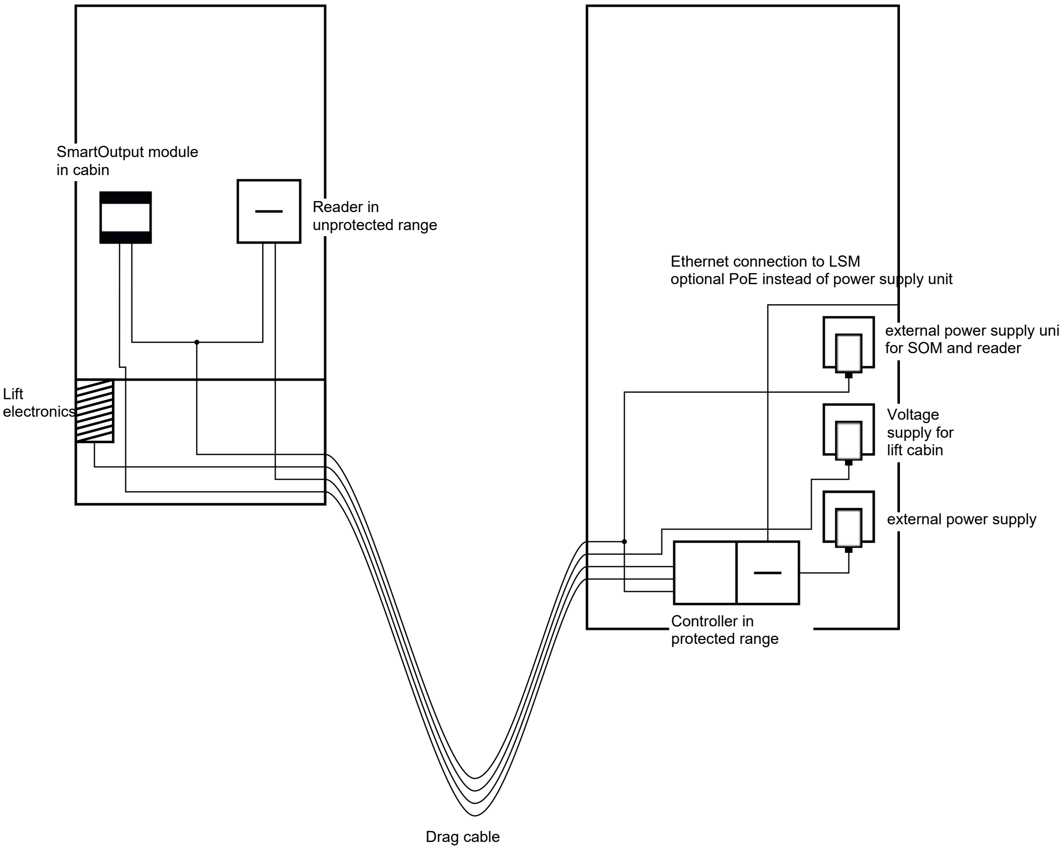
The physically induced voltage drop in the trailing cable may cause low voltages in power supplies which come from outside the cab.

1. Take the cable length into account.
2. Switch to a version with power supply in the cab if necessary (see *Common earth with power supply [▸ 85]* and *Common earth with SREL3 components [▸ 86]*).
3. Make the cable gauge larger by merging lines in the trailing cable.

Insert: Reader with SmartOutput module and common supply

The SmartOutput module requires its own power supply. The reader can also be connected to this power supply. Six free lines are required in addition to the existing lines.

Line	Use
1	Earth connection between controller, reader and SmartOutput modules
2	Positive terminal on the power supply
3	Controller – reader Data line A
4	Controller – reader Data line B
5	Controller – SmartOutput module: Data line A
6	Controller – SmartOutput module: Data line B


SmartOutput module in cabin
Reader in unprotected range
Lift electronics
Ethernet connection to LSM optional PoE instead of power supply unit
external power supply uni for SOM and reader
Voltage supply for lift cabin
external power supply
Controller in protected range
Drag cable

NOTE

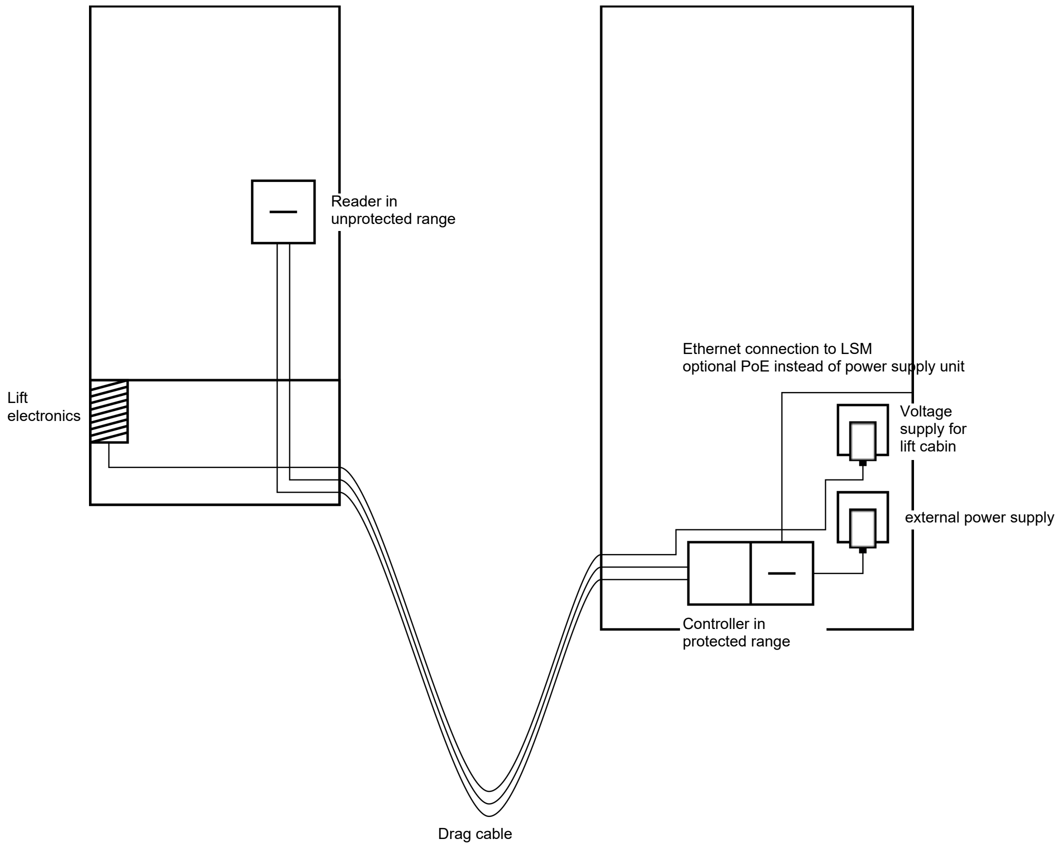
The power supply unit for the reader and the SmartOutput modules can be omitted if the controller power supply unit can deliver sufficient electricity and supply a voltage of 12 V_{DC}.

See *Power supply through trailing cable [▸ 87]* and *Connecting one or more readers [▸ 58]* on wiring.

Insert: Reader without SmartOutput module

The controller powers the reader. An additional power supply unit is not required. Four free lines are required in addition to the existing lines.

Line	Use
1	Earth connection between controller and reader
2	Positive terminal on the power supply
3	Controller – reader: Data line A
4	Controller – reader Data line B



See *Power supply through the controller [▸ 90]* on wiring.

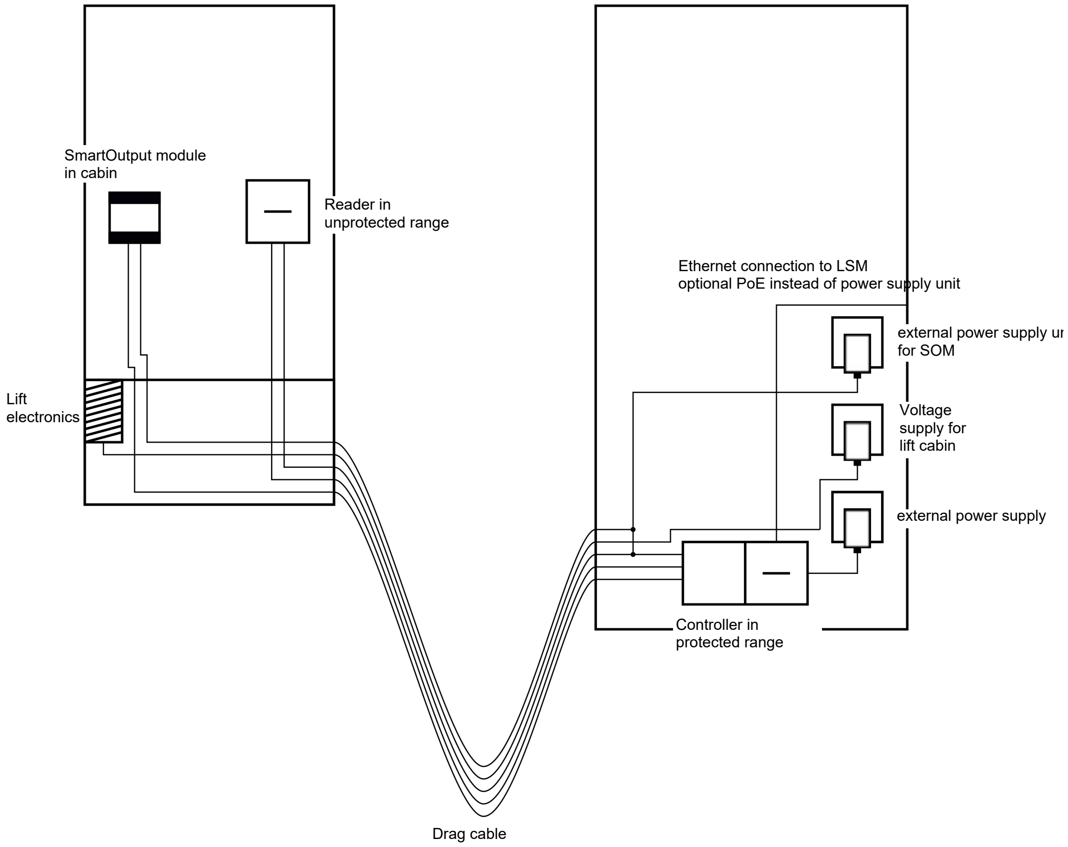
Insert: Controller-fed reader with SmartOutput module

The controller powers the reader. Connected SmartOutput modules are powered via an additional power supply unit at the other end of the trailing cable. Nine free lines are required in the trailing cable in addition to the existing lines.

The reader and its connection to the controller do not need to be removed. This means it is possible to retrofit SmartOutput modules to an existing connection.

Line	Use
1	Earth connection between SmartOutput module and power supply unit
2	Positive terminal for power supply between SmartOutput module and power supply unit
3	Earth connection between controller and reader
4	Positive terminal for power supply between controller and reader

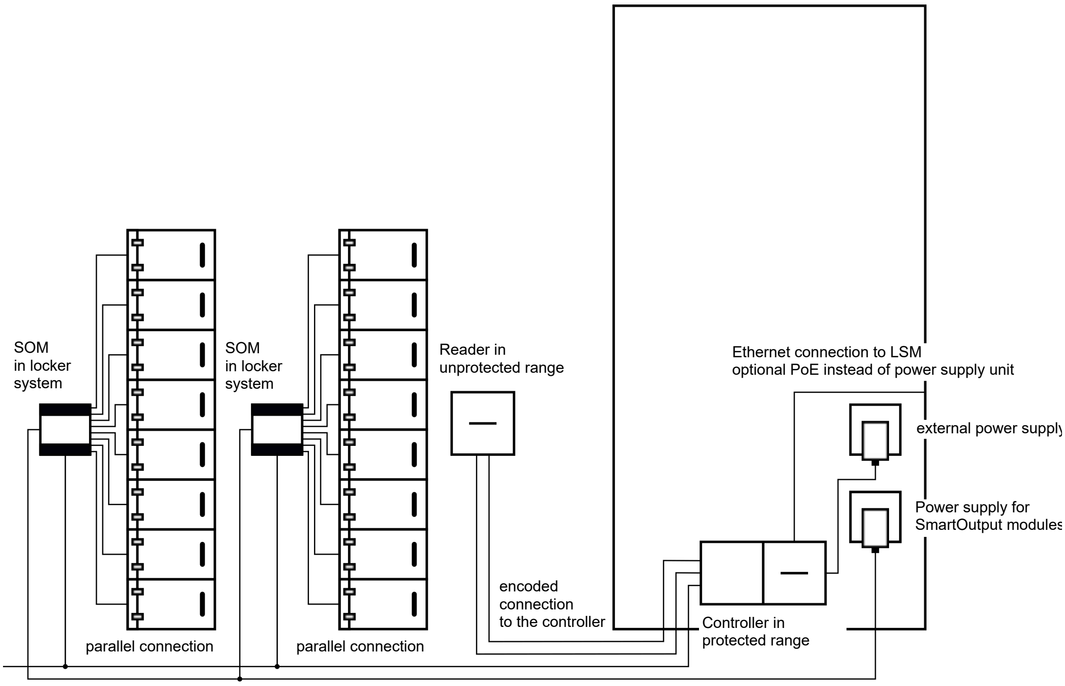
Line	Use
5	Controller – SmartOutput module: Data line A
6	Controller – SmartOutput module: Data line B
7	Controller – SmartOutput module: Data line earth connection
8	Controller – reader Data line A
9	Controller – reader Data line B



See *Controller-fed reader with SmartOutput modules [▸ 91]* and *Connecting one or more readers [▸ 58]* on wiring.

8.4.4.4 Safe deposit boxes

Safe deposit box systems are used by a variety of users. Only authorised persons should be able to open their designated deposit boxes. Deposit box systems are not always installed in areas protected from the weather. Suppliers, deliverers and a selected group of people should be able to access all deposit boxes. Some people may need to be able to open several deposit boxes.



The existing connections to open the locking system can be actuated with the SmartOutput modules, no matter whether a direct or alternating current is used. The SmartOutput modules are connected in parallel for this purpose. The address can be configured individually on each SmartOutput module. This allows up to fifteen SmartOutput modules with eight outputs each to be connected to the system (except the last module, which supports only four relays). The deposit box is opened as soon as the controller receives an opening command to the corresponding relay.

Identification media can be authorised for individual relays and, consequently, individual deposit boxes in LSM. However, it is also possible to group identification media together, for a department, for example, and authorise this group to use a single relay, in a departmental deposit box. Identification medium verification means you can trace which of the group's identification media has operated the relay (and taken documents, for example). If individual persons are supposed to be able to open a number of deposit boxes, relays can be grouped – in different trust levels, for example. The group of authorised persons becomes smaller as the trust level increases.

There are two options for installing the reader:

- The reader is installed in an existing housing – in an intercom housing, for example. This variant is hidden from view and offers effective protection against the weather, vandalism and sabotage.
- The reader is fitted on the wall. This variant is visible on the outside and makes it easier for users to place their identification medium onto the reader. The read range is better compared to a reader fitted inside the

housing. If the reader is installed outdoors, protection against the weather, vandalism and sabotage can be assured with the protective housing (SREL2.COVER1).

A master identification medium can be created for emergencies. This can be used to open several or all boxes at the same time.

The controller can be powered either via an external power supply unit or via the network line. The controller, in turn, can power the reader. If the voltage drop is too great, the reader can also be supplied by an external power supply unit (see *External power supply [▸ 59]*).

See *Connecting one or more readers [▸ 58]* and *Connecting one or more SmartOutput modules [▸ 63]* on wiring.

8.4.4.5 Machine safety

Machines can pose significant hazards:

- Cuts
- Burns
- Electric shocks
- Laser radiation
- Crushing

For safety reasons, only qualified people should therefore be allowed to operate hazardous machines. Unauthorised persons must not be able to put hazardous machines into operation.

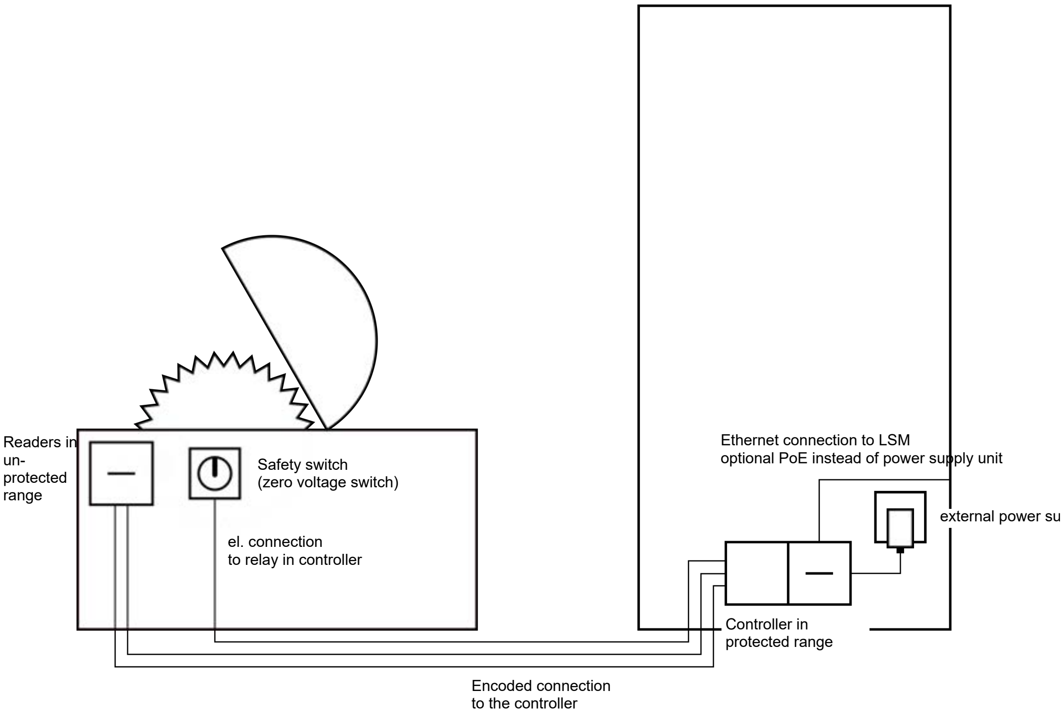
An option to switch off the machine without authorised identification media further increases operational safety.

DANGER

Risk of injury due to incorrect programming

The SREL3 ADV system is not suitable as a sole disconnecting device. A contactor activated via the controller must never be the only means to switch off a machine.

1. Use the SREL3 ADV system as an additional disconnecting device only, not as the sole one.
2. Use the actuated contactor in a series circuit with the machine's emergency stop switch only.


Readers in un-protected range
Safety switch (zero voltage switch)
el. connection to relay in controller
Ethernet connection to LSM optional PoE instead of power supply unit
external power su
Controller in protected range
Encoded connection to the controller

The SREL3 ADV system provides effective protection to prevent unauthorised persons from putting dangerous machines into operation and injuring themselves. The reader is fitted to the machine requiring protection and connected to the controller. The relay in the controller does not switch until an authorised identification medium has been activated on the reader, thus unblocking the power supply to the machine by switching the contactor. Only then can the machine be switched on at the safety switch. There are two options for installing the reader:

- The reader is fitted into the machine housing. This variant is hidden from view and offers effective protection against the weather, dirt, fluids and mechanical impacts, depending on the machine housing.
- The reader is fitted on or next to the machine housing. This variant is visible on the outside and makes it easier for users to place their identification medium onto the reader. The read range is better compared to a reader fitted inside a (metal) housing. The protective housing (SREL2.COVER1) ensures protection against the weather, dirt, liquids and slight mechanical impacts.

No-one can manipulate the data since communication is secured from the reader to the controller and to LSM. When the data reach the controller, the controller evaluates them. If there is a virtual network and connection to LSM (Ethernet), the latest information is retrieved using the identification medium; if not, the system used the last status saved internally. Depending on the result of the evaluation, the controller triggers the required action, such as actuate a relay.

The machine can only be put into operation if an identification medium is used on the reader. In the event of damage, the access list (for ZK variants only) will allow management to identify exactly who operated the machine last and take appropriate measures.

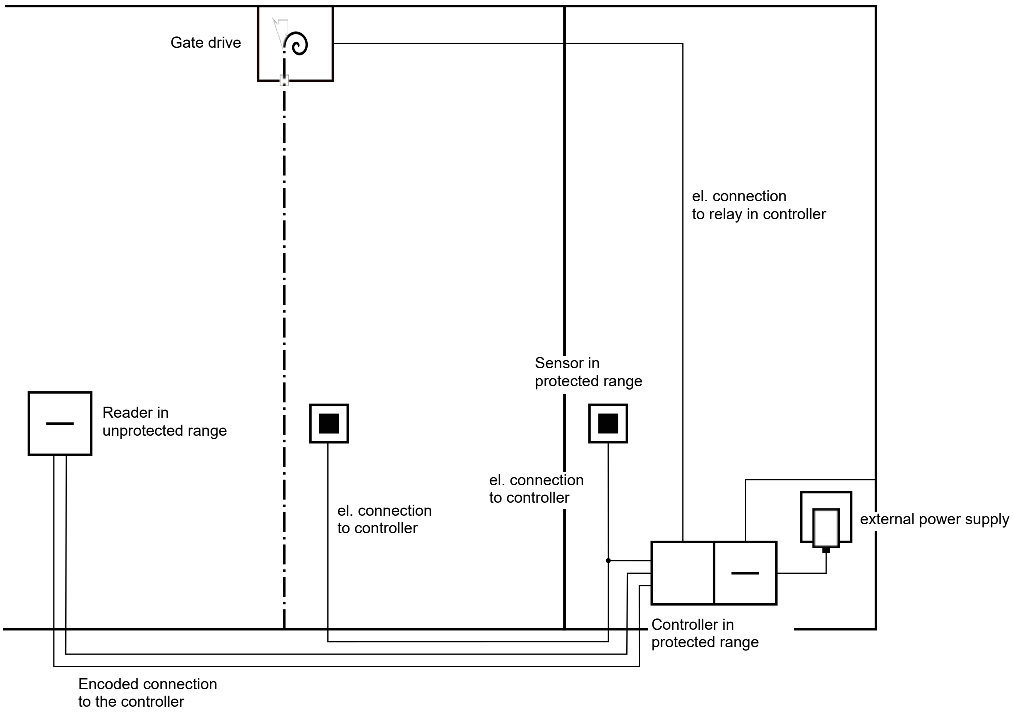
The controller can be powered either via an external power supply unit or via the network line. The controller, in turn, can power the reader. If the voltage drop is too great, the reader can also be supplied by an external power supply unit (see *External power supply [▸ 59]*).

See *Connecting one or more readers [▸ 58]* on wiring.

8.4.4.6 Underground car park entrance

An underground car park entrance is a similar situation to an entrance barrier (see *Entrance barrier [▸ 43]*) since anyone who wants to enter an underground garage from the outside must use the entrance. Some of these people, such as business customers, do not have an identification medium. The exterior part is also not exposed to the weather, vandalism and sabotage. The main difference is that an underground car park can be secured with elements such as roll-up doors to ensure unauthorised persons cannot walk through the entrance.

The underground car park interior can thus be regarded as a protected area.



The SREL3 ADV system can be used to provide a convenient underground car park control. As with all other use cases, the controller is installed in a protected area, such as the engineering room. A reader is also needed in front of the roll-up door, close to the entrance:

- The reader is installed in a suitable position in an existing housing – in an existing intercom housing, for example. This variant is inconspicuous and offers effective protection against the weather, vandalism and sabotage.
- The reader is fitted on the wall. This variant is visible on the outside and makes it easier for users to place their identification medium onto the reader. The read range is better compared to a reader fitted inside an existing housing. The protective housing (SREL2.COVER1) ensures protection against the weather, vandalism and sabotage.

The user can use their identification media to check authorisation while in the car. If the user does not have an identification medium, but is expected, they can still announce their arrival, using an intercom, for example. Another person who is in the protected area can then let the user in by pressing the connected button. The button can be installed in a gatehouse, for example, which only allows external customers to enter during business hours while users with identification media can come in at any time.

Users who wish to leave the underground car park are within a protected area. Consequently, there is no need to re-verify authorisation for the door. Greater convenience is provided by connecting one button in a parallel circuit with another button (in the gatehouse) and positioning it near to the exit within the protected area.

No-one can manipulate the data since communication is secured from the reader to the controller and to LSM. When the data reach the controller, the controller evaluates them. If there is a virtual network and connection to LSM (Ethernet), the latest information is retrieved using the identification medium; if not, the system used the last status saved internally. Depending on the result of the evaluation, the controller triggers the required action, such as actuate a relay.

If a virtual network is used, the system is ideal for use as a gateway. The underground car park entrance features a locking device which is heavily used. This means that each identification medium used here is verified on the reader and, consequently, in the LSM database via the controller. Authorisation changes, IDs to be blocked and time budgets are thus efficiently managed.

The controller can be powered either via an external power supply unit or via the network line. The controller, in turn, can power the reader. If the voltage drop is too great, the reader can also be supplied by an external power supply unit (see *External power supply [▸ 59]*).

IMPORTANT

Manipulation of unprotected electrical connections

Unprotected electrical connections can be short-circuited or manipulated in another way.

1. Install electrical connections from buttons to the controller within protected areas only.
2. Install electrical connections from the controller to the contactor or the device being activated within protected areas only.

See *Connecting one or more readers [▸ 58]* and *Connecting one or more buttons [▸ 61]* on wiring.

8.4.5 wiring

8.4.5.1 Connecting one or more readers

NOTE

If you use one or two card readers, you may wire them either to the first, second or third connection. If you wish to connect SmartOutput modules, you may only use the connection on the third reader.

Power supply through the controller

The readers (up to three readers per controller) are connected to the controller at the designated points. This type of wiring is the simplest type of connection between readers and controllers. The controller loops the power supply through to the connections for the readers, which can then be operated without an additional power supply unit.

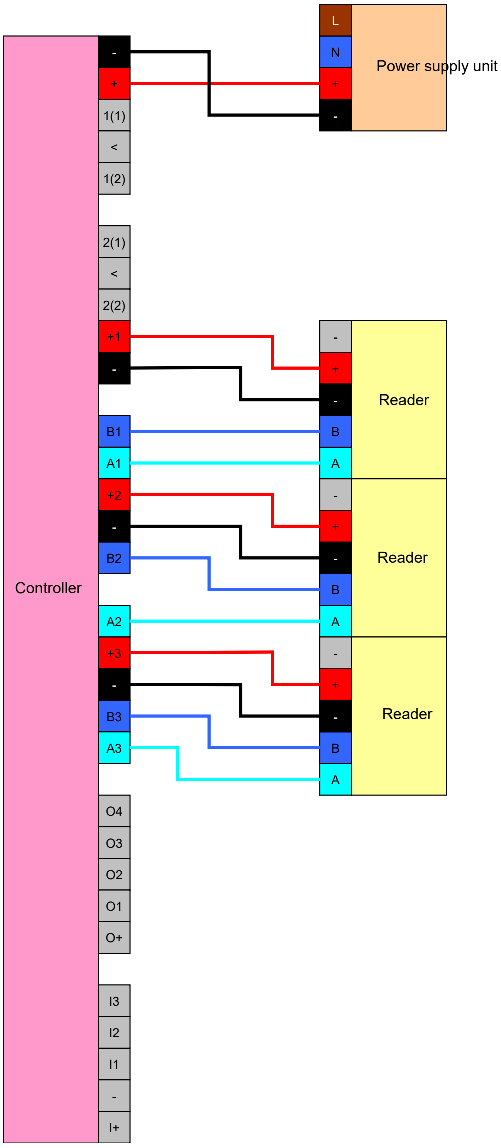
IMPORTANT

Malfunctions due to voltage drop

A voltage drop occurs in the lines between the controller and reader. If the voltage drop is too great, the voltage on the reader is no longer sufficient for reliable operation.

1. Observe the cable length specifications (see *Properties [▸ 166]*).
2. Use an external power supply unit to power readers in cases of doubt (see *External power supply [▸ 59]*).

Use this configuration to verify that the components which they contain function correctly.

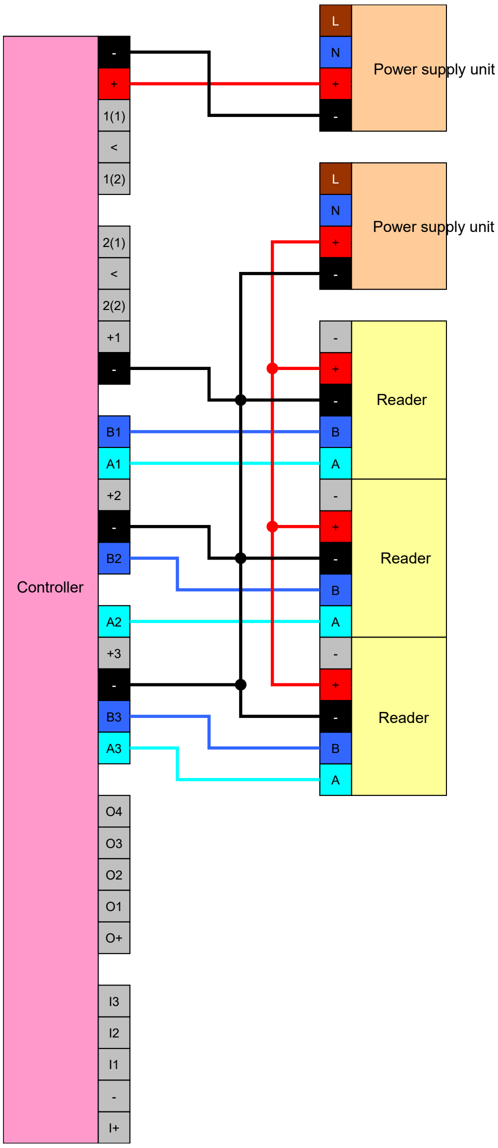


External power supply

The readers (up to three readers per controller) are connected to the controller at the designated points. The power for readers is provided from an own power supply unit. A common reference potential is required for data transmission between controllers and readers. As a result, the earth systems in power supply units, the power supply and the controller must be connected. Using an external power supply unit avoids potential problems with voltage drops between controllers and readers.

Option 1: Using a earth connection

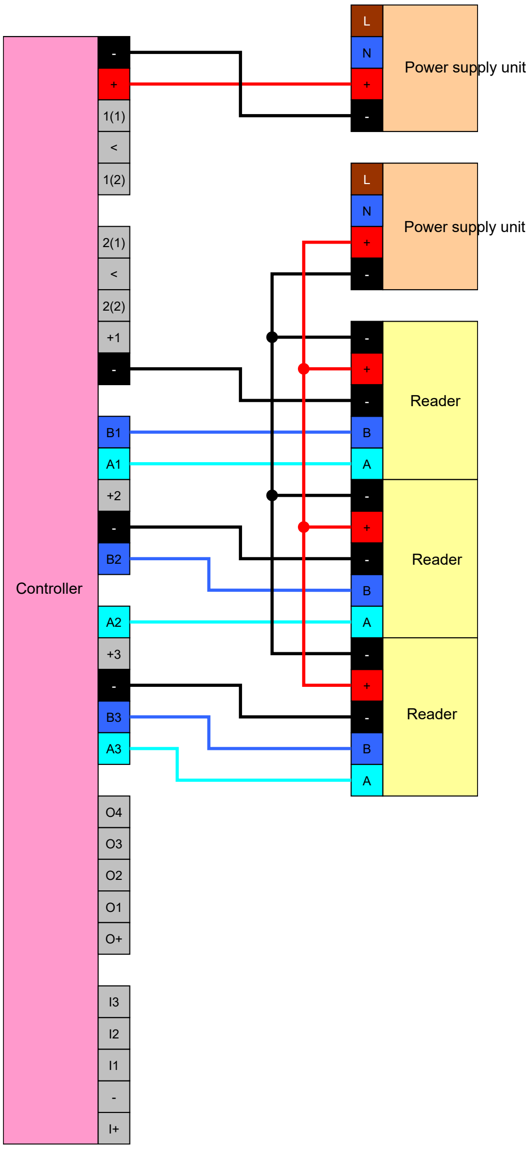
This configuration uses just one of the two earth connections available on the reader. Since the two earth connections are connected to one another electrically, it does not matter which one is connected to the earth. It is sufficient to assign one earth connection to the controller. This establishes a common reference potential, allowing data transmission to take place. Since the earth connections on the controller are connected to one another electrically, it does not matter which one is connected to the earth (see *Controller [⏵ 17]* for details). The diagram shows all possible earth connections between the readers and the controller. However, it is sufficient if one earth connection on the controller is connected to the reader earth systems.



Option 2: Using two earth connections

This configuration uses both earth connections available on the reader. The power supply unit's earth is wired to one earth connection, the controller's earth to the other earth connection. This establishes a common reference potential, allowing data transmission to take place. Since the earth connections on the controller are connected to one another electrically, it does not matter which one is connected to the earth (see *Controller [⏵ 17]* for details). It is sufficient if one earth connection on the controller is connected to the readers' earth systems.

This configuration is ideal if you wish to reduce the number of branches in the wiring. Both configurations function in exactly the same way.

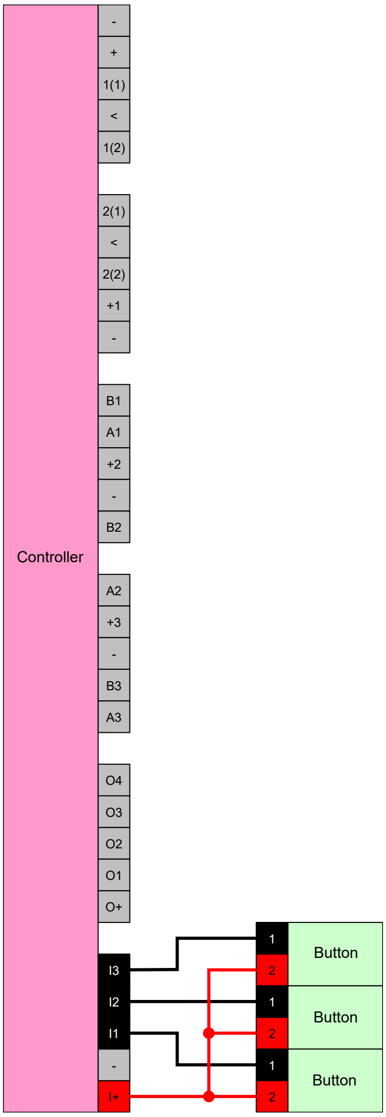


8.4.5.2 Connecting one or more buttons

As a general rule, buttons are always connected to the digital inputs on the controller. Up to three buttons can be connected per controller (see *Controller [▸ 17]*). Button functions can be configured in LSM. The inputs are low in a non-actuated state, i.e. logic 0. They are registered as high if the voltage present exceeds a threshold value (see *Properties [▸ 166]*). The threshold voltage can be exceeded (as shown) by connecting to the controller's operating voltage. Alternatively, any voltage within the specified levels (see *Properties [▸ 166]*) can be used with a common reference potential to the controller.

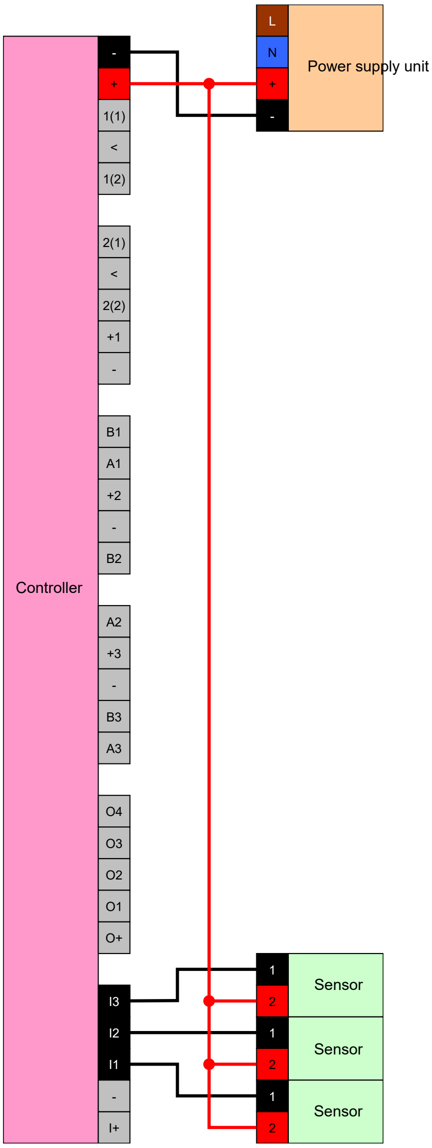
Option 1: Using the I+ connection

In addition to the digital inputs, there is also an output which transmits an operating voltage of - 1 V_{DC} to make it easier to use buttons. The output can be used to increase the inputs to a higher voltage than the threshold voltage, thus switching to logic 1.



Option 2: Using V_{IN}

If I+ is not to be used, another voltage can be used with a common reference potential (same earth) with the controller – from the power supply unit in this case. This option is recommended if the power supply unit and buttons are close to one another, but are far from the controller. There is no need to install another cable (the I+ to be precise) in this case.

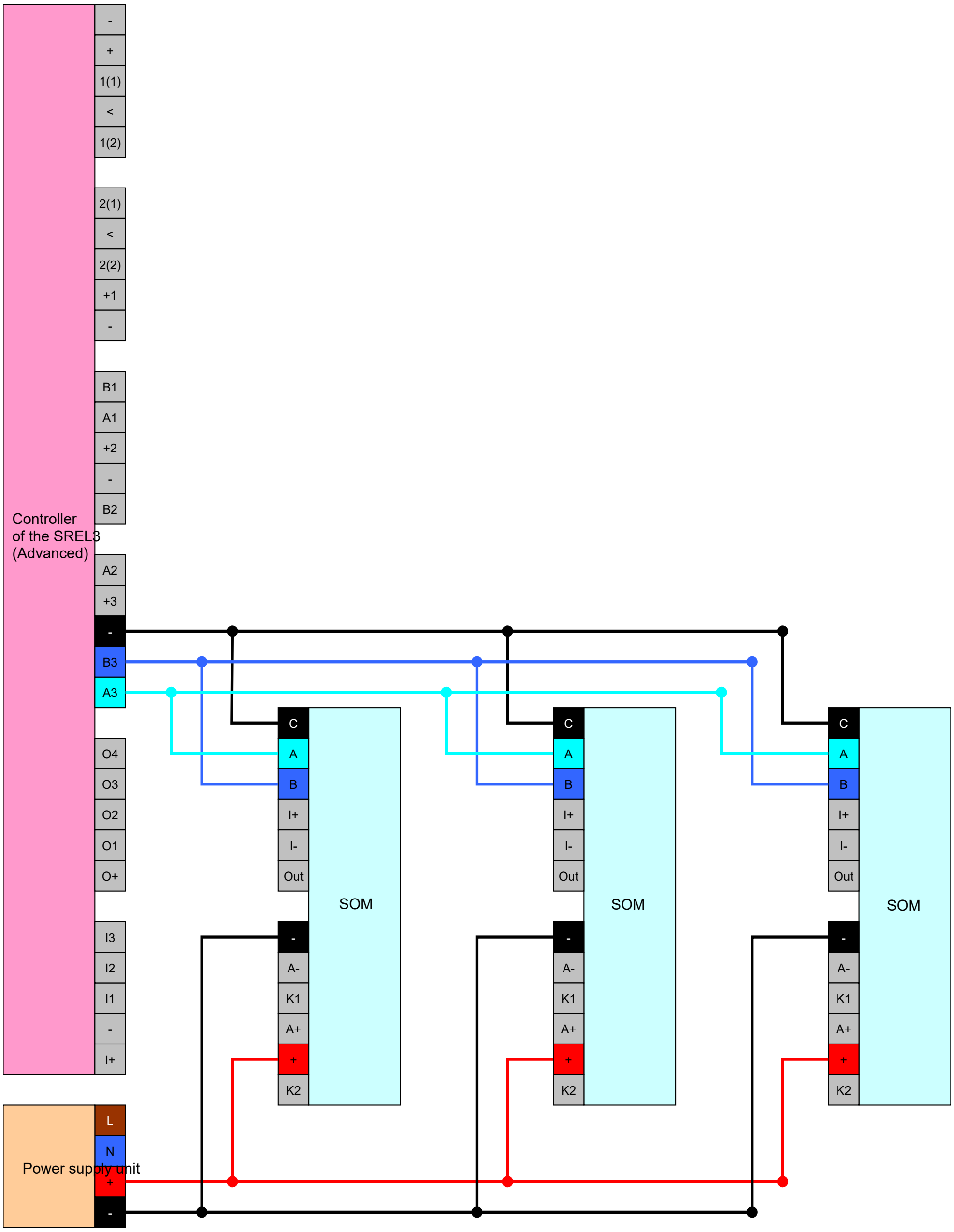


8.4.5.3 Connecting one or more SmartOutput modules

SmartOutput modules require a supply voltage which may differ from the controller's supply voltage. For this reason, it is recommended to use their own power supply unit. SmartOutput modules are connected in parallel on the bus (A, B). The bus is connected to the controller instead of a third reader. To ensure the SmartOutput modules are activated correctly, an address needs to be configured on each SmartOutput module (see SmartOutput module manual).

NOTE

If the controller's power supply unit delivers 12 V_{DC} and sufficient electricity, there is no need for a power supply unit for the SmartOutput modules; the controller's power supply can be used instead. In this case, the earth system in the SmartOutput modules is connected to the controller power supply unit and V_{IN} in the SmartOutput modules with the power supply unit's 12 V_{DC}.



Configuring the address for modules

Each connected module is actuated using its address. This address is set on the address switch. If you connect a SmartOutput module to a SmartRelay 3, set the following addresses:

Module	Address
Module 1	0 (initial setting in the factory)
Module 2	1

Module	Address
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

1. Press the sides of the transparent inlay together.
2. Remove the transparent inlay.
3. Use a screwdriver to configure the address as per the table.
4. Insert the transparent inlay again.

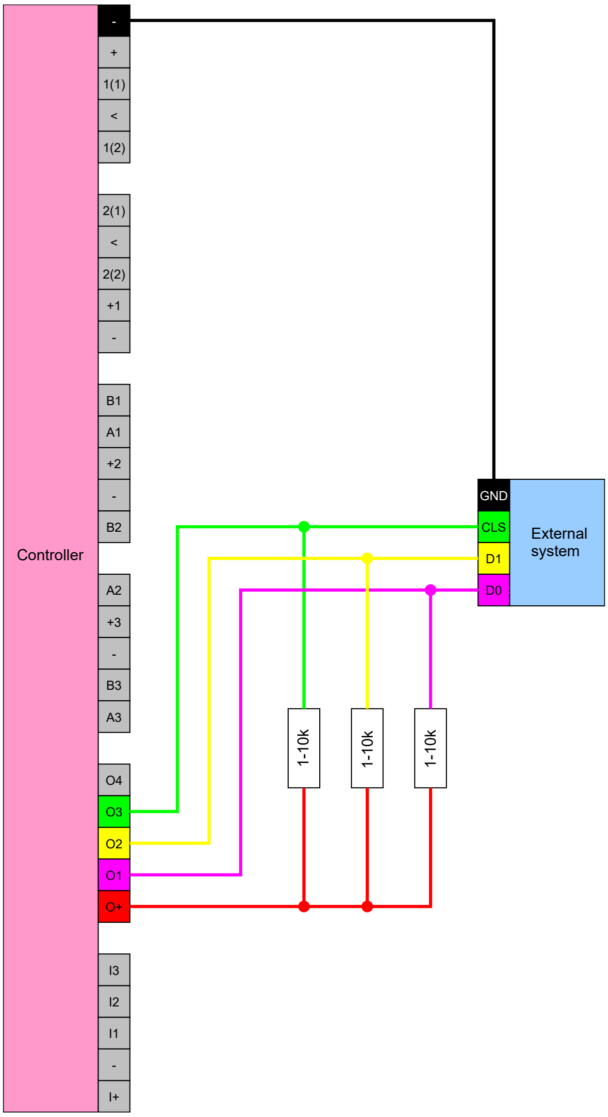
8.4.5.4 Using the serial interface

The digital outputs used for the serial interface are open drain connections. This means that a pull-up resistance in the data lines and 3–24 V_{DC} are required for operation as a serial interface. The O+ connection can be used for this purpose. A value of 1 kΩ is recommended. The earth system in the controller and the earth system in the third-party system must also be connected for data transmission.

You can obtain detailed information and the specifications from Support (see Help and contact). The required pull-up resistances may already be integrated in your third-party system. In doubt, please ask the manufacturer of your third-party system.

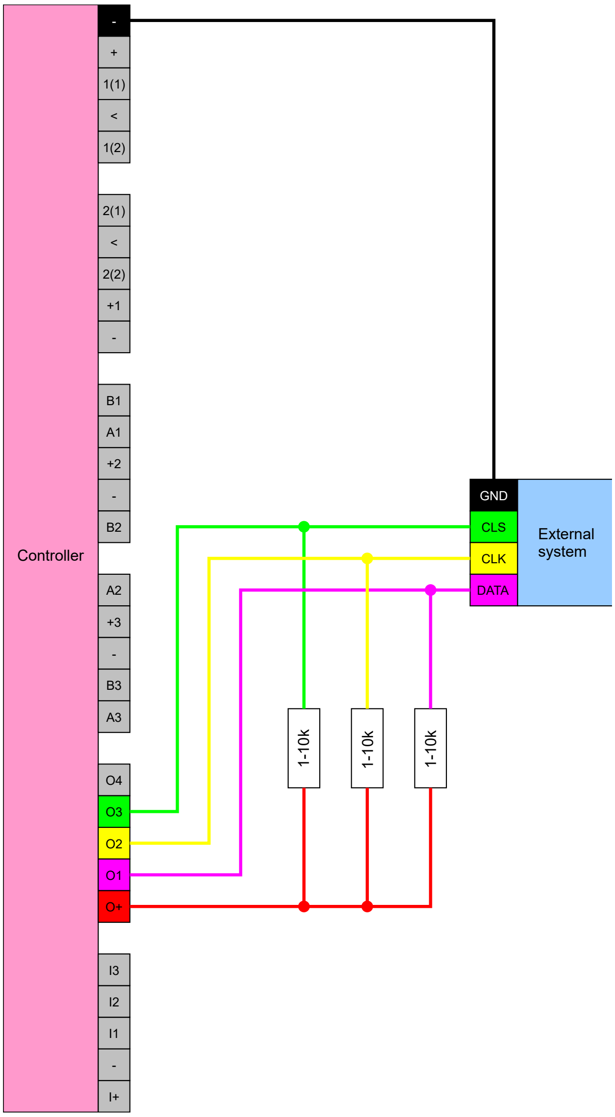
Wiegand 26-bit and 33-bit

The controller can communicate with systems which use one of the Wiegand protocols. Once an authorised identification medium is detected, the data are forwarded to the third-party system via the serial interface. The controller must be wired as follows to make this possible.



Primion, Siemens Cerpass, Kaba Benzing, Gantner Legic and Isgus

The controller can communicate with systems which use one of the protocols. Once an authorised identification medium is detected, the data are forwarded to the third-party system via the serial interface. The controller must be wired as follows to make this possible.



Specifications for the serial interfaces with CLS

Your SmartRelay is not only able to read identification media and switch a relay, but also serve solely as a reader for identification medium data. This data comprises:

- Customer ID or locking system ID
- Transponder ID

The identification medium data read is then forwarded to third-party systems via a serial interface in various data formats. Examples of such external systems:

- Attendance recording systems
- Canteen billing systems

This allows to control all relevant systems with just one identification medium, e.g.:

- Building automation systems

- Access control
- Time-and-attendance
- Canteen billing

The serial interface supports different signal and data format variants for the different manufacturers:

- Wiegand26 (standard format)
- Wiegand33 (for PRIMION connections)
- OMRON Primion
- OMRON Siemens-CerPass
- OMRON Gantner-Legic
- OMRON Dormakaba
- OMRON Isgus

Wiegand26 (standard format)

Signal description

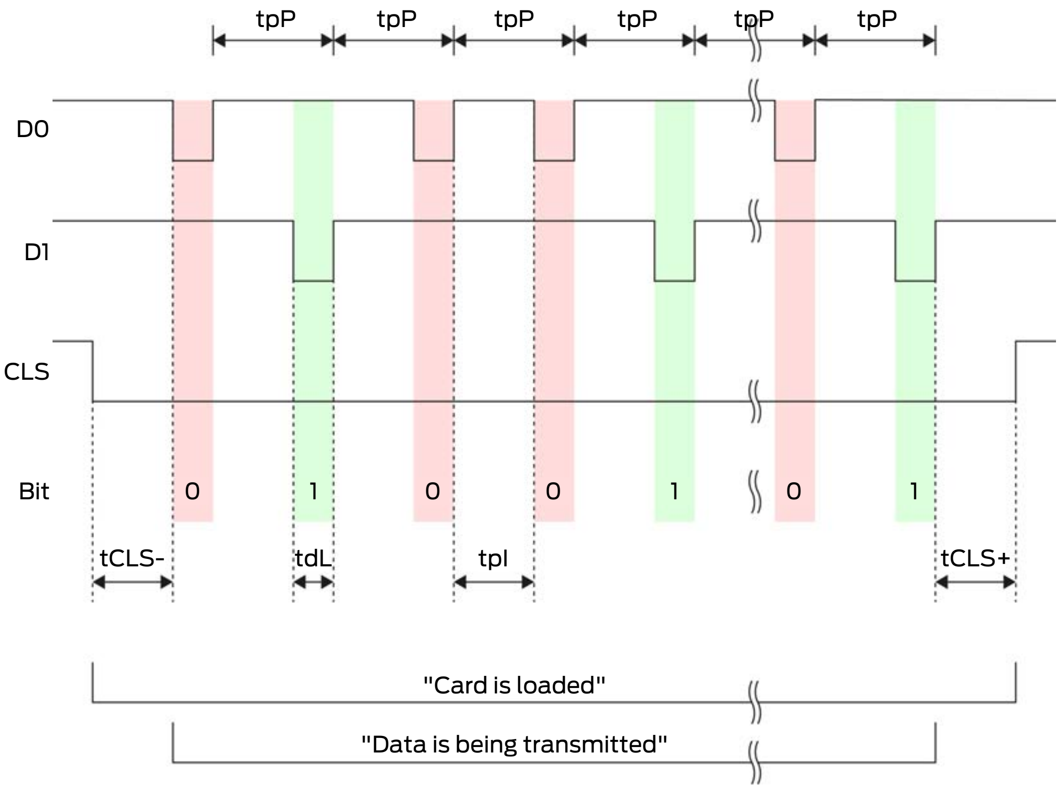
A Wiegand interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
D0	Data 0		F1 ("D0")	O1	Output 1
D1	Data 1		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	10	12	ms
t_{dL}	Data bit pulse width	80	100	120	µs
t_{pl}	Time between two bits (idle time)	800	900	1000	µs
t_{pP}	Signal period (data rate period)	900	1000	1100	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	10	12	ms

Data format (Wiegand 26-bit)

This is the standard Wiegand interface. The facility code is shortened to 8 bits.

Bit number	Meaning
Bit 1	Parity bit (even) spanning bits 2 to 13
Bits 2 to 9	Facility code (0 to 255). Bit 2 is MSB.
Bits 10 to 25	User ID number (0 to 65,535). Bit 10 is MSB.
Bit 26	Parity bit (odd) spanning bits 14 to 25.

Wiegand33 (for PRIMION connections)

Signal description

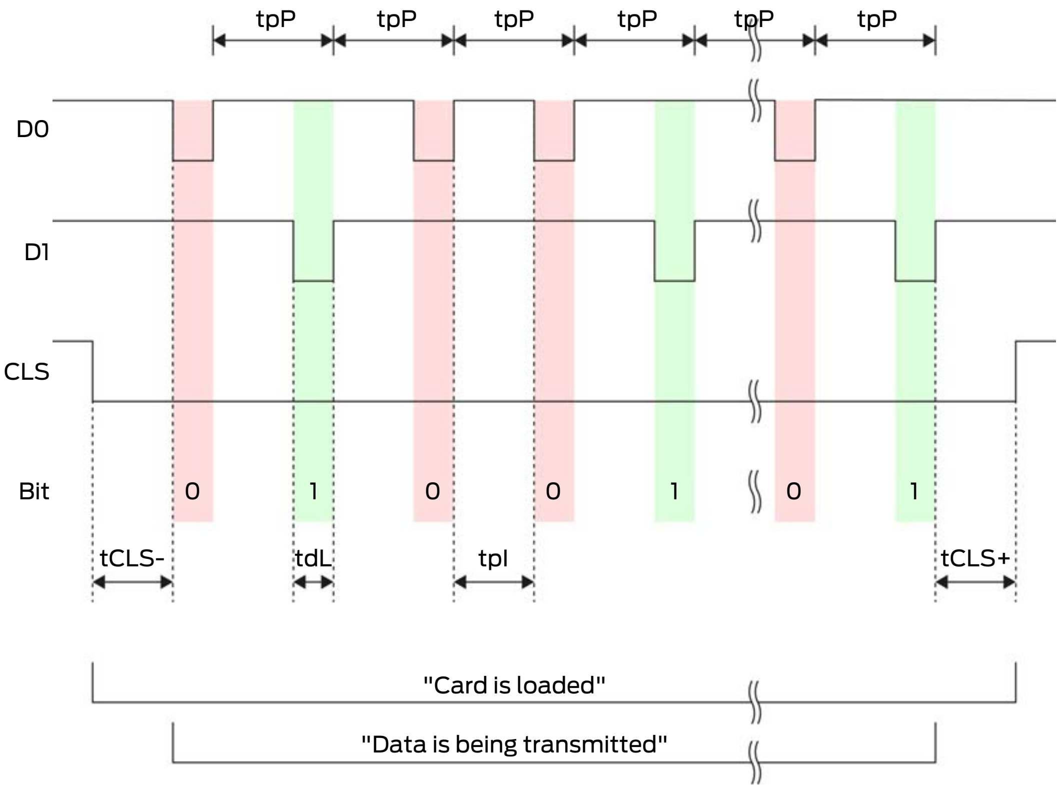
A Wiegand interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
D0	Data 0		F1 ("D0")	O1	Output 1
D1	Data 1		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	10	12	ms
t_{dL}	Data bit pulse width	80	100	120	µs
t_{pl}	Time between two bits (idle time)	800	900	1000	µs
t_{pP}	Signal period (data rate period)	900	1000	1100	µs

Time	Description	Min.	Typ.	Max.	Unit
t $_{CLS+}$	Time between last data bit and deactivation of the CLS signal	8	10	12	ms

Data format (Wiegand 33-bit)

This is a modified Wiegand format. It contains the complete 16-bit facility code (or locking system ID).

Bit number	Meaning
Bits 1 to 16	Facility code (0 to 65,535). Bit 1 is MSB.
Bits 17 to 32	User ID number (0 to 65,535). Bit 17 is MSB.
Bit 33	Parity bit (odd) spanning bits 1 to 32.

OMRON Primion

Signal description

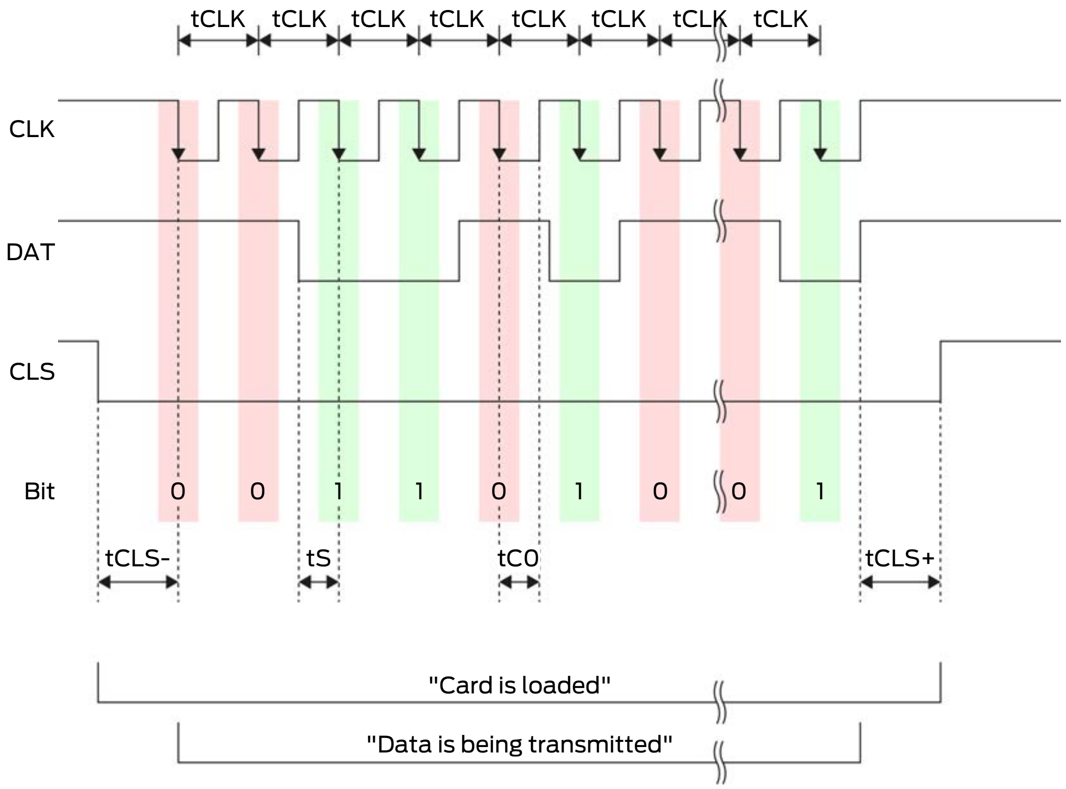
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Primion)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

S AAAAA BBBBB E

Meaning:

S	Start character (hex B)
A	Facility code (0 to 99,999)
B	User ID number (0 to 99,999)
E	End character (hex F)

Example:

- Facility code: 563
- User ID: 3,551

S	A	A	A	A	A	B	B	B	B	B	E
Start character	Facility code					User ID					End character
11010	00001	00001	10101	01101	11001	00001	11001	10101	10101	10000	11111
B	0	0	5	6	3	0	3	5	5	1	F

OMRON Siemens-CerPass

Signal description

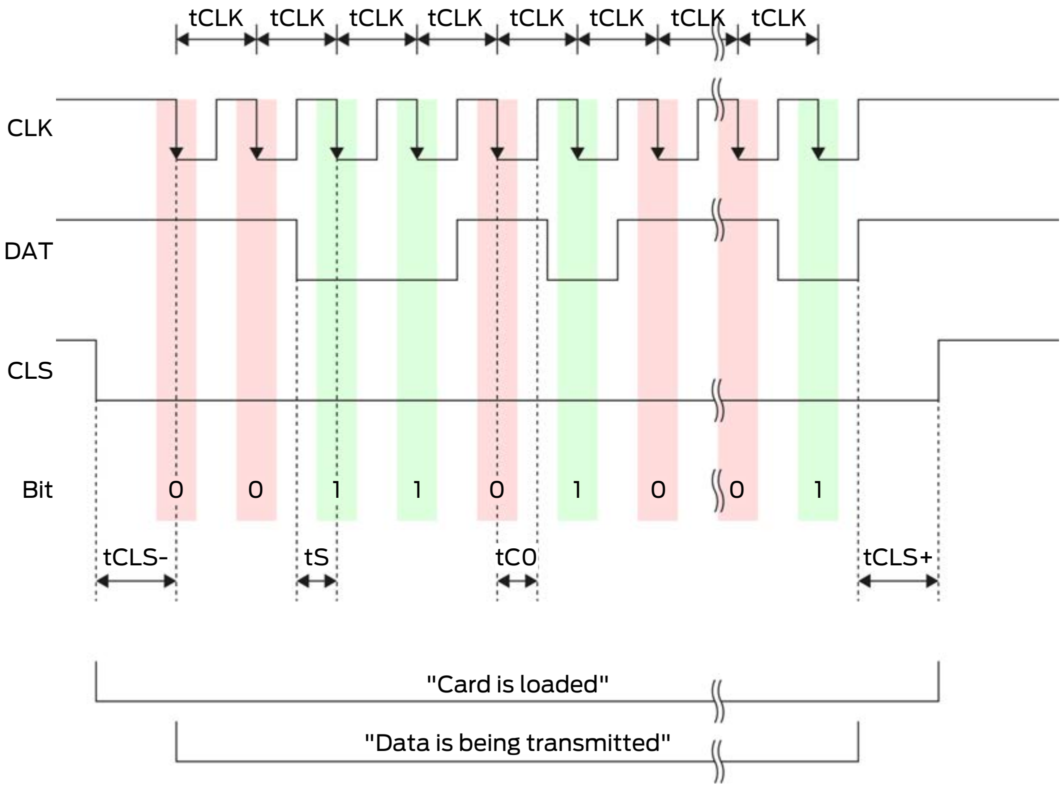
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{CO}	Clock set to “low” level (clock low)	50	100	150	µs
t_{CLS+}	Time between last data bit and de-activation of the CLS signal	8	12	20	ms

Data format (OMRON Siemens-CerPass)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
<10 leading zero bits> S AAAAA BBBBB E L
```

Meaning:

S	Start character (hex B)
A	Facility code (0 to 99,999)

B	User ID number (0 to 99,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

OMRON Gantner-Legic

Signal description

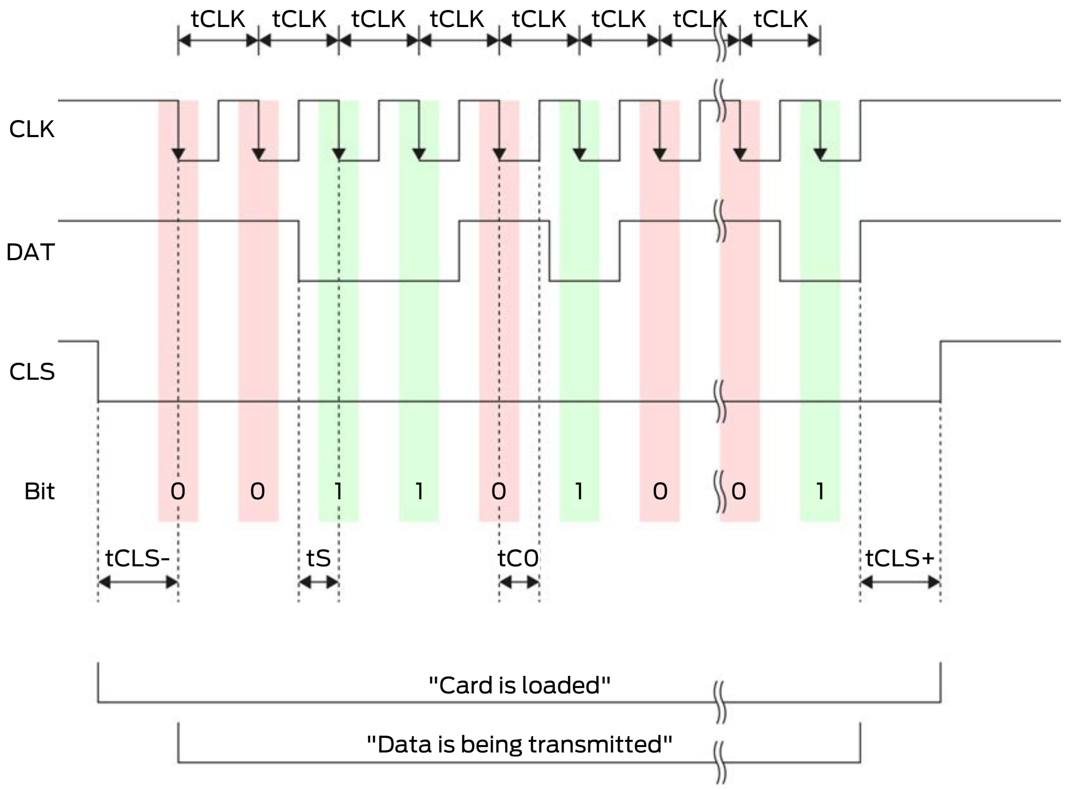
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Description	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_{S}	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Gantner-Legic)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
<15 leading zero bits> S CCCCCCCC AAAA M N BBBBBB E L <15
trailing zero bits>
```

Meaning:

S	Start character (hex B)
C	Constant (hex 1A210001)
A	Facility code (0 to 9,999)
M	Separator (hex 0)
N	Separator (hex 1)
B	User ID number (0 to 999,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

OMRON Kaba Benzing

Signal description

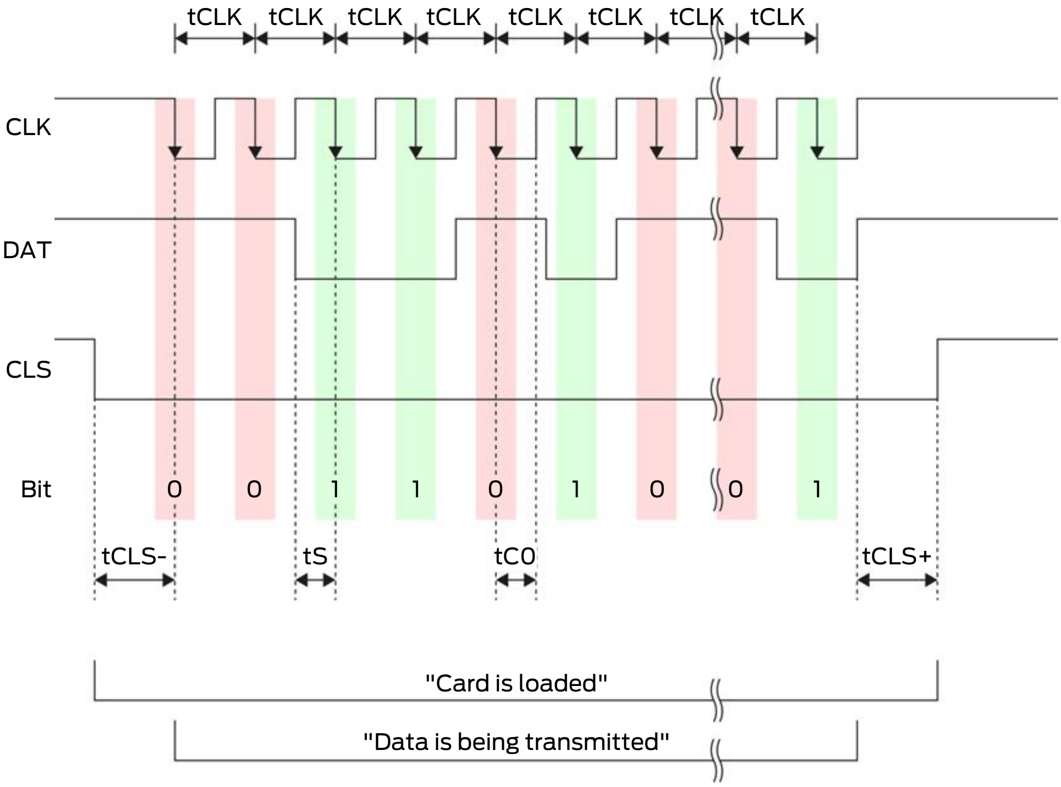
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Description	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{CO}	Clock set to “low” level (clock low)	50	100	150	µs
t_{CLS+}	Time between last data bit and de-activation of the CLS signal	8	12	20	ms

Data format (OMRON Kaba Benzing)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
<15 leading zero bits> S CCCCCCCC AAAAAAAA BBBBBB E L <15 lagging
zero bits>
```

Meaning:

S	Start character (hex B)

C	Constant (hex 00000000)
A	Facility code (0 to 99,999,999)
B	User ID number (0 to 999,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

OMRON Isgus

Signal description

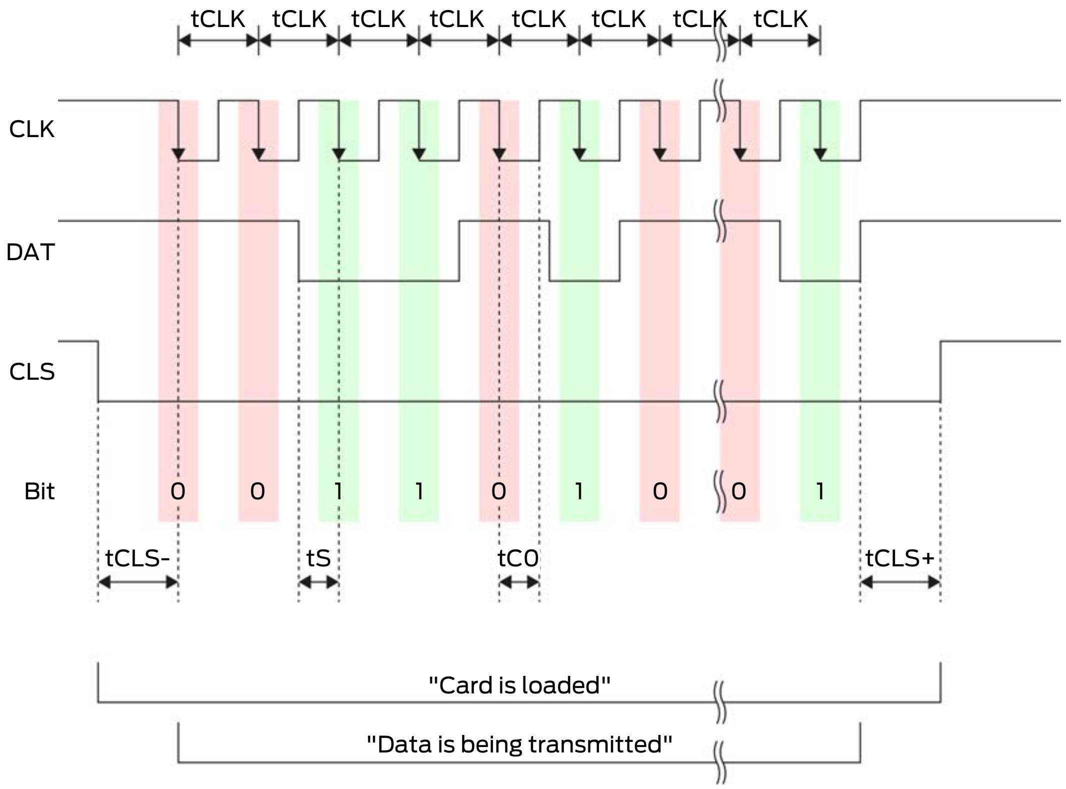
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 ("LED/ buzzer/input1")	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are "Active low". The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Isgus)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
S BBBB M AAAA E L
```

Meaning:

S	Start character (hex B)
B	User ID number (0 to 9,999)
M	5th digit of the user ID number
A	Facility code (0 to 9,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transmitted characters XOR[S...E])

8.4.5.5 Wiring in lift

Lift cabs are connected to the external system via trailing cables. The number of available lines is limited by the trailing cable type. You can save on free lines if you decide on a configuration with few lines.

IMPORTANT

Malfunctions due to voltage drop

The physically induced voltage drop in the trailing cable may cause low voltages in power supplies which come from outside the cab.

1. Take the cable length into account.
2. Switch to a version with power supply in the cab if necessary (see *Common earth with power supply [▸ 85]* and *Common earth with SREL3 components [▸ 86]*).
3. Make the cable gauge larger by merging lines in the trailing cable.

Common earth with power supply

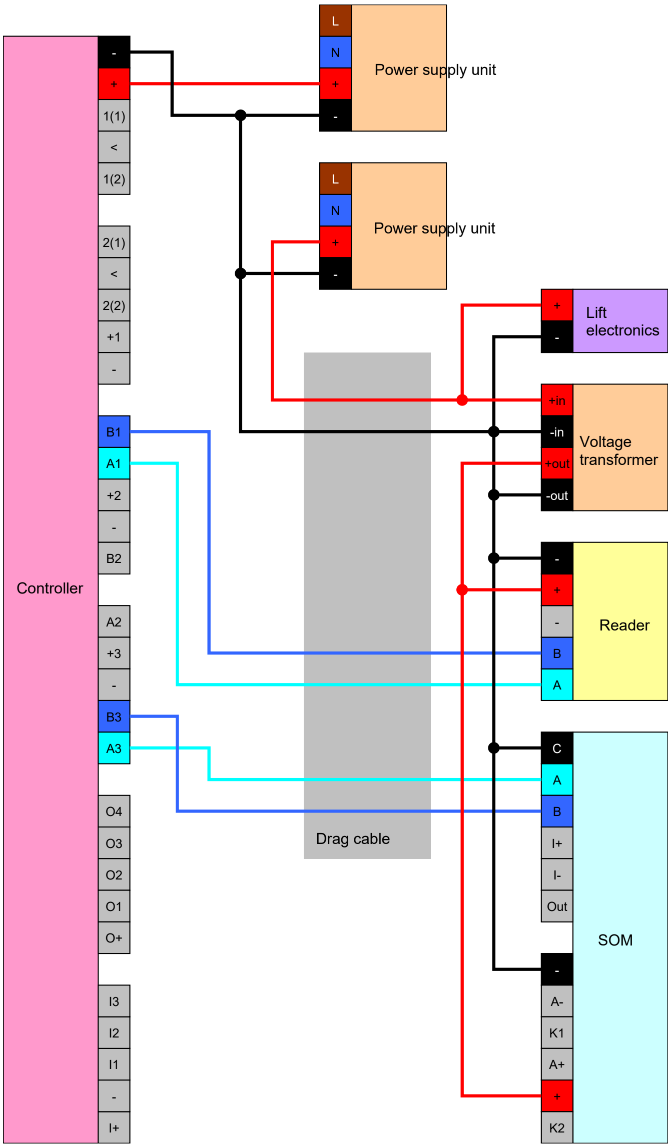
This wiring layout presupposes that the cab already has a power supply line connected to the outside world. In the cab, a voltage converter transforms the voltage and provides the power to the reader and SmartOutput modules. The power supply's earth is also used for the lift electronics as a common reference potential for data transmission between the reader, controller and SmartOutput module.

DANGER

Electric shock due to mains voltage

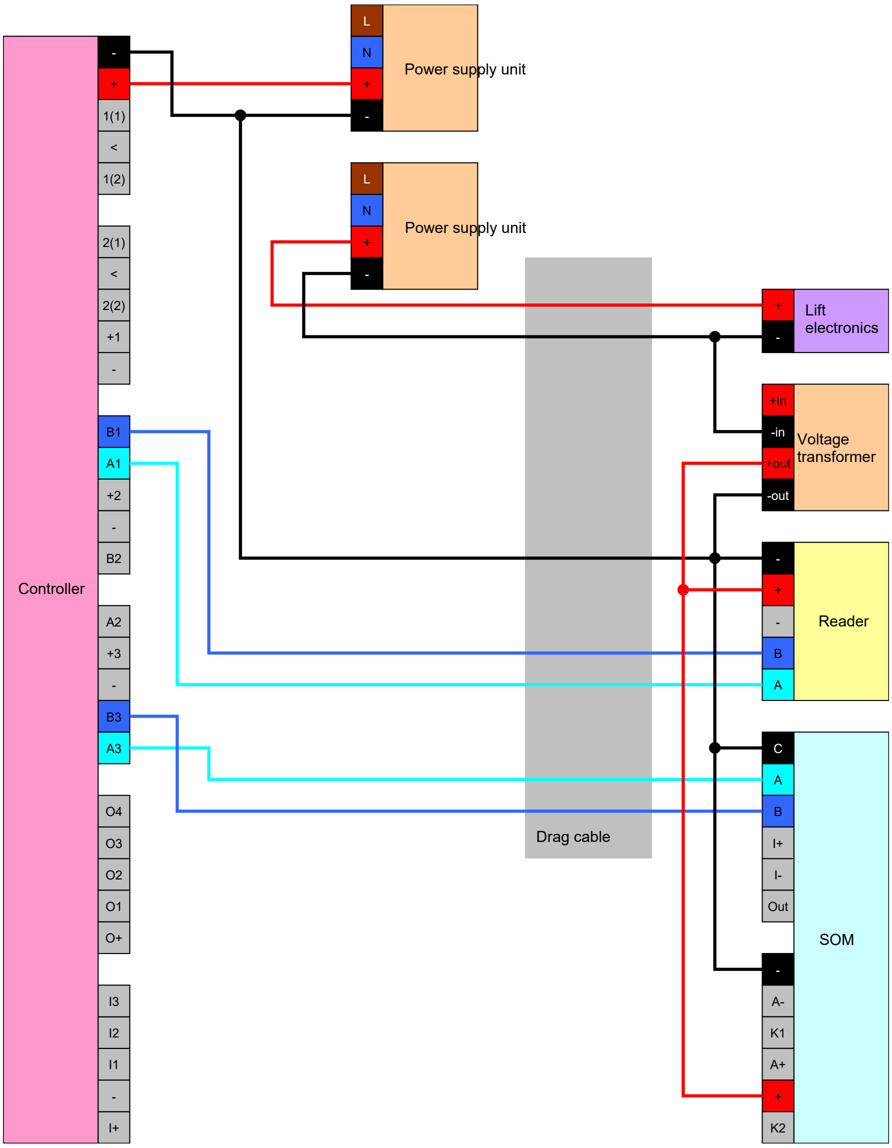
An electric shock may be caused when connecting the non-hazardous earth (low voltage) to a conductor which carries the mains voltage.

1. Only use conductors with a low-voltage potential (< 42 V) as a common earth cable!
2. Protect live cables, so people do not touch them accidentally!



Common earth with SREL3 components

This wiring layout presupposes that the cab already has a power supply line connected to the outside world. In the cab, a voltage converter transforms the voltage and provides the power to the reader and SmartOutput modules. Unlike variants with a common earth line (see *Common earth with power supply [▸ 85]*), the power supply's earth line is not used in this case; a separate line is used as a common reference potential between, the controller, reader and SmartOutput modules instead. Depending on the voltage converter design, the SREL3 ADV system can thus be disconnected from the lift electronics.



Power supply through trailing cable

If the cab does not have its own power supply (voltage too high or insufficient power reserves) or is not suitable to supply power to the SREL3 ADV system for other reasons, the power supply must be provided via the trailing cable.

Option 1: Tapping the power supply for the controller

This configuration dispenses with the need for a separate power supply unit for the reader and SmartOutput modules. The data lines are connected as described in the sections on the reader (see *Connecting one or more readers [▸ 58]*) and SmartOutput module (see *Connecting one or more SmartOutput modules [▸ 63]*).

WARNING

Overload in the power supply unit

The SmartOutput module and reader are additional power consumers. They may overload the controller's power supply unit and cause a fire.

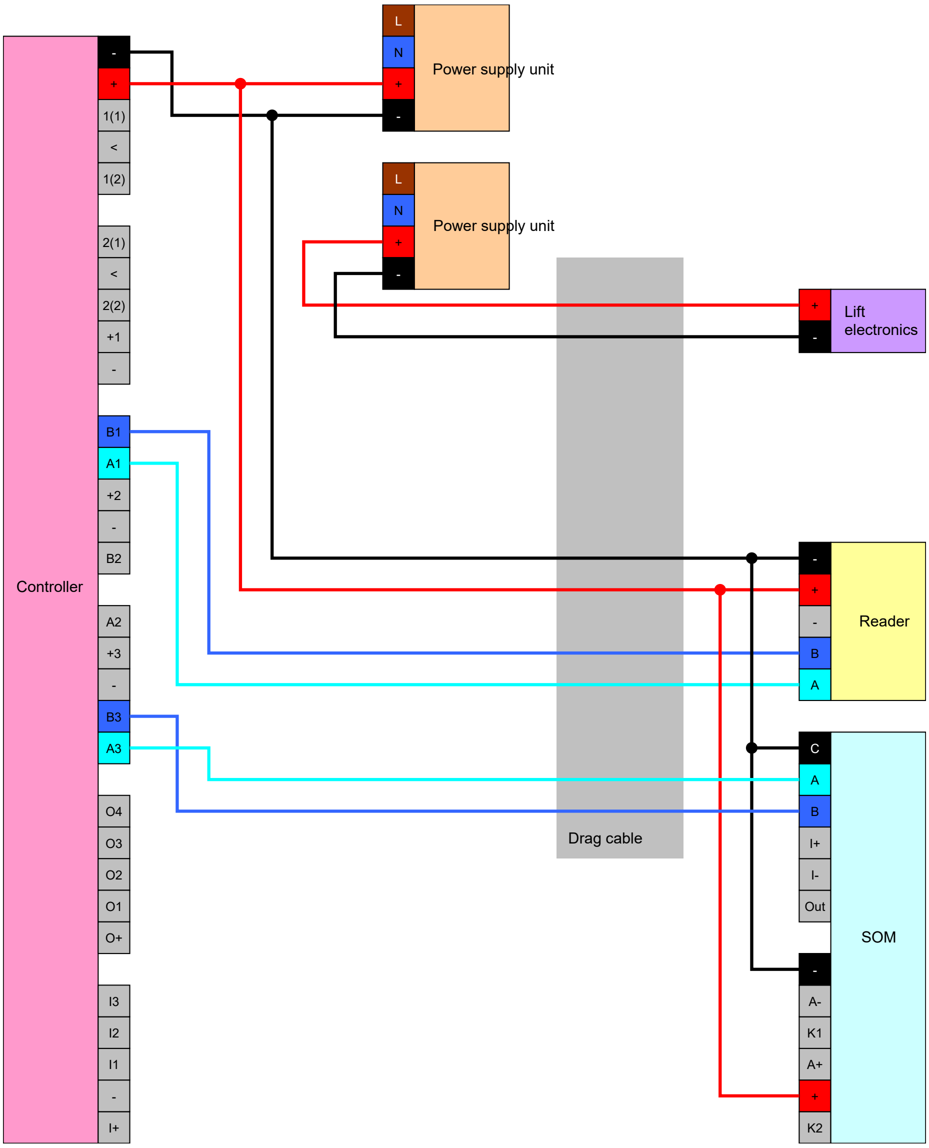
- Use a power supply unit which is designated for the total continuous currents for all connected components.

IMPORTANT

Overvoltage on the SmartOutput module

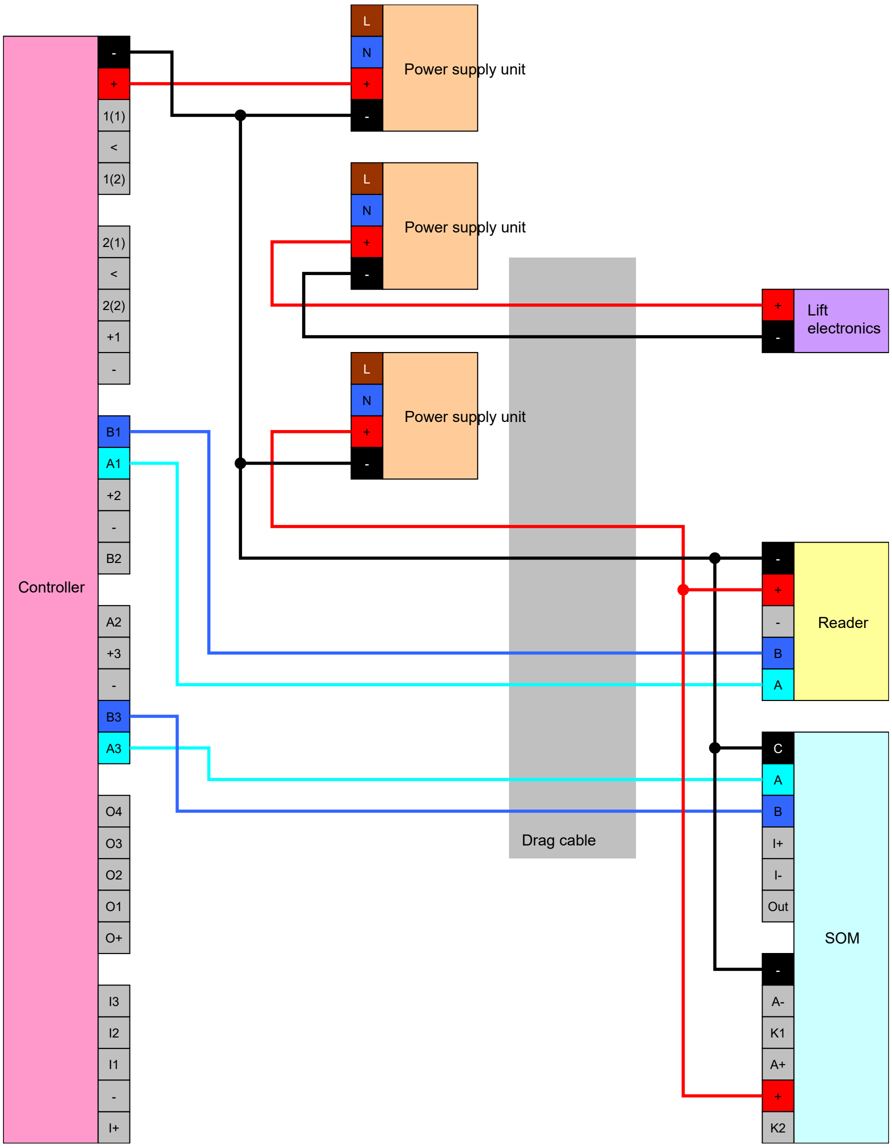
The permitted supply voltage for the SmartOutput module differs from the permitted supply voltage for the reader or controller (see *Properties [▸ 166]*).

- Use Option 2 if the controller's supply voltage is outside the range in the SmartOutput module's specifications.



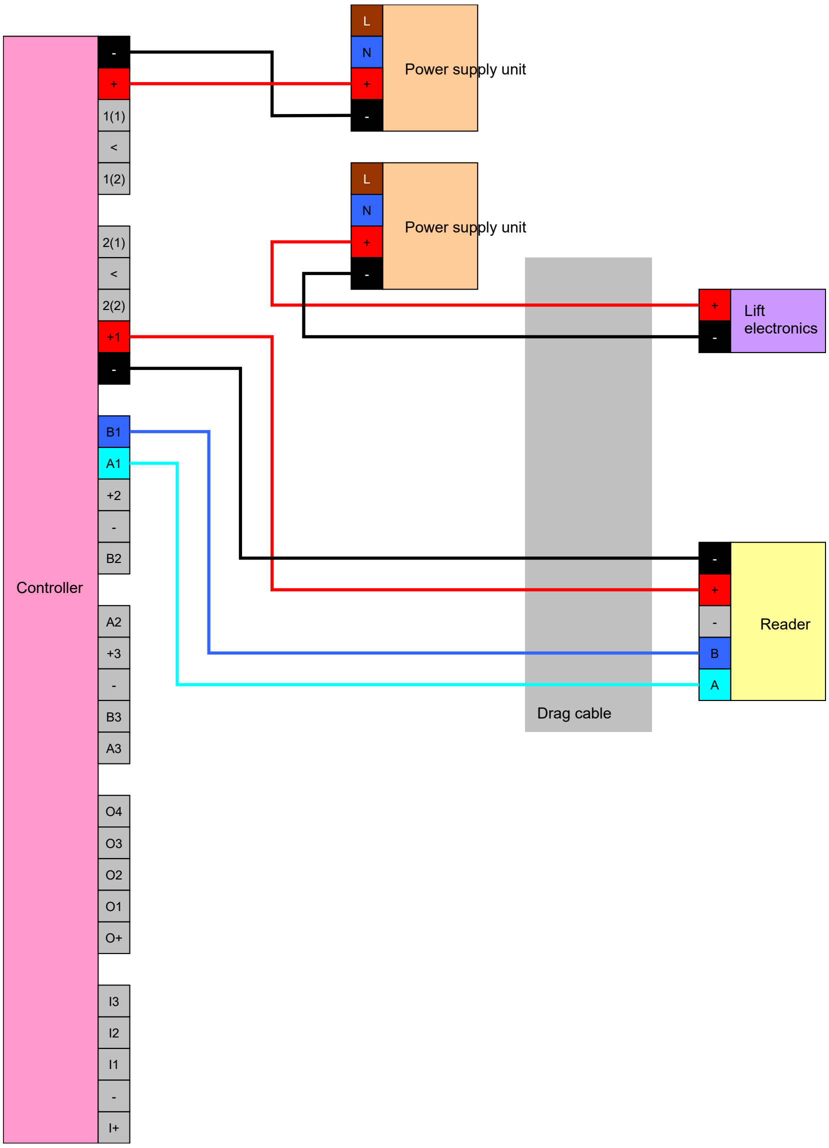
Option 2: Own power supply unit for reader and SmartOutput module

This configuration requires a separate power supply unit for the reader and SmartOutput modules. The earth systems in the controller, power supply unit and reader/SmartOutput modules must be interconnected to establish a common reference potential for data transmission.



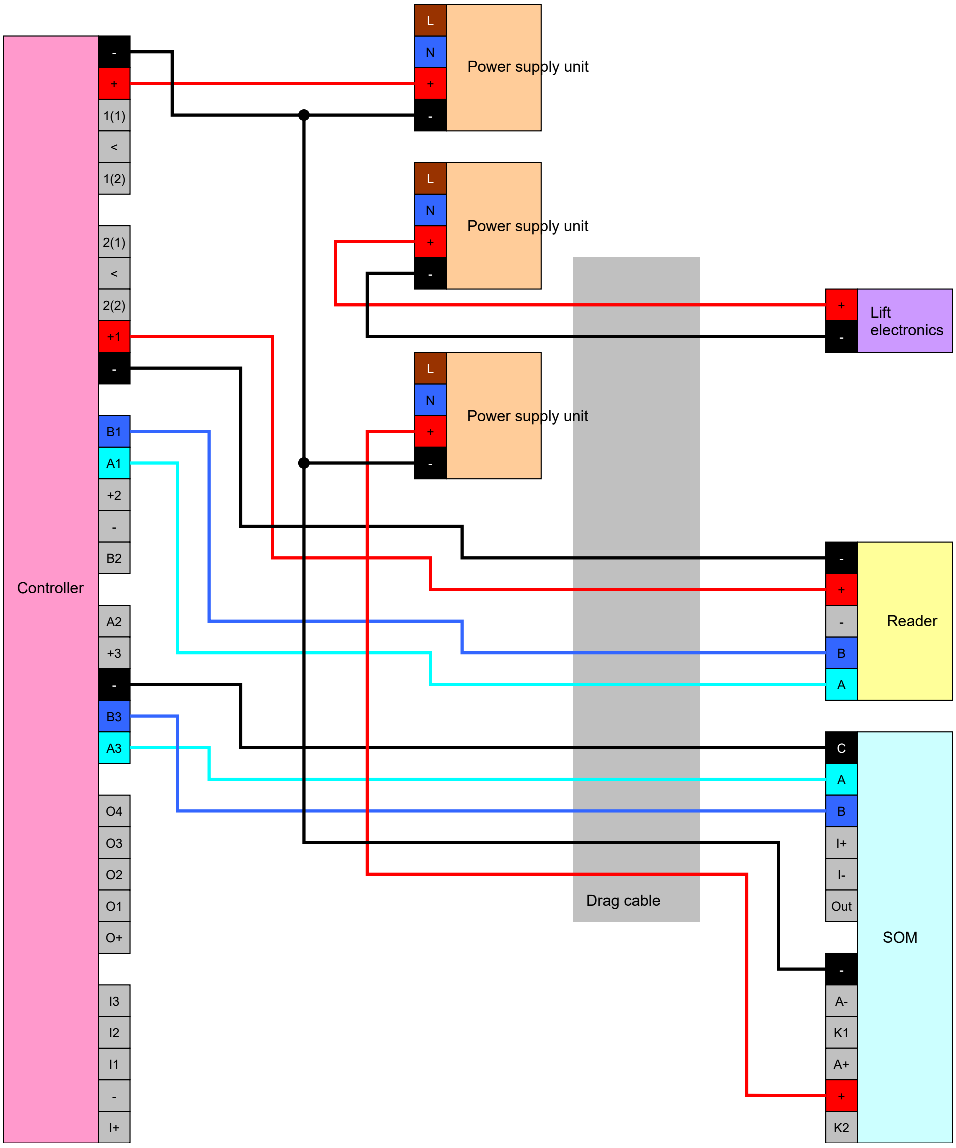
Power supply through the controller

This wiring layout can only be used if no SmartOutput modules are to be used. The reader is connected via the trailing cable as described before (see *Power supply through the controller [▸ 58]*).



Controller-fed reader with SmartOutput modules

The reader is connected as described before (see *Power supply through the controller [▸ 58]*). The SmartOutput modules are also powered via a power supply unit outside the cab. The SmartOutput modules' earth system must be connected to the controller's earth system.



NOTE

There is also no need for a power supply unit for the SmartOutput module if the controller has a 12 V_{DC} power supply unit. The SmartOutput module's V_{IN} is then not connected to its own power supply unit but to the controller's V_{IN} instead (compare *Power supply through trailing cable [▸ 87]*).

WARNING

Overload in the power supply unit

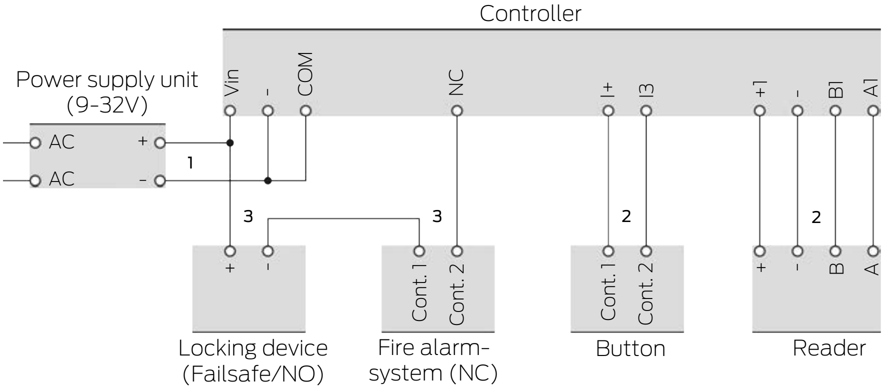
The SmartOutput module and reader are additional power consumers. They may overload the controller's power supply unit and cause a fire.

- Use a power supply unit which is designated for the total continuous currents for all connected components.

8.4.6 Block diagrams

All calculations and thus cable type recommendations refer to a voltage supply of 12 V.

Currentless open closing (failsafe) with fire alarm system, push-button and reader



The used locking device opens when it is disconnected from the power. In the normal state the contacts of the fire alarm system are connected to each other and the relay contacts of the SmartRelay are also connected to each other. The current can flow from the power supply unit through the locking device, through the contacts of the fire alarm system and the relay contacts of the SmartRelay. The locking device remains closed.

If the circuit of the locking device is interrupted, the locking device opens. Possible causes:

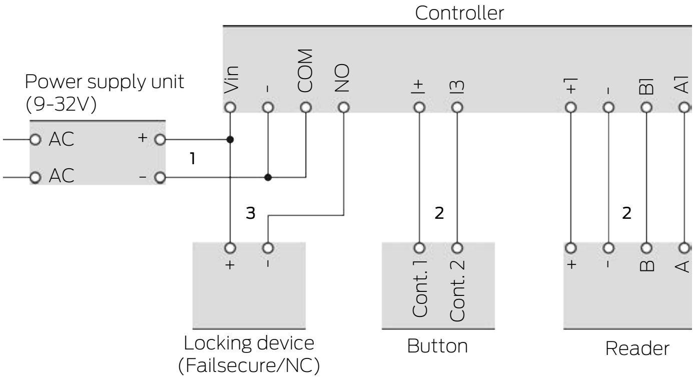
- An authorised identification device is activated on the reader. The relay contact of the SmartRelay opens.
- The button is actuated. The relay contact of the SmartRelay opens.
- The fire alarm system detects a fire. The contacts of the fire alarm system are no longer connected.
- The power fails (for example due to a fire).
- A remote opening of the SmartRelay is performed.

You can use the following cable types under the following conditions. (For detailed wiring information, see *Information on cabling [▸ 176]*).

Number	Framework conditions	Cable type
1	Cable length power supply unit to controller ≤ 15 m (15 m outward and 15 m return)	F-YAY 2x2x0.6

Number	Framework conditions	Cable type
2	Cable length controller to reader (or controller to button) ≤ 15 m (15 m outward and 15 m return)	CAT5, shielded
3	- Connection directly to the power supply unit - Cable length power supply unit-locking device-fire alarm system controller ≤ 50 m (50 m outward and 50 m return) - Locking device suitable for 9 V_{DC} to maximum power supply, maximum power of the locking device ≤ 4.5 W	F-YAY 2x2x0.6

Currentless closed closing (fail-secure) with button and reader



The used locking device opens when it is supplied with power. Normally the relay contacts of the SmartRelay are not interconnected. Current cannot flow from the power supply through the SmartRelay relay contacts to the locking device. The locking device remains closed.

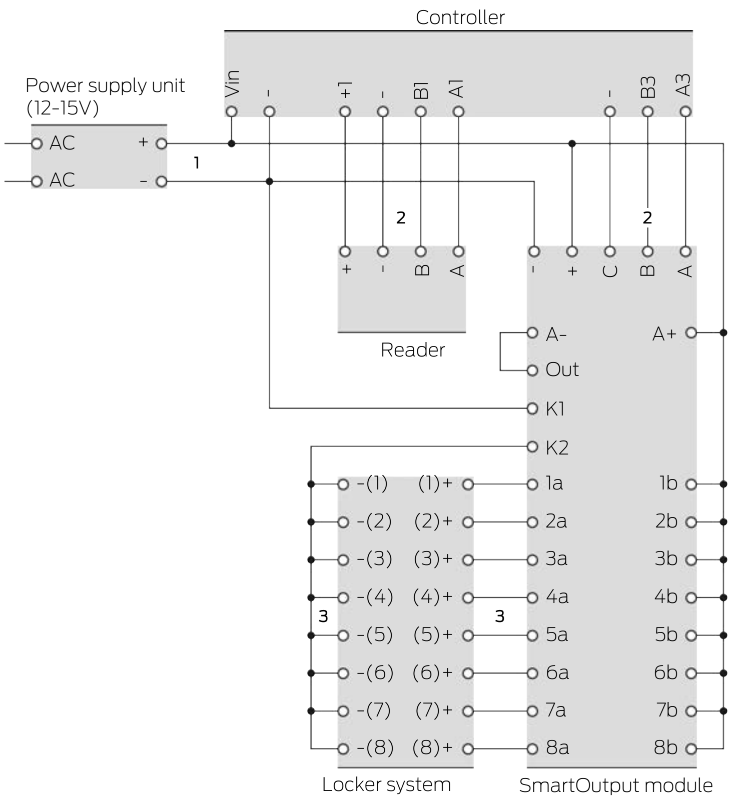
When the circuit of the locking device is closed, the locking device opens. Possible causes:

- An authorised identification device is activated on the reader. The relay contact of the SmartRelay closes.
- The button is actuated. The relay contact of the SmartRelay closes.
- A remote opening of the SmartRelay is performed.

You can use the following cable types under the following conditions. (For detailed wiring information, see *Information on cabling [▸ 176]*).

Number	Framework conditions	Cable type
1	Cable length power supply unit to controller ≤ 15 m (15 m outward and 15 m return)	F-YAY 2x2x0.6
2	Cable length controller to reader (or controller to button) ≤ 15 m (15 m outward and 15 m return)	CAT5, shielded
3	- Connection directly to the power supply unit - Cable length power supply unit-locking device-controller ≤ 50 m (50 m outward and 50 m return) - Locking device suitable for 9 V_{DC} to maximum power supply, maximum power of the locking device ≤ 4.5 W	F-YAY 2x2x0.6

Locker system with direct cabling



The locker of the locker system opens when power is supplied to the locker locking device. Normally, the contacts of the SmartOutput module are open and the current does not flow through the contacts of the SmartOutput module to the locker locking devices. When the contact on the SmartOutput module is closed, the locker opens. Possible causes:

- An authorised identification device is activated on the reader. The relay contact of the SmartOutput module closes.
- The button is actuated. The relay contact of the SmartOutput module closes.
- A remote opening of the SmartRelay is performed.

You can use the following cable types under the following conditions. (For detailed wiring information, see *Information on cabling [▸ 176]*).

Number	Framework conditions	Cable type
1	Cable length power supply unit to controller ≤ 15 m (15 m outward and 15 m return)	F-YAY 2x2x0.6

Number	Framework conditions	Cable type
2	Cable length controller to reader ≤ 15 m (15 m outward and 15 m return)	CAT5, shielded
3	- Connection directly to the power supply unit - Cable length power supply SmartOutput module ≤ 53 m (53 m outward and 53 m return) - Total length of the current path Power supply unit-K1-K2-[-(1)]-[+(1)] ≤ 66 m - Locker system locking devices suitable for 9 V_{DC} up to maximum power supply, maximum power of one locking device ≤ 4.5 W	F-YAY 2x2x0.6

9. Installation

9.1 Controller

The controller can be installed horizontally or vertically. You can use the integrated fastening holes to install it safely and easily in a horizontal position (see *Drilling templates [▸ 181]*).

IMPORTANT

Adverse effect on reception due to interferences

This device communicates wirelessly. Wireless communication can be affected or may fail due to metal surfaces or interference.

1. Do not fit the device to metal surfaces.
2. Keep the device away from sources of electrical or magnetic interference.

Unauthorised access

The relay in the controller can be short-circuited by unauthorised persons.

- Mount the controller with the relay in an environment that is protected against unauthorised access.

Unauthorised switching of the relay by magnet

The relay can switch unintentionally due to strong magnets nearby.

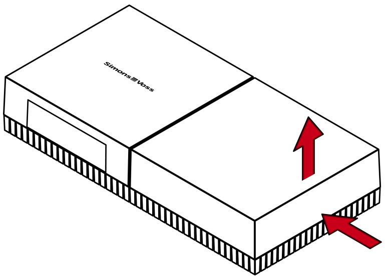
1. Mount the controller with the relay in an environment that is inaccessible to unauthorised persons with magnets.
2. Alternatively, operate the relay permanently activated (invert output and use NC+COM instead of NO+COM).

Malfunctions due to weather conditions

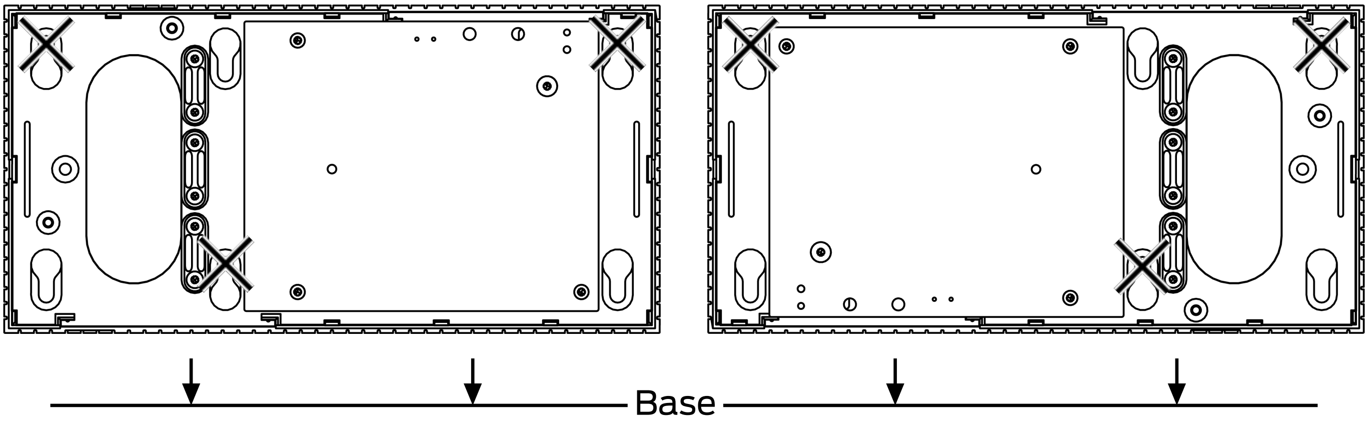
The controller is not protected against splash water and other weather influences.

- Mount the controller in an environment that is protected from the weather.

1. Push in the housing cover as shown and remove the cover.



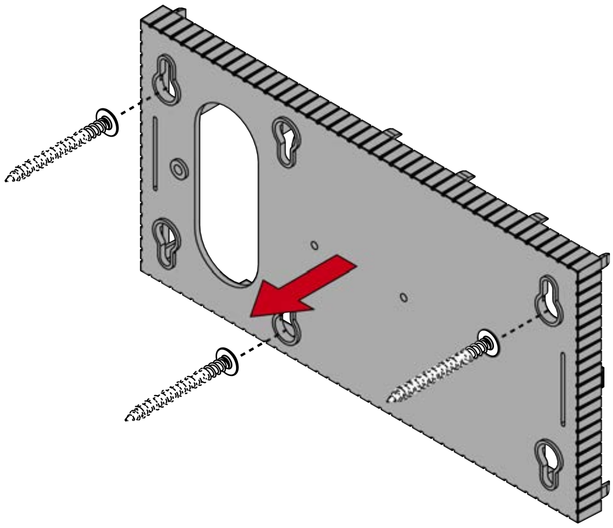
2. Hold the base plate in the required position and mark the drill holes.



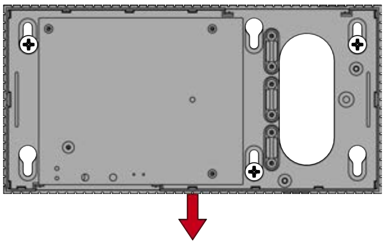
Version 1: Left-hand opening

Version 2: Right-hand opening

3. Drill the required holes with a suitable drill.
4. Use suitable dowels and fasten the screws for the base plate into position.
5. Place the base plate so that the screw heads are fed through the recesses.



6. Slide the base plate so that the screw heads slide along the grooves.



CAUTION

Additional fixation for ceiling mounting

The device may fall from the ceiling.

- Tighten the screws after sliding on the base plate.

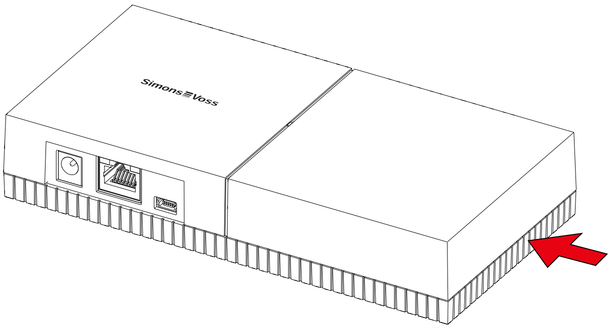
7. Place the cover on the base plate again.

↳ Installation completed.

If necessary, you can also modify the housing:

✓ Power supply disconnected.

1. Push the ribbed area laterally inwards and remove the housing cover.



2. Check the required width of the housing opening. The height of the opening is approx. 7 mm. Each removed bar widens the opening by 4 mm.
3. Select a location where you want to remove the bars.

IMPORTANT

Insufficient fit due to removed clips

The housing cover is positioned and held by clips on the webs. If you saw off or break off these clips, the housing cover will no longer be held at this point.

1. Do not remove any bars that have a clip over them.
2. Do not damage clips during sawing.

4. Use a suitable saw to saw through the bars at both ends of the desired opening to the base plate.
5. Bend the bars back and forth at the desired opening until the bars break.

↳ The housing is designed to be mounted on a surface.

9.2 Reader

The reader can be mounted in any position.

IMPORTANT

Adverse effect on reception due to interferences

This device communicates wirelessly. Wireless communication can be affected or may fail due to metal surfaces or interference.

1. Do not fit the device to metal surfaces.
2. Keep the device away from sources of electrical or magnetic interference.

Malfunctions due to weather conditions

In the standard version, the reader is not protected against splash water and other weather influences.

1. If you want to use the reader in an environment that is not protected against splash water, use the WP variant.
2. Ensure complete protection against splash water by means of additional sealing.

Transmission errors due to unshielded cable

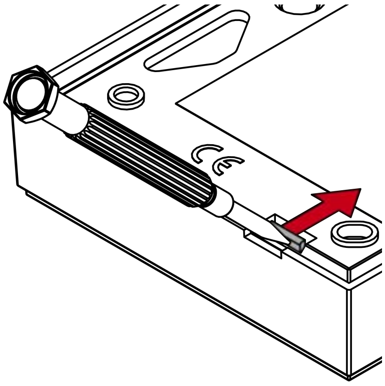
Unshielded cables are more susceptible to interference.

- Use shielded cables for the connection to the reader (see *Information on cabling [▸ 176]* and *Block diagrams [▸ 93]*).

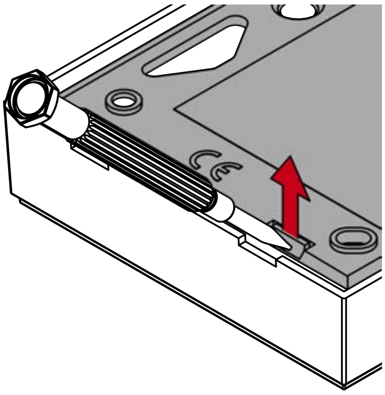
The following graphics and instructions refer to the LED reader. A normal reader is installed in a similar way.

✓ Have a slotted-head screwdriver ready.

1. Place the reader on the lid.
2. Use a slotted-head screwdriver to push one of the clips inwards.

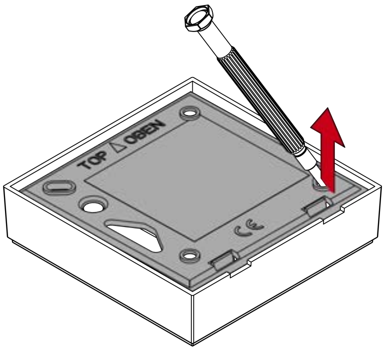


3. Press and hold the clip down and use the slotted screwdriver to slide the base plate upwards.



   ↳ Clip stays pressed down.

4. Do the same with the other clip.
5. Insert the screwdriver into the hole and lever the base plate out of the lid.



   ↳ Base plate and lid are separated.

6. Fasten the base plate in its required location (see *Determining installation position for an external reader [▸ 102]*).
7. Wire the reader (see Connections).
8. Place the lid on the base plate again.

↳ Reader is installed.

9.2.1 Determining installation position for an external reader

The type of identification media used determines the external reader installation position.

Active ID media (transponders) have a wider read range than passive ID media (cards).

9.2.1.1 Use of transponders

The transponder-to-reader range (read range) extends up to 100 cm.

Readers are able to communicate through materials such as wood, steel and concrete when used with active transponders. The reader can be mounted either on the inside or on the outer side.

NOTE

A transponder's read range may be reduced due to interference in the surrounding area.

Strong magnetic fields can shorten the read range. Aluminium structures may block communication between the transponder and reader.

You can enable the ☑ Close-up range mode option in the LSM software. This option reduces the B field reader range, reduces the impact from possible sources of interference and can prevent a transponder from overmodulating.

9.2.1.2 Use of cards

The card-to-reader range (read range) extends up to 1.5 cm.

Direct contact must be established between the card and reader once the reader is mounted.

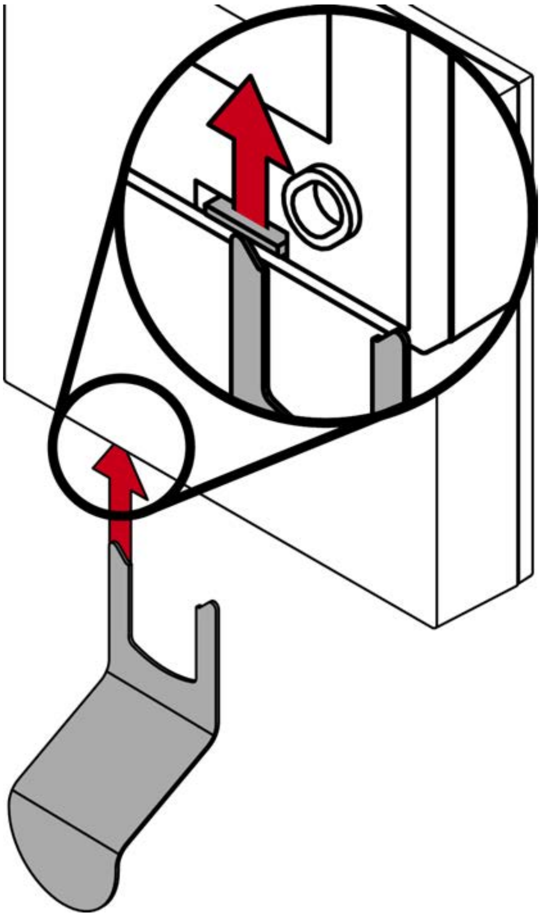
9.2.2 Opening the housing

The housing is secured by two catch lugs. These latches can be pressed in with a pointed, flat object and remain engaged as long as the cover is in place. When the housing is correctly mounted, the lugs are on the underside.

✓ SmartHandle tool, flat-bladed screwdriver or similar object.

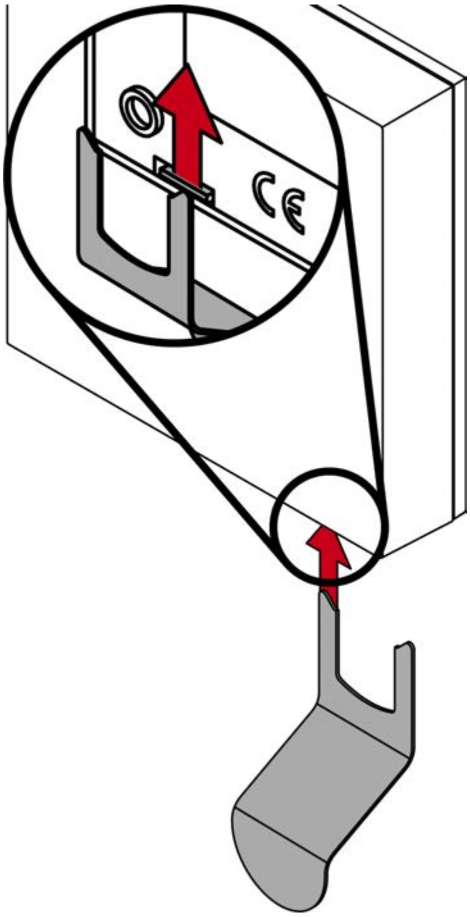
1. Carefully pull the cover while performing the following steps.

2. Press one of the two locking lugs upwards using the SmartHandle tool.



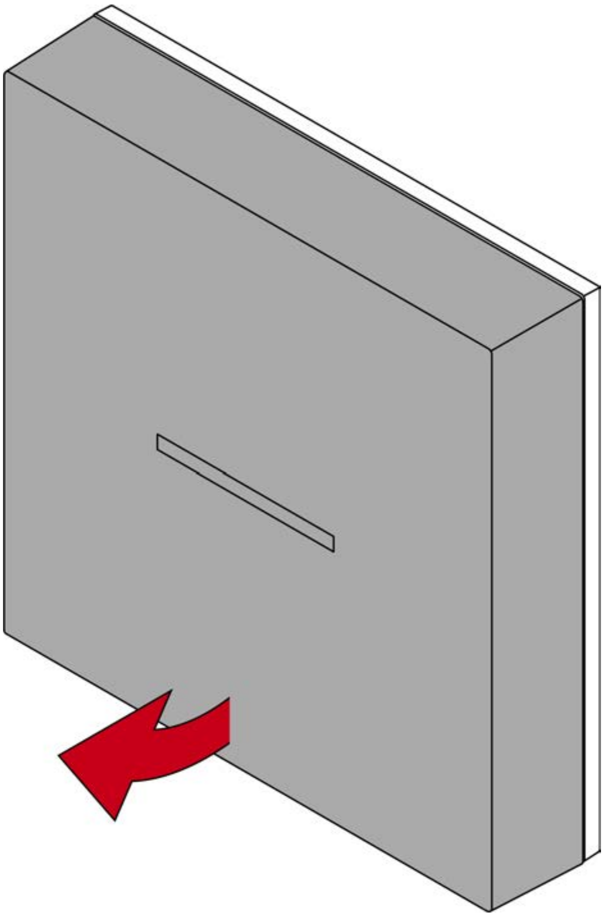
↳ The lug remains pressed in.

3. Push the second locking lug upwards using the SmartHandle tool.

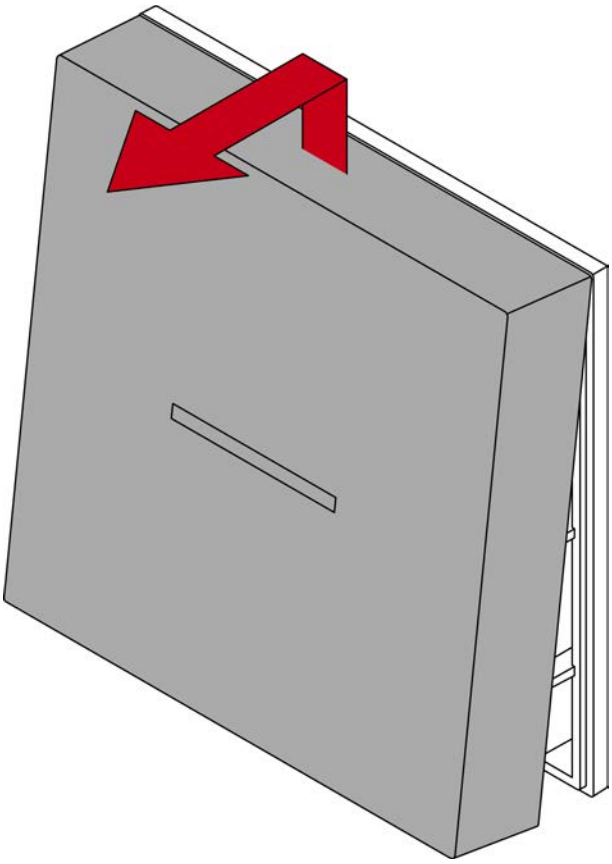


↳ Both catch lugs are pressed in.

4. Fold the cover upwards.



5. Remove the lid.



9.3 SmartOutput module

The SmartOutput module is designed for fitting onto a DIN rail.

10. SREL3 ADV in LSM

10.1 Changing over from SREL2 to SREL3.ADV

It is possible to change between SmartRelay system generations. Contact Support to ensure a smooth changeover process (see Help and contact).

10.2 Access list

NOTE

The access list is only available in the .ZK version.

10.2.1 Import access list

The SmartRelay 3 can be configured in such a way that all identification attempts, including unauthorised ones, are saved to the access list. You can read this access list. Access list readouts can also be automated in Task Manager (see LSM manual).

10.2.1.1 Reading the access list with USB cable

Proceed as follows if you wish to read the access list using a USB connection:

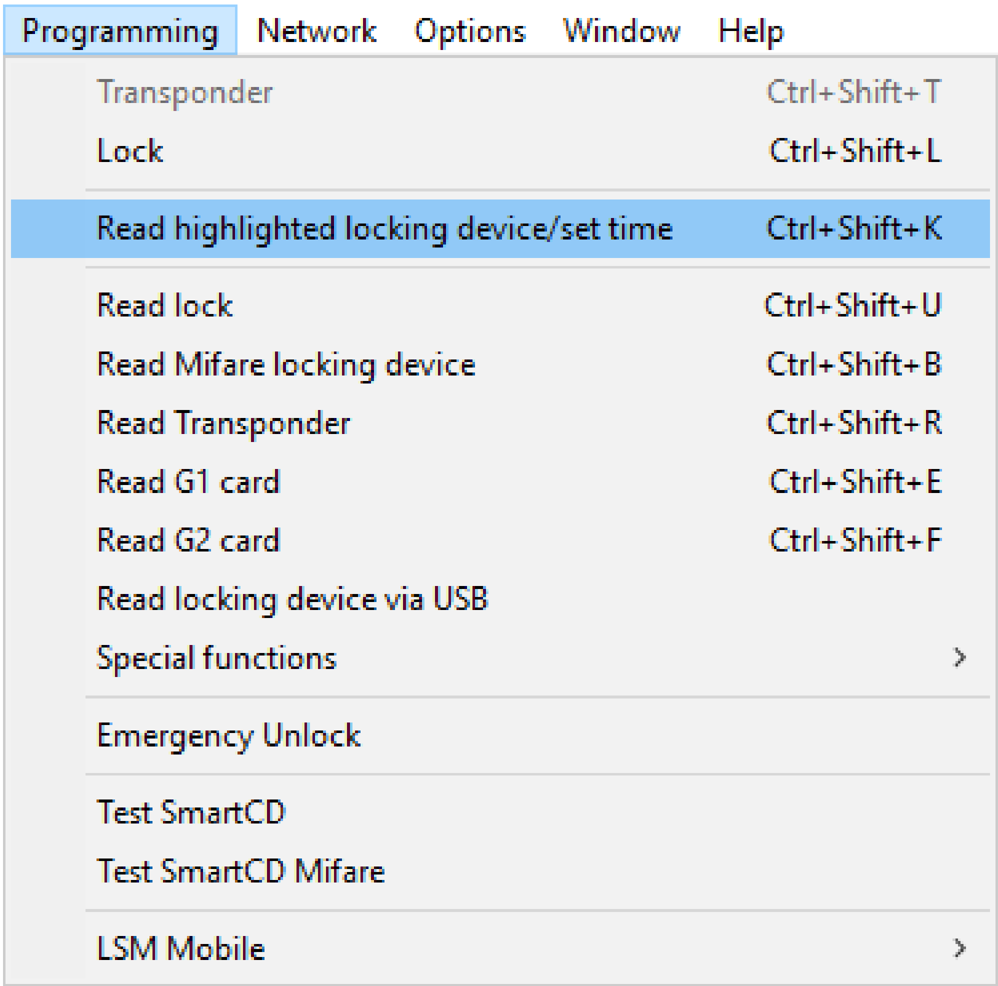
✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

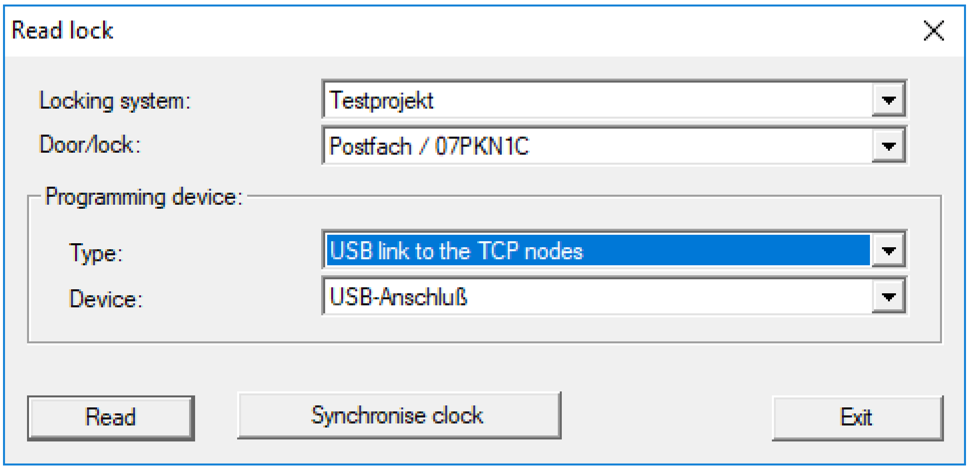
✓ Controller connected to computer with USB cable.

1. Mark the entry on the SmartRelay 3 controller in the matrix.

2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile

↳ The "Read lock" window will open.


Read lock

Locking system: Testprojekt

Door/lock: Postfach / 07PKN1C

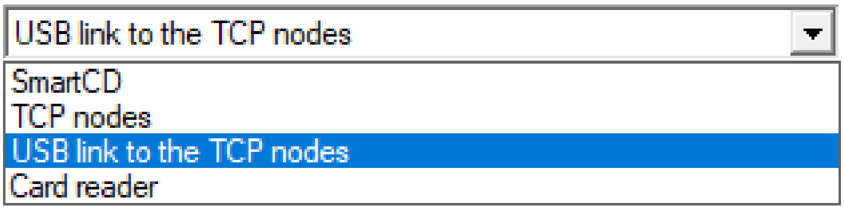
Programming device:

Type: USB link to the TCP nodes

Device: USB-Anschluß

3. Open the ▼ **Type** drop-down menu.

4. Select the "USB link to the TCP nodes" item.



5. Click on the Read button.
   ↳ "G2 SmartRelay 3" window opens.
6. Click on the Read button.
7. Click on the Audit Trail button.

↳ Access list is displayed.

10.2.1.2 Reading the access list over network

Proceed as follows if you wish to read the access list using a network connection:

✓ Components wired correctly (see *wiring [▸ 58]*).

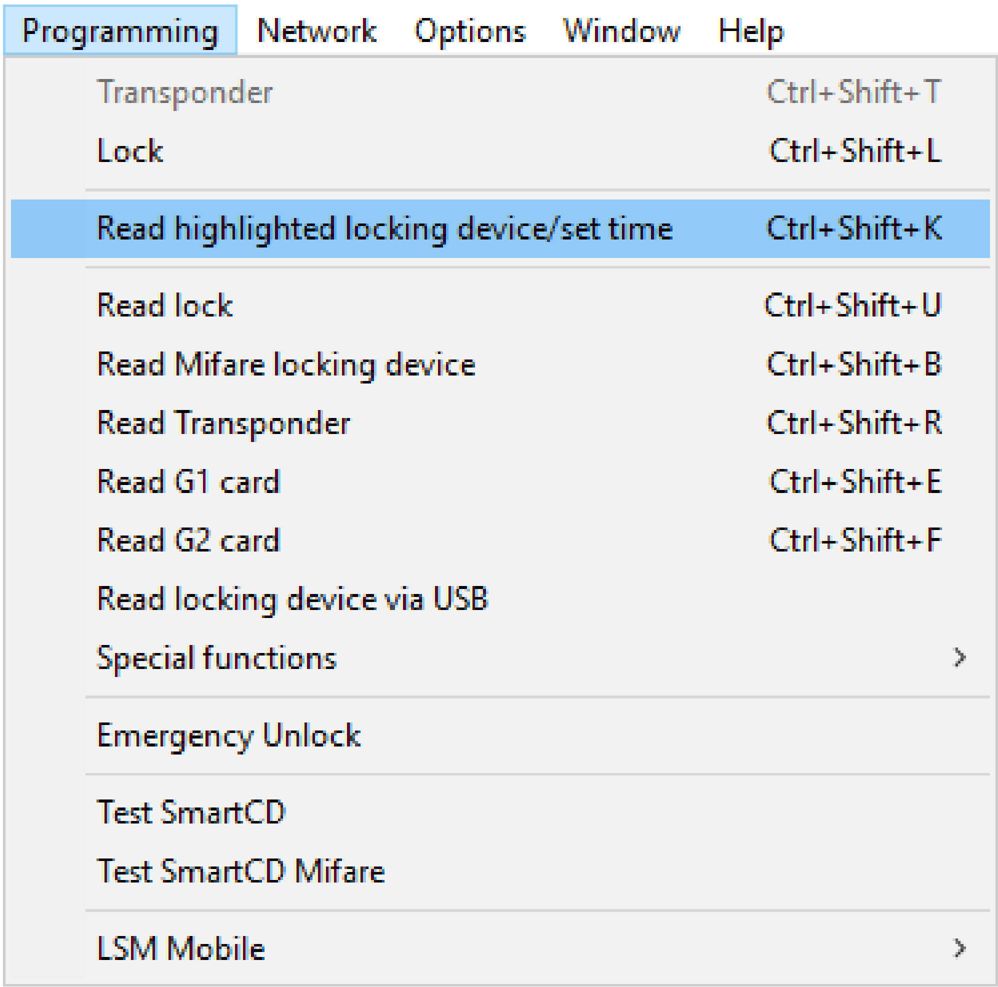
✓ Components connected to power.

✓ Controller has already been programmed.

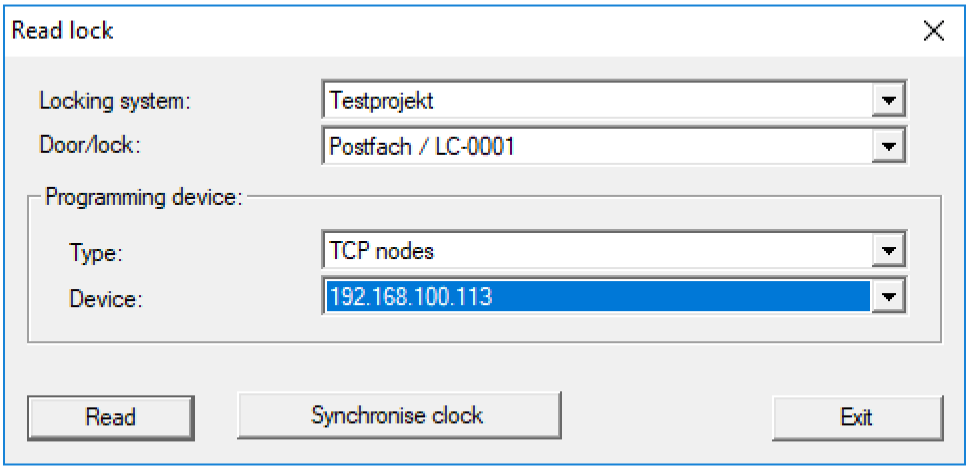
✓ Controller connected to computer via network.

1. Mark the entry on the SmartRelay 3 controller in the matrix.

2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile

↳ The "Read lock" window will open.


Read lock

Locking system: Testprojekt

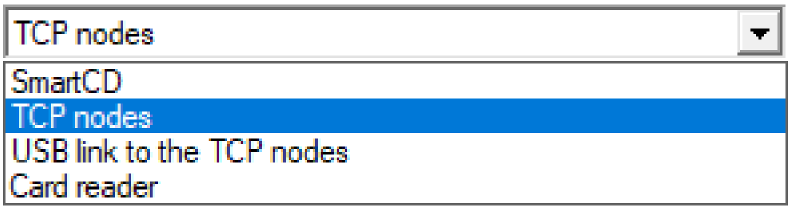
Door/lock: Postfach / LC-0001

Programming device:

Type: TCP nodes

Device: 192.168.100.113

3. Open the ▼ **Type** drop-down menu.



4. Select the "TCP nodes" item.
5. Click on the Read button.
   ↳ Locking device is read.
   ↳ The "G2 Smart Relay 3" window will open.
6. Click on the Read button.
7. Click on the Audit Trail button.

↳ Access list is displayed.

10.2.2 Resetting the access list

If you wish to delete the access list permanently, you must delete it in LSM and in the controller. The access list is synchronised between the controller and LSM and stored in both. The controller features a built-in memory module for this purpose.

10.2.2.1 Resetting the access list with USB cable

Deleting the access list in the controller

Reset the controller (see *Resetting controller with a USB cable [▸ 33]*).

Deleting the access list in LSM

1. Double-click on the entry in the matrix to open the settings for SmartRelay 3.
2. Change to the [Audit trail] tab.
3. Click on the Delete Audit Trail button.
4. Press on OK to accept query.

↳ Access list is now deleted.

Programming the controller

Resetting the controller results in a programming requirement. Execute programming for the controller (see *Programming [▸ 29]*).

10.2.2.2 Resetting the access list over network

Deleting the access list in the controller

Reset the controller (see *Resetting controller over the network [▸ 35]*).

Deleting the access list in LSM

1. Double-click on the entry in the matrix to open the settings for SmartRelay 3.
2. Change to the [Audit trail] tab.
3. Click on the Delete Audit Trail button.
4. Press on OK to accept query.

↳ Access list is now deleted.

Programming the controller

Resetting the controller results in a programming requirement. Execute programming for the controller (see *Programming [▸ 29]*).

10.2.3 Event logging of unauthorised accesses

Only authorised accesses are logged in storage mode. There is an option to log unauthorised access attempts too.

✓ LSM 3.4 or higher installed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enable the ☑ Log unauthorised attempts checkbox.
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming (see *Programming [▸ 29]*).

↳ Unauthorised access attempts are now also logged.

10.3 Flip-flop

The switching time for the relay in the controller can be freely programmed between 0 s and 25 s. If the controller relay needs to be permanently operated, you can activate flip-flop mode.

IMPORTANT

Changing over the relay contact if power fails

The relays in the controller are not bi-stable. Consequently, permanent power is required for switched mode. Relays are no longer supplied with electricity if there is a power outage. In such cases, they switch to a power-off state even without using an identification medium, depending on the original position.

- Connect external components in such a way that a power-off state poses no risks.

NOTE

The flip-flop option is not available if the SREL3 ADV system is used with SmartOutput modules.

✓ LSM 3.4 SP1 or higher installed.

✓ Components connected to power.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Controller has already been programmed.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enable the ☑ Flip Flop checkbox.
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming (see *Programming [▸ 29]*).

↳ Flip-flop mode is activated.

10.4 Time budgets

Time budgets are a convenient way to ensure regular identification media updating in the virtual network. If a time budget is issued, which must be uploaded to a gateway, users are forced to use their identification medium on the gateway on a regular basis. During this process, not only is the time budget uploaded, but other updates are also transmitted.

Identification media may become lost or stolen. Issuing a time budget ensures that identification media are automatically no longer authorised on the locking devices, because their time budget can no longer be uploaded once rights are withdrawn. Issuing a time budget thus increases security in the locking system.

10.4.1 Time budget template for new locking system identification media

- ✓ Controller has already been programmed.
- ✓ Components wired correctly (see *wiring [▸ 58]*).
- ✓ Components connected to power.
- ✓ Controller linked to the computer via USB or TCP/IP.
- ✓ Virtual network set up.
- ✓ Controller set up as a gateway.

1. Click on the ... button.
2. Change to the [Name] tab.
3. Select one of the options in the "Dynamic time window for G2 transponder" section.
4. Enter the number of hours if required.
5. Click on the Apply button.
   ↳ Global time budget set.
6. Click on the Exit button.
7. Execute programming (see *Programming [▸ 29]*).

↳ Newly created identification media automatically apply this time budget setting when they are created.

NOTE

If a differing time budget or even no time budget is to be assigned to identification media which have already been created, you can issue them a time budget on an individual basis.

1. Double-click on the entry in the matrix to open the identification medium's properties.
2. Switch to the [Configuration] tab.
3. Issue an individual time budget in the "Dynamic time window" section.
4. Click on the Transmit button.
5. Click on the Exit button.

↳ Individual time budget assigned.

10.4.2 Ignoring activation/expiry date

Identification media can be given a validity date. This validity date can be ignored if identification media need to be used regardless.

✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enable the ☑ Ignore activation or expiry date checkbox.
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming (see *Programming [▸ 29]*).

10.5 Consequences in the event of a network failure

If the network fails, only part of the information will still be transferred:

- Time budgets and buffer-stored block IDs are still transmitted from the controller to the identification media. The locking system continues to function.
- Block feedback signals are transmitted from the identification media to the controller. The physical access list is also transmitted to the controller in the case of cards. All information is buffered in the controller. Once connection is re-established, the controller transmits the stored information to LSM.
- Authorisation changes are not edited in the virtual network.
- Input events are not transmitted to the database and expire.

10.6 Signal settings

In some cases, an optical or audible feedback signal may not be wanted. You can also change signal settings as you wish.

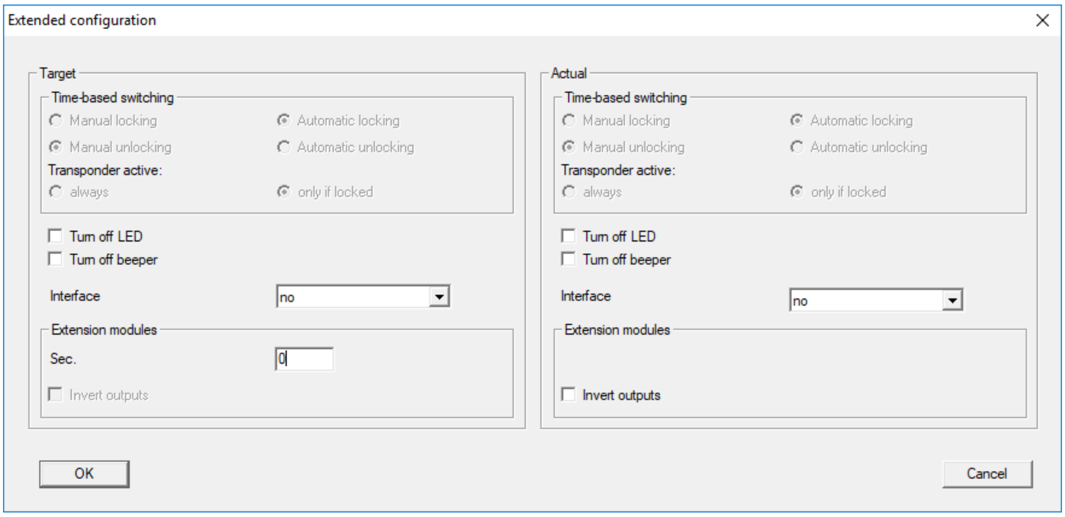
✓ LSM 3.4 or higher installed.

✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Click on the Extended configuration button.
   ↳ The "Extended configuration" window will open.



Extended configuration

Target

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

Sec.: 0

□ Invert outputs

Actual

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

□ Invert outputs

4. Enable or disable the ☑ Turn off LED checkbox.
5. Enable or disable the ☑ Turn off beeper checkbox.
6. Click on the OK button.
   ↳ Window closes.
7. Click on the Apply button.
8. Click on the Exit button.
9. Execute programming (see *Programming [▸ 29]*).

↳ Signalling has been adjusted.

10.7 Operation as interface

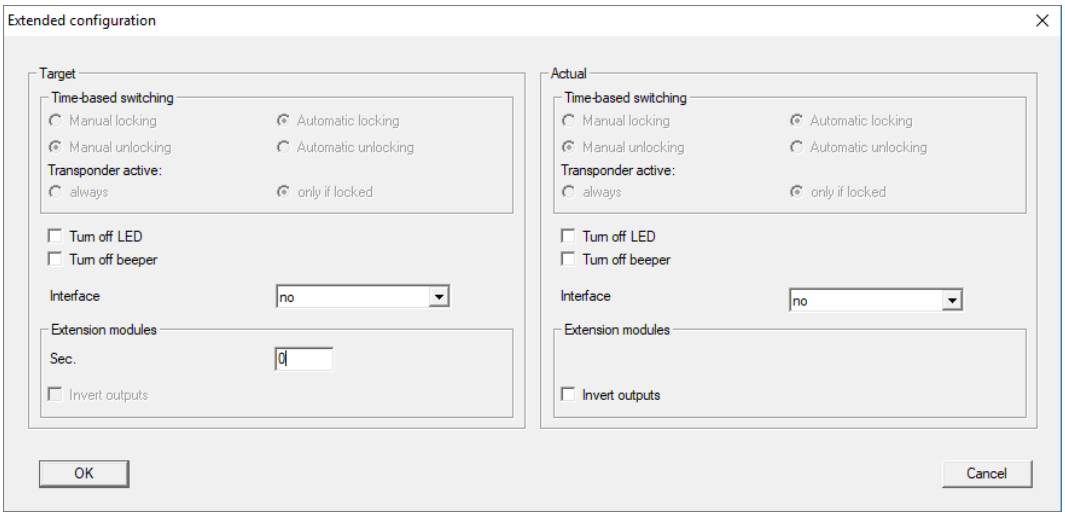
The SREL3 ADV system can be used to actuate a third-party system with identification media. You can select the specified interfaces for this purpose (see *Controller [▸ 166]*). See *Using the serial interface [▸ 65]* on wiring. You can receive detailed specifications on the interfaces offered from Support (see Help and contact). If data need to be transferred via the serial interface, then the serial interface needs to be enabled and the corresponding protocol configured:

✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Click on the Extended configuration button.
   ↳ The "Extended configuration" window will open.



Extended configuration

Target

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

Sec.: 0

□ Invert outputs

Actual

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

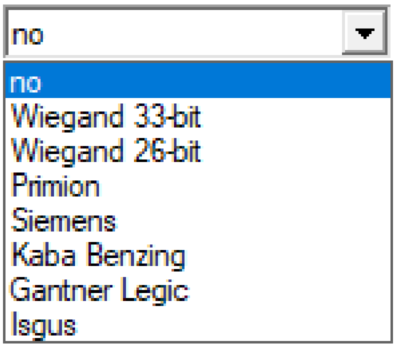
□ Turn off beeper

Interface: no

Extension modules

□ Invert outputs

4. Open the ▼ **Interface** drop-down menu.
5. Select the entry which corresponds to your third-party system.



6. Click on the OK button.
   ↳ Window closes.
7. Click on the Apply button.
8. Click on the Exit button.
9. Execute programming (see *Programming [▸ 29]*).

↳ Data are emitted via the serial interface.

10.7.1 Specifications for the serial interfaces with CLS

Your SmartRelay is not only able to read identification media and switch a relay, but also serve solely as a reader for identification medium data. This data comprises:

- Customer ID or locking system ID
- Transponder ID

The identification medium data read is then forwarded to third-party systems via a serial interface in various data formats. Examples of such external systems:

- Attendance recording systems

- Canteen billing systems

This allows to control all relevant systems with just one identification medium, e.g.:

- Building automation systems
- Access control
- Time-and-attendance
- Canteen billing

The serial interface supports different signal and data format variants for the different manufacturers:

- Wiegand26 (standard format)
- Wiegand33 (for PRIMION connections)
- OMRON Primion
- OMRON Siemens-CerPass
- OMRON Gantner-Legic
- OMRON Dormakaba
- OMRON Isgus

10.7.1.1 Wiegand26 (standard format)

Signal description

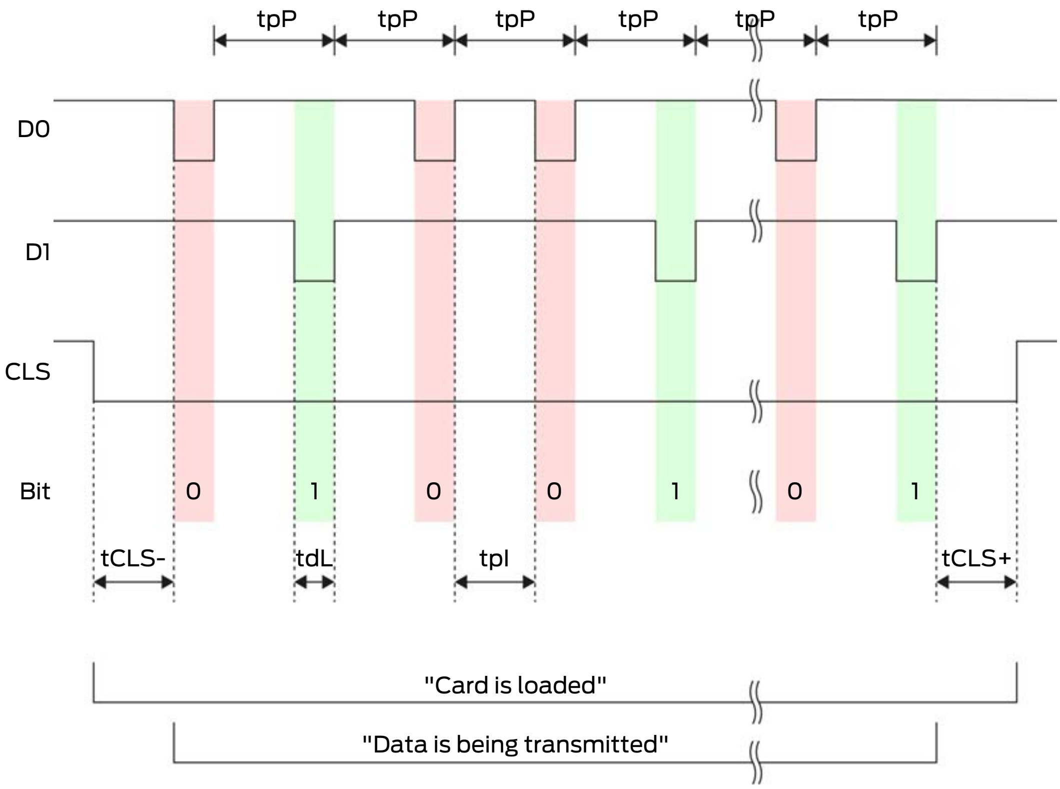
A Wiegand interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
D0	Data 0		F1 ("D0")	O1	Output 1
D1	Data 1		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	10	12	ms
t_{dL}	Data bit pulse width	80	100	120	µs
t_{pI}	Time between two bits (idle time)	800	900	1000	µs
t_{pP}	Signal period (data rate period)	900	1000	1100	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	10	12	ms

Data format (Wiegand 26-bit)

This is the standard Wiegand interface. The facility code is shortened to 8 bits.

Bit number	Meaning
Bit 1	Parity bit (even) spanning bits 2 to 13
Bits 2 to 9	Facility code (0 to 255). Bit 2 is MSB.
Bits 10 to 25	User ID number (0 to 65,535). Bit 10 is MSB.
Bit 26	Parity bit (odd) spanning bits 14 to 25.

10.7.1.2 Wiegand33 (for PRIMION connections)

Signal description

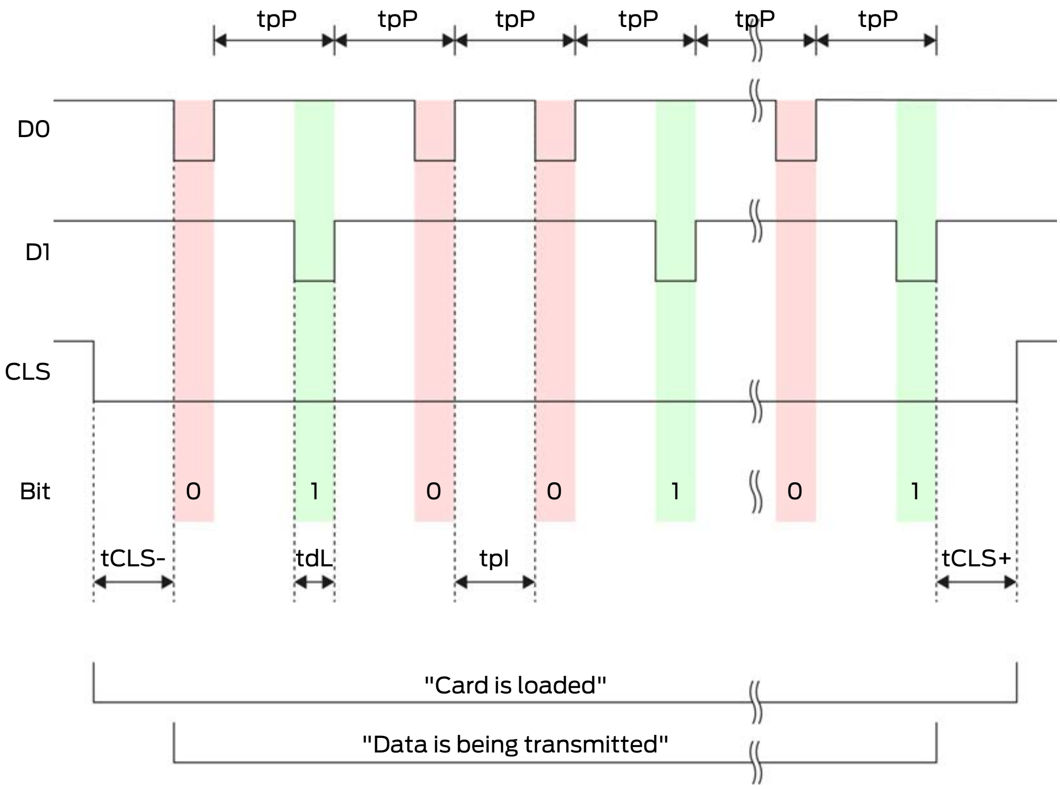
A Wiegand interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
D0	Data 0		F1 ("D0")	O1	Output 1
D1	Data 1		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”.

Signal timing



Time	Description	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	10	12	ms
t_{dL}	Data bit pulse width	80	100	120	µs
t_{pl}	Time between two bits (idle time)	800	900	1000	µs
t_{pP}	Signal period (data rate period)	900	1000	1100	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	10	12	ms

Data format (Wiegand 33-bit)

This is a modified Wiegand format. It contains the complete 16-bit facility code (or locking system ID).

Bit number	Meaning
Bits 1 to 16	Facility code (0 to 65,535). Bit 1 is MSB.
Bits 17 to 32	User ID number (0 to 65,535). Bit 17 is MSB.
Bit 33	Parity bit (odd) spanning bits 1 to 32.

10.7.1.3 OMRON Primion

Signal description

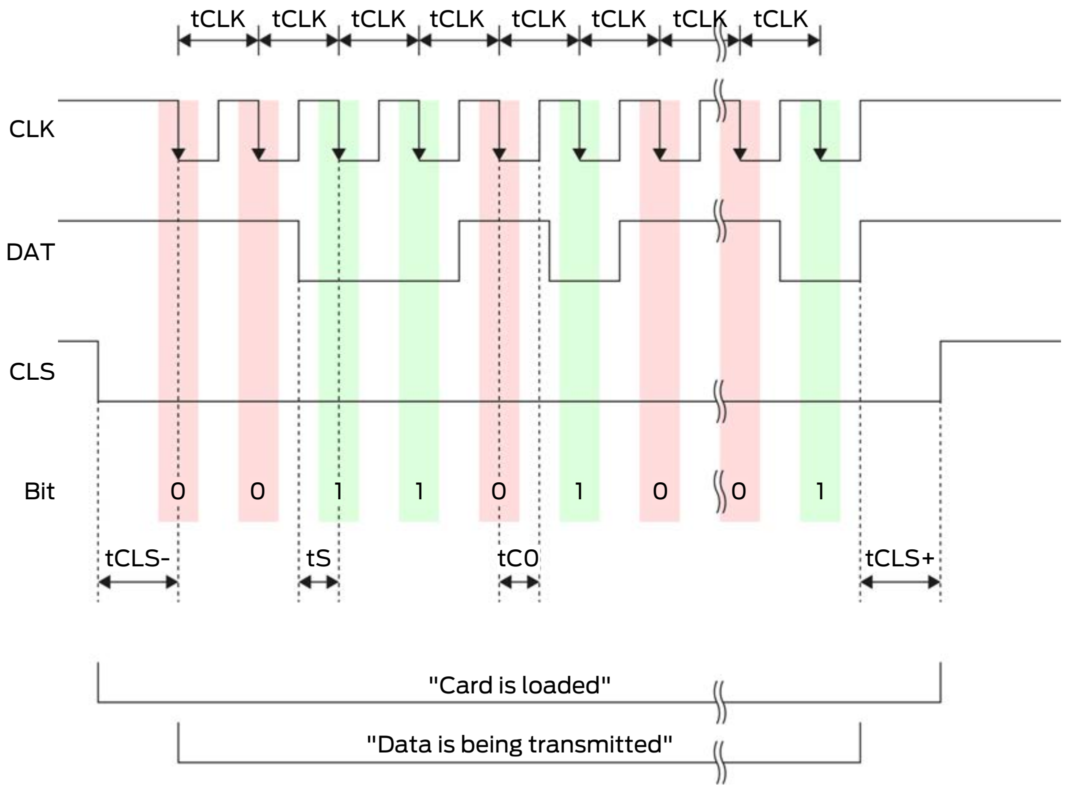
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Primion)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

S AAAAA BBBBB E

Meaning:

S	Start character (hex B)
A	Facility code (0 to 99,999)
B	User ID number (0 to 99,999)
E	End character (hex F)

Example:

- Facility code: 563
- User ID: 3,551

S	A	A	A	A	A	B	B	B	B	B	E
Start character	Facility code					User ID					End character
11010	00001	00001	10101	01101	11001	00001	11001	10101	10101	10000	11111
B	0	0	5	6	3	0	3	5	5	1	F

10.7.1.4 OMRON Siemens-CerPass

Signal description

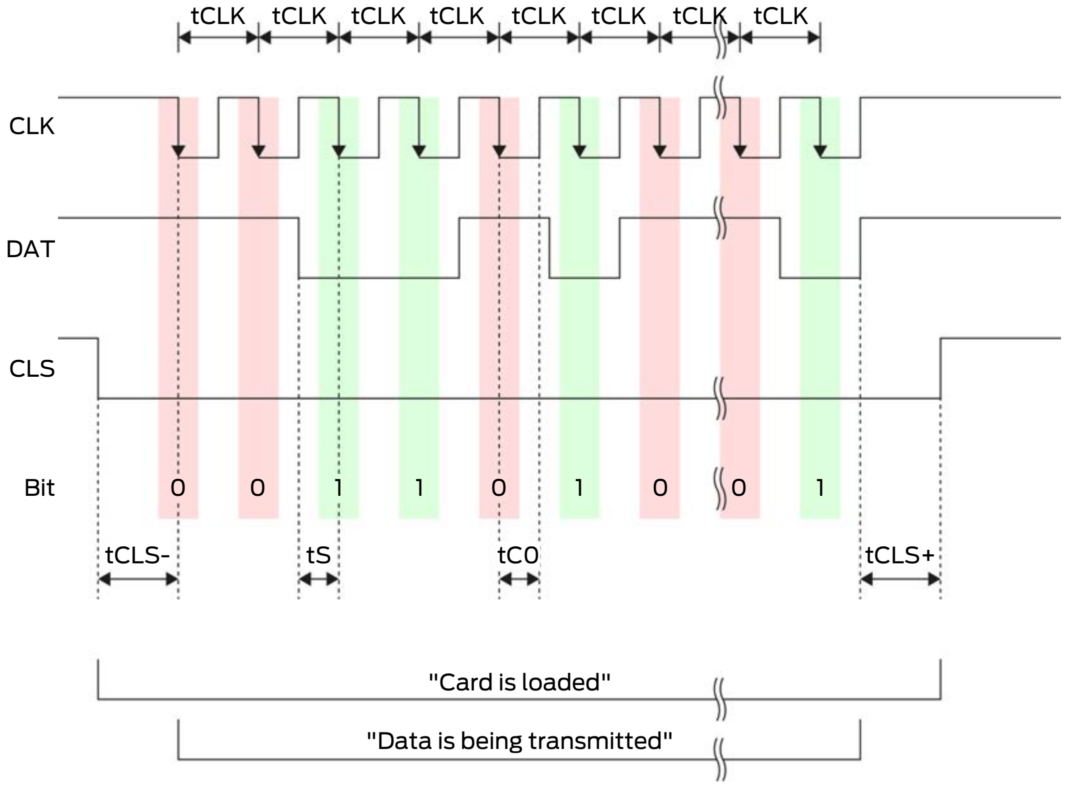
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Description	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{CO}	Clock set to “low” level (clock low)	50	100	150	µs
t_{CLS+}	Time between last data bit and de-activation of the CLS signal	8	12	20	ms

Data format (OMRON Siemens-CerPass)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

`<10 leading zero bits> S AAAAA BBBBB E L`

Meaning:

S	Start character (hex B)
A	Facility code (0 to 99,999)

B	User ID number (0 to 99,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

10.7.1.5 OMRON Gantner-Legic

Signal description

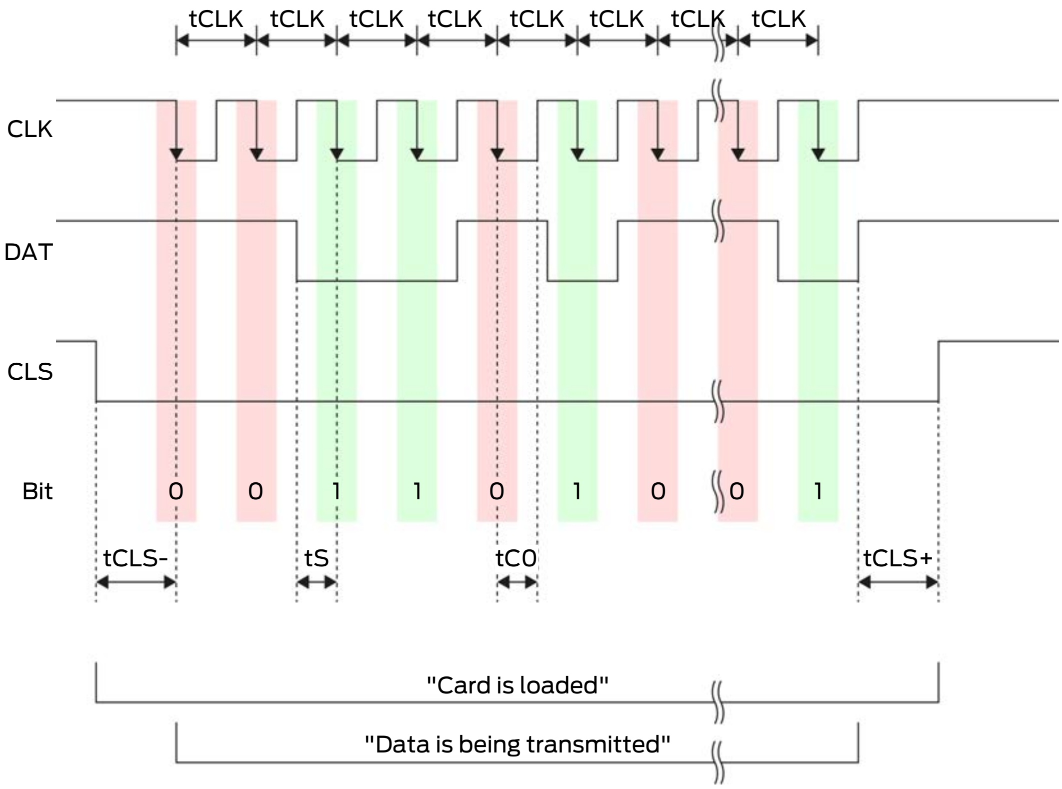
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 (“LED/ buzzer/input1”)	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are “Active low”. The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t $_{CLS+}$	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Gantner-Legic)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
<15 leading zero bits> S CCCCCCCC AAAA M N BBBBBB E L <15
trailing zero bits>
```

Meaning:

S	Start character (hex B)
C	Constant (hex 1A210001)
A	Facility code (0 to 9,999)
M	Separator (hex 0)
N	Separator (hex 1)
B	User ID number (0 to 999,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

10.7.1.6 OMRON Kaba Benzing

Signal description

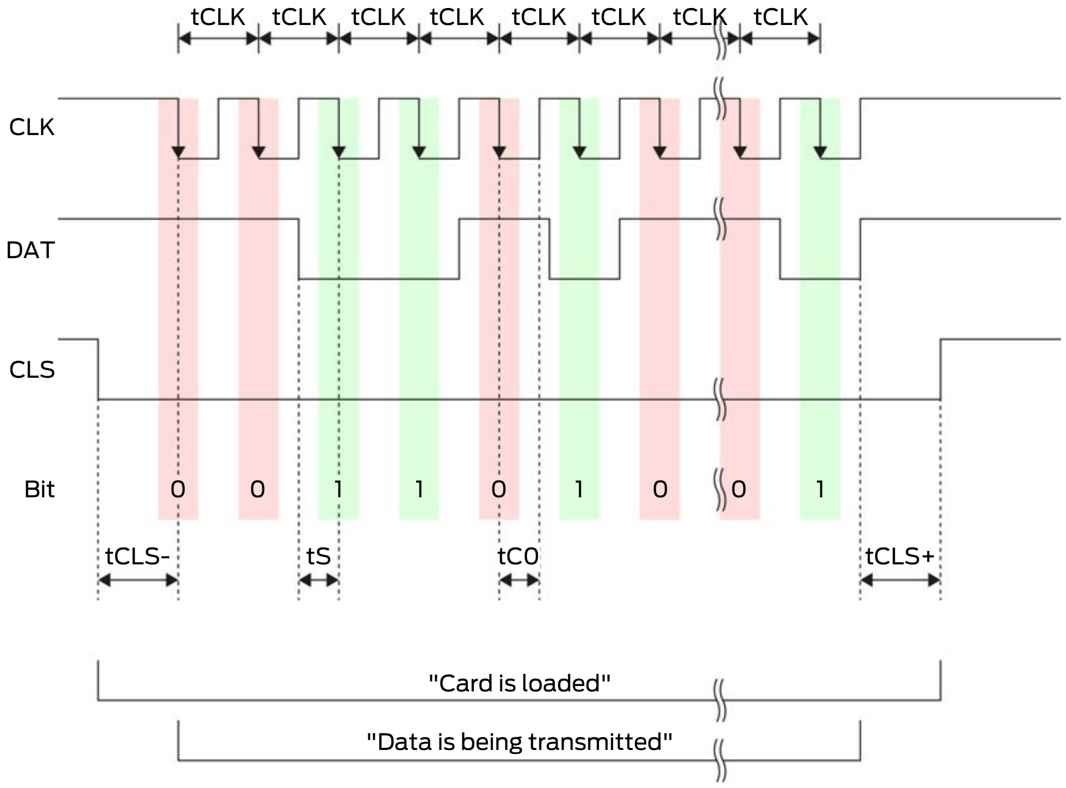
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 ("LED/ buzzer/input1")	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are "Active low". The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Description	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_S	Set-up time for data bit	50	100	150	µs
t_{CO}	Clock set to "low" level (clock low)	50	100	150	µs
t_{CLS+}	Time between last data bit and de-activation of the CLS signal	8	12	20	ms

Data format (OMRON Kaba Benzing)

Each message below consists of a sequence of letters ("characters").

Each "character" is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
<15 leading zero bits> S CCCCCCCC AAAAAAAA BBBBBB E L <15 lagging zero bits>
```

Meaning:

S	Start character (hex B)

C	Constant (hex 00000000)
A	Facility code (0 to 99,999,999)
B	User ID number (0 to 999,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transferred characters S...E)

10.7.1.7 OMRON Isgus

Signal description

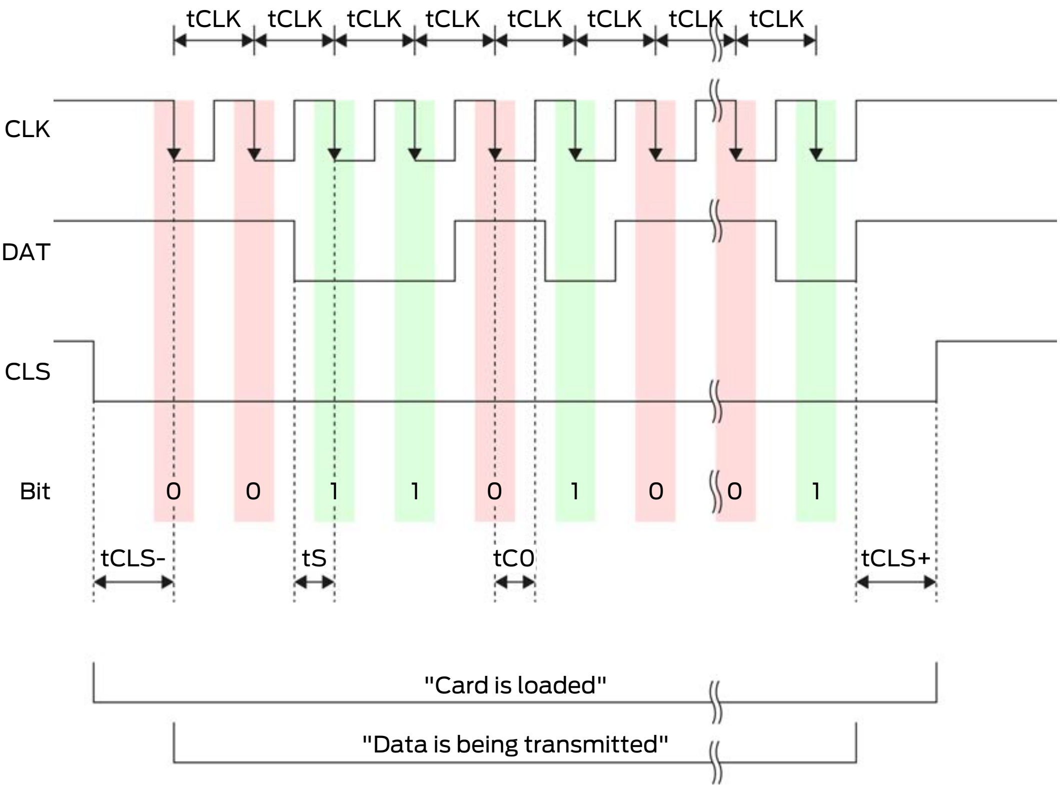
An OMRON interface uses the following standardised signals:

Signal	Meaning	Explanation	SREL.ADV connection	SREL3 ADV connection	SREL AX Classic connection
DATA	Data		F1 ("D0")	O1	Output 1
CLK	Clock		F2 ("D1")	O2	Output 2
CLS	Card loading signal	Optionally configurable	F3 ("LED/ buzzer/input1")	O3	Not available

All outputs are open-drain. A pull-up resistor (1kΩ to 10kΩ type) and the positive power supply (3 V_{DC} to 24 V_{DC}) must be provided for signal lines.

The signals are "Active low". The data becomes valid on the falling edge of the CLK signal.

Signal timing



Time	Descrip-tion	Min.	Typ.	Max.	Unit
t_{CLS-}	Time between activation of the CLS signal and first data bit	8	12	20	ms
t_{CLK}	Clock period	290	320	350	µs
t_{S}	Set-up time for data bit	50	100	150	µs
t_{C0}	Clock set to “low” level (clock low)	50	100	150	µs

Time	Description	Min.	Typ.	Max.	Unit
t_{CLS+}	Time between last data bit and deactivation of the CLS signal	8	12	20	ms

Data format (OMRON Isgus)

Each message below consists of a sequence of letters ("characters").

Each “character” is represented by a sequence of 5 bits (BCD code + parity):

Bit 1 (LSB)	Bit 2	Bit 3	Bit 4 (MSB)	Bit 5 (odd parity bit over bits 1 to 4)

Data structure of a message:

```
S BBBB M AAAA E L
```

Meaning:

S	Start character (hex B)
B	User ID number (0 to 9,999)
M	5th digit of the user ID number
A	Facility code (0 to 9,999)
E	End character (hex F)
L	Longitudinal parity check character (over all transmitted characters XOR[S...E])

10.8 Near-field option

A reduced reader range is required in some situations. The near-field option reduces the reader range for transponders. This reduces the influence of possible interferences and prevents the transponder from overriding.

- ✓ LSM 3.4 or higher installed.
- ✓ Components wired correctly (see *wiring [▸ 58]*).
- ✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enable the ☑ Close-up range mode checkbox.
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming (see *Programming [▸ 29]*).

↳ The near-field option is activated.

10.9 Switching interval

You can freely configure the duration of opening between 0 s and 25 s. The opening interval configured on the controller also applies to the SmartOutput modules.

IMPORTANT

Unintentional opening of the SmartOutput module

If a pulse length of 0 s has been configured in LSM, the SmartOutput module still activates for about three seconds.

NOTE

Long release by SmartOutput modules not supported

SmartOutput modules use the G1 protocol. The G1 protocol does not support the Long opening function. The SmartOutput modules used open for the time configured on the controller regardless of this setting on the transponder.

- ✓ Components wired correctly (see *wiring [▸ 58]*).
- ✓ Components connected to power.

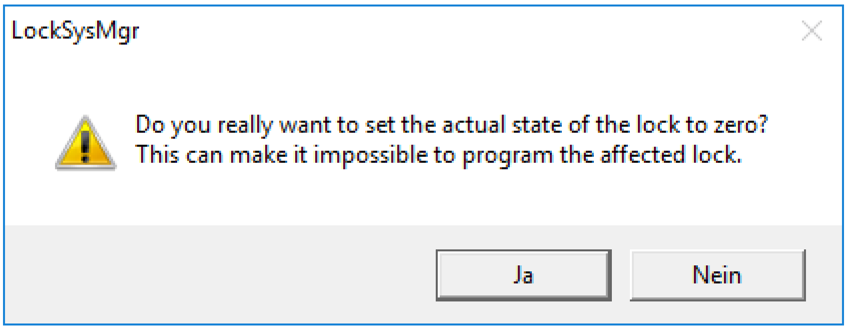
1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enter the desired pulse length.
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming (see *Programming [▸ 29]*).

↳ Switching interval is set.

10.10 Software reset

You can initiate a software reset in LSM. If the controller has been reset by a different LSM, LSM is no longer able to activate the reset controller. LSM still contains information on the controller which is no longer up to date. The software reset clears all the controller information saved in LSM in the software. This means that LSM and the controller are synchronised once more (both reset) and LSM can address the controller again.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Click on the Software reset button.
   ↳ The "LockSysMgr" window will open.



LockSysMgr

Do you really want to set the actual state of the lock to zero?
This can make it impossible to program the affected lock.

4. Click on the OK button.
5. Click on the Yes button.

↳ Software reset has been completed.

10.11 Time switch-over function

IMPORTANT

Unintentional opening due to use with SmartOutput module

The opening behaviour with a SmartOutput module in conjunction with time zone control deviates from the opening behaviour without the SmartOutput module.

All relays in the SmartOutput module are switched.

- See the sections on *Extended configuration with SmartOutput modules [▸ 140]* and *Extended configuration without SmartOutput module [▸ 139]*.

The fifth group in the time zone plan is relevant for time changeover.

Assignment of a time zone plan

✓ LSM launched.

✓ SREL3 ADV System added.

✓ Time zone plan added.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Door] tab.
3. Open the ▼ **Time zone** drop-down menu.
4. Select your time zone.
5. Click on the Apply button.
6. Click on the Exit button.

↳ Time zone is selected.

Activating time zone control and time changeover

Whereas time zone control itself can only influence identification media authorisations, the time changeover also activates time-dependent switching of the relay in the controller. Both need to be activated.

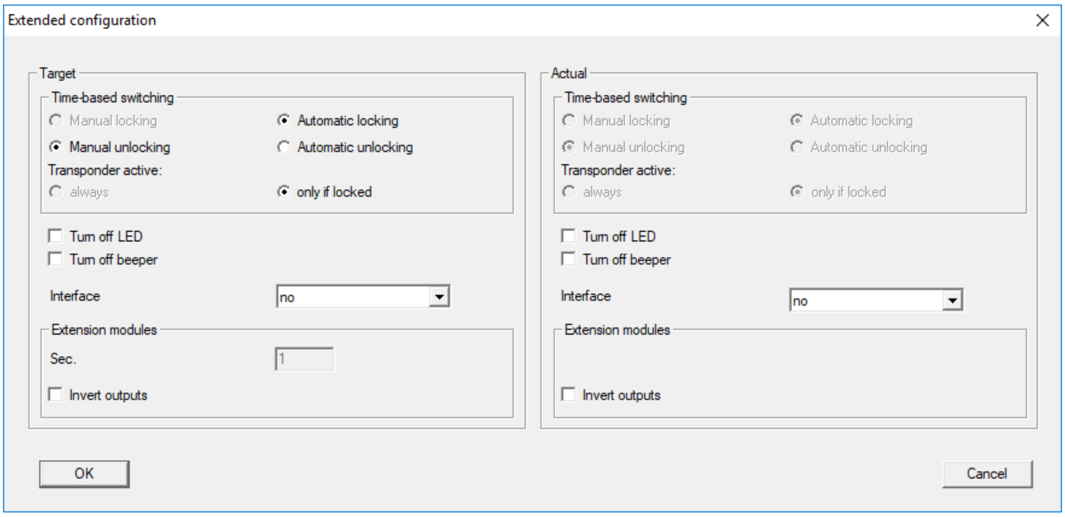
✓ LSM launched.

✓ SREL3 ADV System added.

✓ Time zone plan assigned.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [Configuration/Data] tab.
3. Enable the ☑ Time zone management checkbox.
4. Enable the ☑ Time switching checkbox.
5. Click on the Extended configuration button.

   ↳ The "Extended configuration" window will open.



Extended configuration

Target

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

Sec. 1

□ Invert outputs

Actual

Time-based switching

○ Manual locking ● Automatic locking

● Manual unlocking ○ Automatic unlocking

Transponder active:

○ always ● only if locked

□ Turn off LED

□ Turn off beeper

Interface: no

Extension modules

□ Invert outputs

6. Set the options for automatic and manual locking and unlocking in the "Time-based switching" section as you require (see *Extended configuration without SmartOutput module [▸ 139]* and *Extended configuration with SmartOutput modules [▸ 140]*).
7. Click on the OK button.
   ↳ Window closes.
8. Click on the Apply button.
9. Click on the Exit button.

↳ Time zone control and time changeover are activated.

Activation within the authorised/non-authorised time period

Time changeover is always activated for the next full quarter of an hour. If programming takes place within a defined time period, the changeover is not implemented until the next full quarter of an hour within the defined time period. If the existing time zone plan allows the SREL3 ADV system to now be closed and the newly programmed time zone plan allows the SREL3 ADV system to now be open, opening does not come into effect until the next full quarter of an hour.

1. Disconnect the power supply temporarily to activate the time changeover immediately.
2. Ensure that there are no unauthorised accesses until the next full quarter of an hour.

Editing the time zone plan

See LSM manual to edit the time zone plan.

10.11.1 Extended configuration without SmartOutput module

Unlocking in the authorised time period (close relay contacts)			
Unlocking automatically		Unlocking manually	
always	only if locked	always	only if locked
Controller: Closes relay contacts (unlocked) as soon as authorisation starts in the time zone plan. Behaves in the same way as a flip-flop for the remaining authorised time period.	Controller: Closes relay contacts (unlocked) as soon as authorisation starts in the time zone plan. No influence by identification media for the rest of the authorised time period.	Controller: Closes relay contacts (unlocked) as soon as identification medium is activated after authorisation starts in the time zone plan. Behaves in the same way as a flip-flop for the remaining authorised time period.	Controller: Closes relay contacts (unlocked) as soon as identification medium is activated after authorisation starts in the time zone plan. No influence by identification media for the rest of the authorised time period.

Locking in the non-authorised time period (open relay contacts)	
Locking automatically	Locking manually

Locking in the non-authorised time period (open relay contacts)			
always	only if locked	always	only if locked
Controller: Opens relay contacts (locked) as soon as authorisation ends in the time zone plan. Identification media close relay contacts (unlock) during non-authorised time period for pre-set pulse duration.	Controller: Opens relay contacts (locked) as soon as authorisation ends in the time zone plan. Identification media close relay contacts (unlock) during non-authorised time period for pre-set pulse duration.	Controller: Opens relay contacts (locked) as soon as identification medium is activated. Identification media close relay contacts (unlock) during non-authorised time period for pre-set pulse duration.	Not possible

10.11.2 Extended configuration with SmartOutput modules

Unlocking in the authorised period (close relay contacts)			
Automatic unlocking		Manual unlocking	
always	only if locked	always	only if locked
Not possible	- Controller: Closes relay contacts (unlocked) as soon as authorisation begins in the time zone plan. Not affected by identification media during the authorised period. - SmartOutput module: Closes relay contacts (unlocked) as soon as authorisation begins in the time zone plan. Not affected by identification media during the authorised period.	Not possible	- Controller: Closes relay contacts (unlocked) as soon as identification medium is actuated after the start of the authorisation in the period. Thereafter, no influence by identification media in the remaining authorised period. - SmartOutput module: Closes relay contacts (unlocked) as soon as authorisation begins in the time zone plan and identification medium is reserved. No affected by identification media during the remaining authorised period.

<table>
<tr><th colspan="3">Locks in unauthorised period (relay contacts open)</th></tr>
<tr><td colspan="2">Automatic locking</td><td>Manual locking</td></tr>
<tr><td>always</td><td>only if locked</td><td rowspan="2">Not possible</td></tr>
<tr><td>Not possible</td><td>- Controller: Opens relay contacts (locked) as soon as authorisation ends in the time zone plan. Identification media closes relay contacts for set pulse duration during the remaining unauthorised period.
- SmartOutput module: Opens relay contacts (locked) as soon as authorisation ends in the time zone plan. Identification media closes relay contacts for set pulse duration during the remaining unauthorised period.</td></tr>
</table>

10.12 Remote opening

You can also use LSM to operate the relay in the controller without identification media at any time.

NOTE

A remote opening takes precedence over time zone control. It also operates the relay if the relay contacts should remain open after time zone control.

Remote opening with USB cable

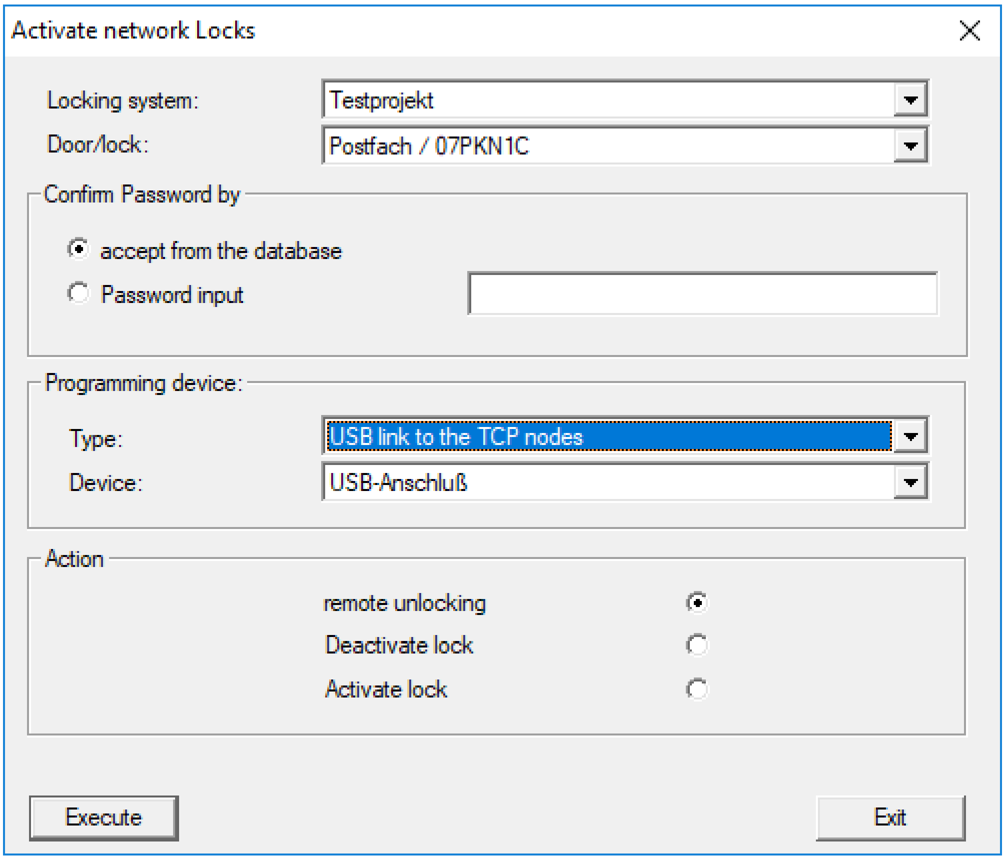
✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Use | Network | to select the Lock activation item.

   ↳ The "Activate network locks" window will open.



Activate network Locks

Locking system: Testprojekt

Door/lock: Postfach / 07PKN1C

Confirm Password by

● accept from the database

○ Password input

Programming device:

Type: USB link to the TCP nodes

Device: USB-Anschluß

Action

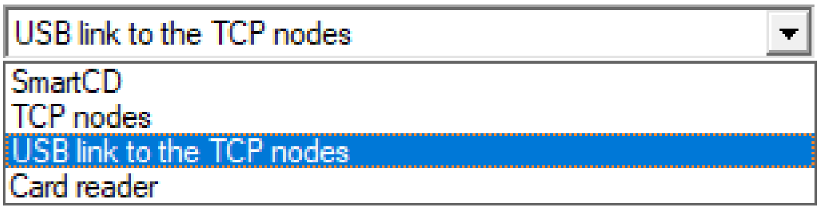
remote unlocking ●

Deactivate lock ○

Activate lock ○

2. Open the ▼ **Door/lock** drop-down menu.
3. Select the SREL3 ADV system controller.
4. Open the ▼ **Type** drop-down menu.

5. Select the "USB link to the TCP nodes" item.



6. Open the ▼ **Device** drop-down menu.
7. Select the IP address if required.
8. Select the ● remote unlocking option.
9. Click on the Execute button.

↳ Relay switches in the controller.

↳ "Programming successful" window is displayed.

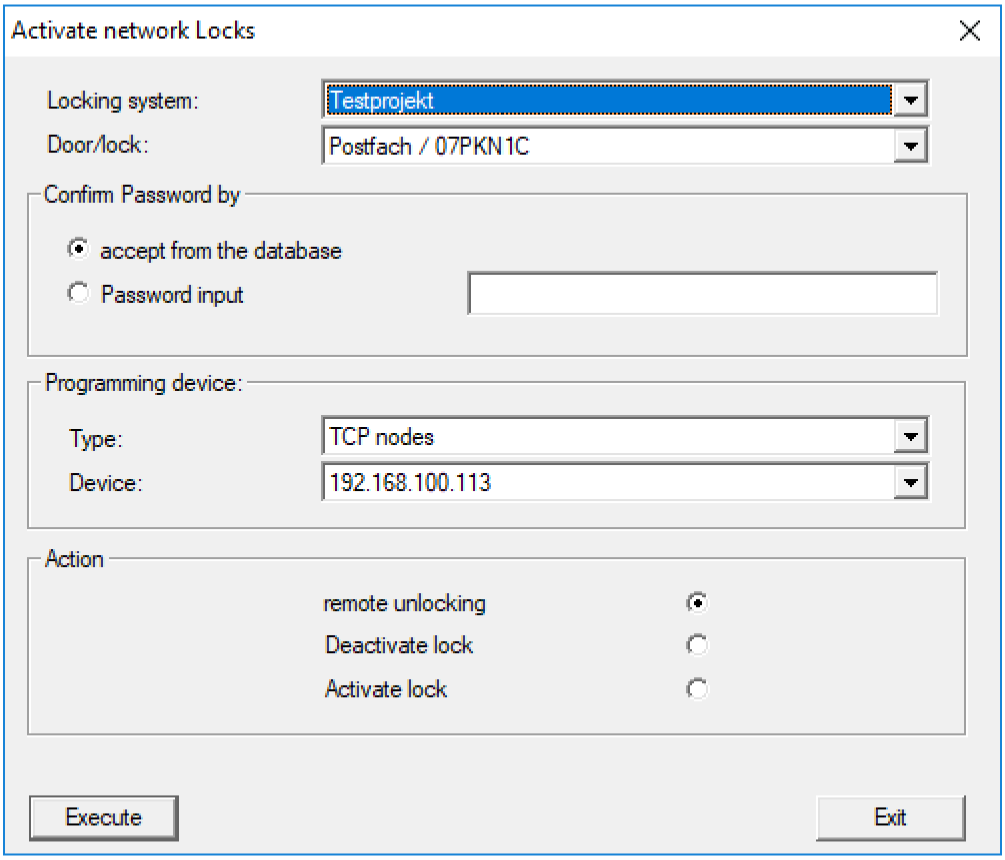
Remote opening via TCP/IP

✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Use | Network | to select the Lock activation item.
   ↳ The "Activate network locks" window will open.



Activate network Locks

Locking system: Testprojekt

Door/lock: Postfach / 07PKN1C

Confirm Password by

● accept from the database

○ Password input

Programming device:

Type: TCP nodes

Device: 192.168.100.113

Action

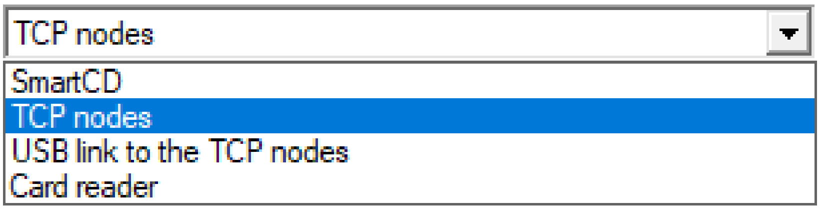
remote unlocking ●

Deactivate lock ○

Activate lock ○

2. Open the ▼ **Door/lock** drop-down menu.

3. Select the SREL3 ADV system controller.
4. Open the ▼ **Type** drop-down menu.
5. Select the "TCP nodes" item.



TCP nodes

SmartCD

TCP nodes

USB link to the TCP nodes

Card reader

6. Open the ▼ **Device** drop-down menu.
7. Select the IP address if required.
8. Select the ◉ remote unlocking option.
9. Click on the Execute button.

↳ Relay switches in the controller.

↳ "Programming successful" window is displayed.

10.13 Firmware update

SimonsVoss products are kept up to date and maintained at all times. It may be necessary to enable new functions to install a new firmware version.

Firmware updates are a complex affair which require detailed specialist knowledge. Contact our Support to install any firmware updates (see Help and contact). The controller may need to reset the controller.

IMPORTANT

Bricking due to firmware update being interrupted

The firmware is also responsible for resetting. If the firmware is partly overwritten and the process is interrupted (connection is cut or the power supply fails), it may no longer be possible to address or reset the device as a result of what is known as bricking.

1. Ensure that the power supply is stable during the firmware update.
2. Ensure that the power supply is not interrupted during the firmware update.
3. Ensure that the connection is not interrupted during the firmware update.

10.14 Events

10.14.1 Evaluating controller inputs

The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

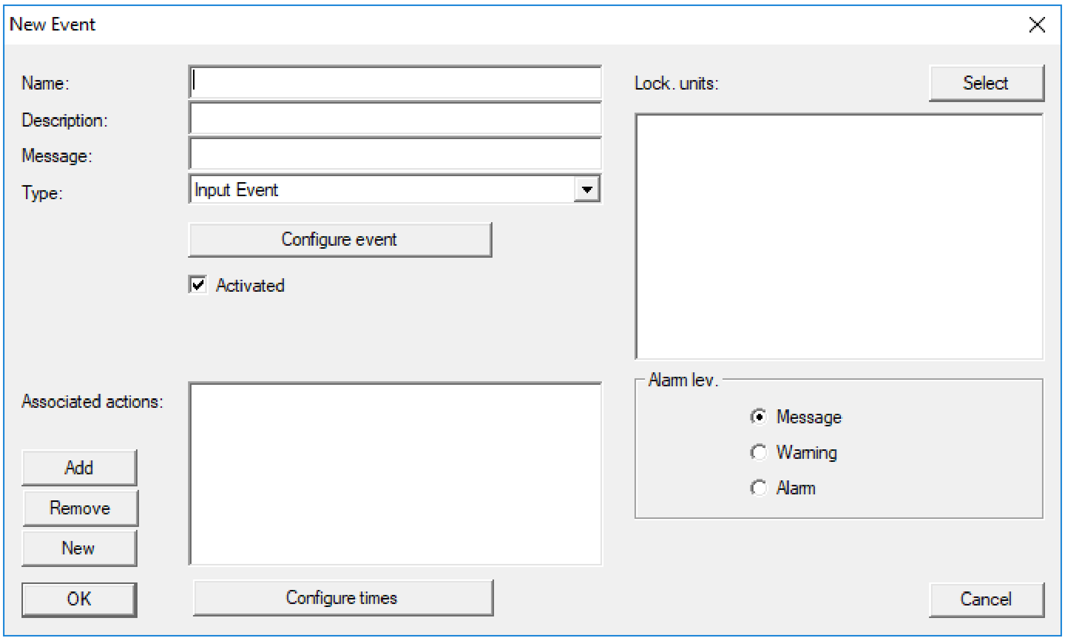
Adding an event

If you wish to use LSM or SmartSurveil (see *SmartSurveil [▸ 147]*) to evaluate an input, you first need to create the corresponding input as an event in LSM. Only then will changes to the input also be saved in the LSM database.

✓ LSM open.

✓ SREL3 ADV System added to the matrix.

1. Use | Network | to select the Event manager item.
   ↳ The "Network event manager" window will open.
2. Click on the New button.
   ↳ The "New Event" window will open.



New Event

Name:

Description:

Message:

Type: Input Event

Configure event

☑ Activated

Associated actions:

Add
Remove
New
OK

Configure times

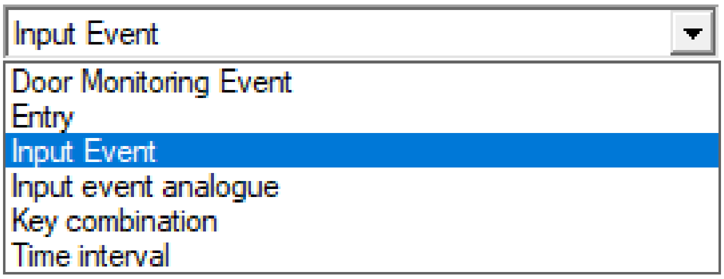
Lock. units: Select

Alarm lev.
● Message
○ Warning
○ Alarm

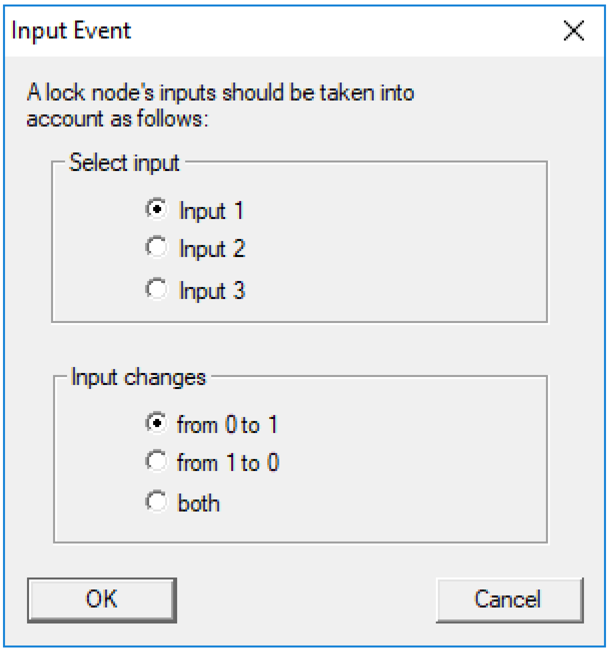
Cancel

3. Enter a suitable name for the event.
4. Enter an optional description for the event.
5. Enter an optional message.
6. Open the ▼ **Type** drop-down menu.

7. Select the "Input Event" item.



8. Click on the Configure event button.
   - ↳ The "Input Event" window will open.


Input Event

A lock node's inputs should be taken into account as follows:

Select input

● Input 1
○ Input 2
○ Input 3

Input changes

● from 0 to 1
○ from 1 to 0
○ both

9. Select the required input in the "Select input" section.
10. Select the status change that the event should trigger in the "Input changes" section.
11. Click on the OK button.
12. Click on the Select button to assign a locking device to the event.
    - ↳ The "Administration" window will open.
13. Highlight one or more locking devices.
14. Click on the □ Add button.
15. Click on the OK button.
    - ↳ Window closes.
    - ↳ Locking device is assigned to the event.
16. You can use the New or Add button to assign an action if you wish to configure an action.
17. Click on the OK button.
    - ↳ Window closes.

↳ Event is displayed in the "Events" section.

18. Click on the Exit button.

↳ Window closes.

↳ Input is added as an event and triggers an action.

10.14.2 SmartSurveil

SmartSurveil is a stand-alone software tool used to simplify the monitoring of door statuses. Events detected by network-capable devices are stored in the LSM database by these devices via the CommNode server. SmartSurveil continuously monitors the LSM database to detect changes and displays the current status of networked and monitored locks.

The controller of the SREL3 ADV system is a networked device and can also be monitored by SmartSurveil. There is one special feature: The controller is not a locking device and therefore cannot automatically detect the locking device status. Instead, the inputs at the digital inputs are evaluated and can be displayed in SmartSurveil as "open", "locked" or "closed". However, SmartSurveil must be set up for this:

✓ Events for inputs to be monitored have been set up in the LSM (see *Evaluating controller inputs [▸ 145]*).

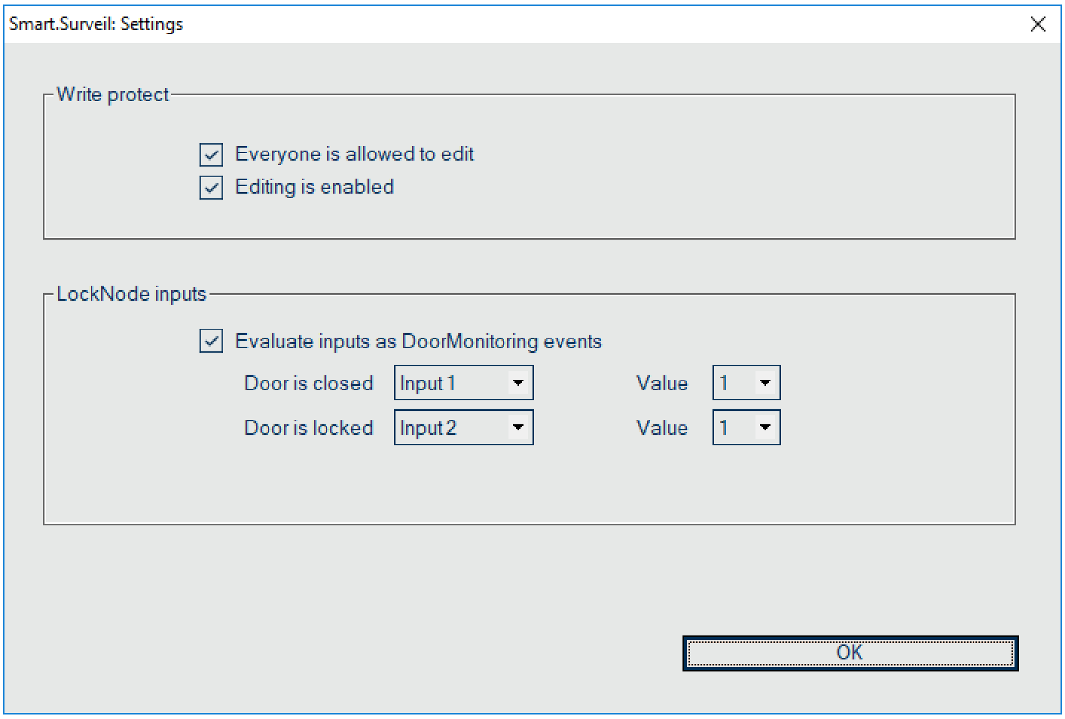
✓ SmartSurveil linked to database.

✓ User logged on to SmartSurveil.

✓ Controller of the SREL3 ADV system is shown.

1. Switch to the [Doors] tab.
2. Click on the button Settings.

↳ Window "SmartSurveil: Settings" opens.



Smart.Surveil: Settings

Write protect

☑ Everyone is allowed to edit

☑ Editing is enabled

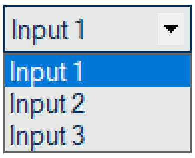
LockNode inputs

☑ Evaluate inputs as DoorMonitoring events

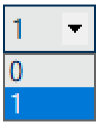
Door is closed: Input 1 — Value: 1

Door is locked: Input 2 — Value: 1

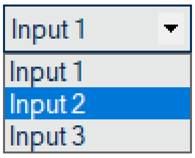
3. Activate the option ☑ Evaluate inputs as DoorMonitoring events.
4. Open the drop-down menu ▼ **Door is closed**.
5. Select the input that monitors whether a door is closed.



6. Open the ▼ **Value** drop-down menu.
7. Select the state of the input to be detected as closed by SmartSurveil.

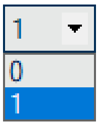


8. Open the drop-down menu ▼ **Door is locked**.
9. Select the input that monitors whether a door is locked.



10. Open the ▼ **Value** drop-down menu.

11. Select the state of the input to be detected as "locked" by SmartSurveil.



12. Click on the OK button.
    - ↳ Window closes.

↳ SmartSurveil is configured to monitor the SREL3 ADV system.

NOTE

SmartSurveil will only detect a door as locked if it has previously been detected as closed.

NOTE

These settings apply to all SREL3 ADV systems in the linked LSM database.Select the input that monitors whether a door is closed.

For details on SmartSurveil, please refer to the SmartSurveil manual.

10.15 Things to do

10.15.1 Initial programming via TCP/IP

In some use cases, the controller needs to be installed first and then programme the address (pre-installed reader). It may no longer be possible to reach the controller with a USB cable after installation. Whatever happens, an IP address assigned to the controller and known to LSM requires initial programming via TCP/IP.

This problem can be avoided if the controller is first programmed via a USB cable separately from other components. During programming, a valid IP address is issued and saved to the controller. The controller is then reset but the IP address is retained.

Initial programming with USB cable and address assignment

Carry out initial programming as described in *Configuration [▸ 24]*.

NOTE

In this case, external components do not need to be connected.

Resetting the controller

Reset the controller as described in *Resetting controller with a USB cable [▸ 33]*.

Installing the controller

Install the controller in its final place of use. Connect the controller to the other components and the power supply (see *wiring [▸ 58]*).

Programming via TCP/IP

Execute programming via the previously assigned TCP/IP address (see *Programming [▸ 29]*).

The SREL3 ADV system is now ready for use.

10.15.2 Different authorisations on transponders

A transponder with an integrated MIFARE chip is regarded as two different identification media for both LSM and the SREL3 ADV system from a logic viewpoint. You can make use of this characteristic and activate different outputs on the controller and the SmartOutput modules using the same transponder by assigning different authorisations to the MIFARE chip than to the transponder.

✓ Controller has already been programmed.

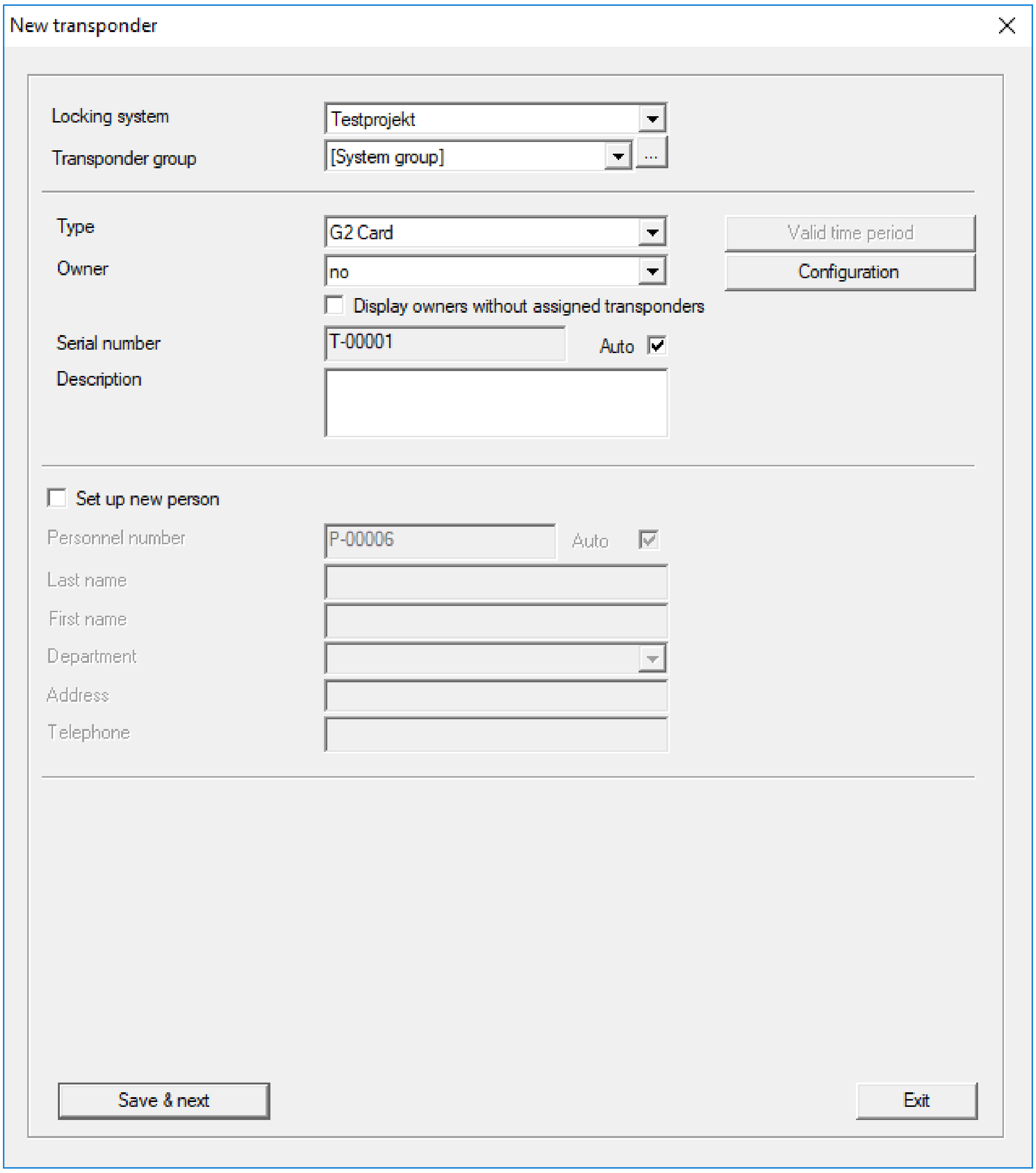
✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

✓ Matrix open for the corresponding locking system.

1. Click on the New transponder button.

↳ The "New transponder" window will open.



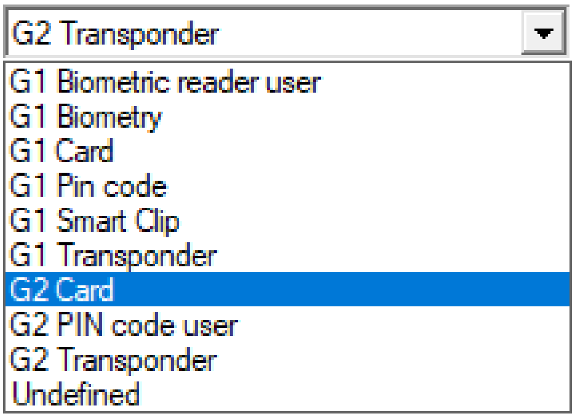
New transponder

Locking system	Testprojekt
Transponder group	[System group]
Type	G2 Card
Owner	no
	□ Display owners without assigned transponders
Serial number	T-00001 Auto ☑
Description	

□ Set up new person

Personnel number	P-00006 Auto ☑
Last name	
First name	
Department	
Address	
Telephone	

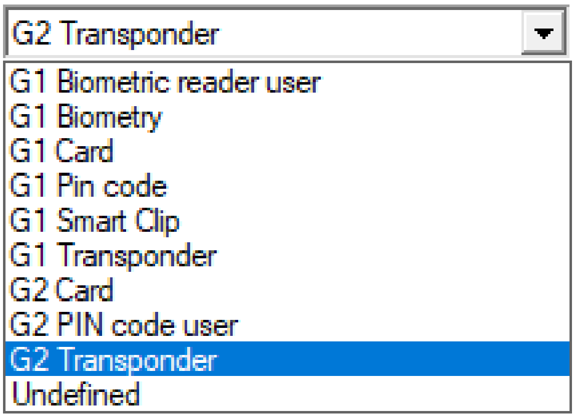
2. Open the ▼ **Type** drop-down menu.
3. Select the "G2 Card" item.



G2 Transponder

4. Complete the form.
5. Click on the Save & next button.

6. Open the ▼ **Type** drop-down menu.
7. Select the "G2 Transponder" item.



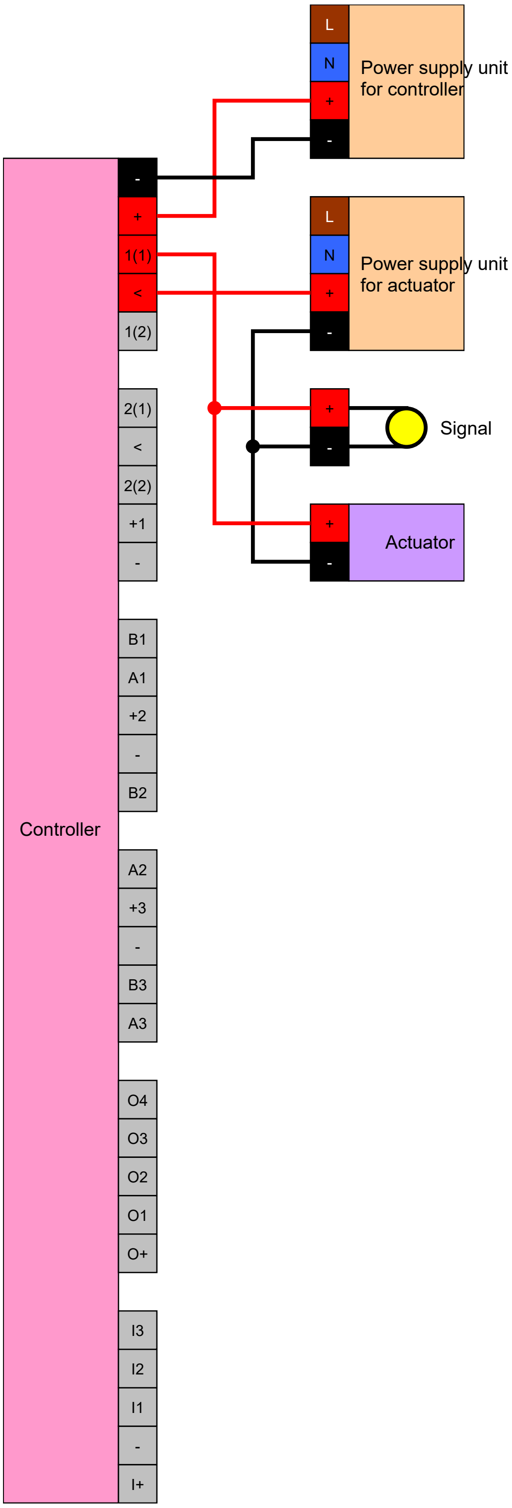
8. Complete the form.
9. Click on the Save & next button.
10. Click on the Exit button.
    ↳ Window closes.
11. Assign the required authorisations.
12. Click on the Apply button.
13. Programme the MIFARE chip (see LSM manual).
14. Programme the transponder (see LSM manual).

↳ When the MIFARE chip is used to log on to the reader, only those relays which the MIFARE chip is authorised to use are actuated.

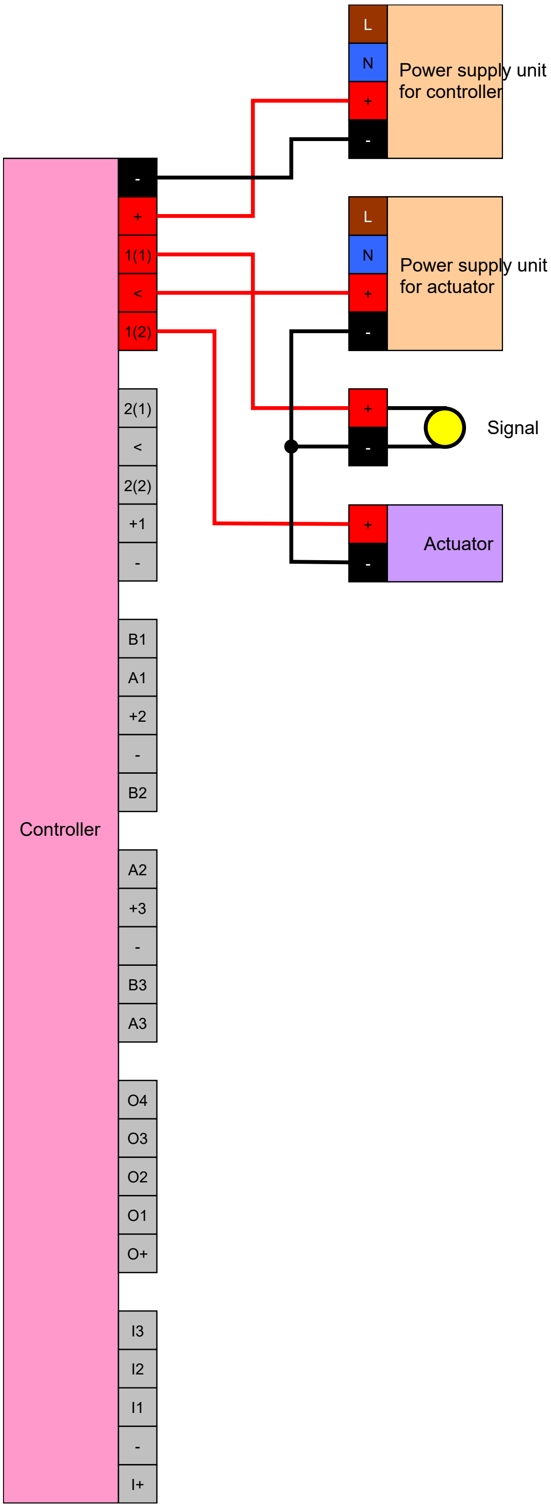
↳ When the transponder is used to log on to the reader, only those relays which the transponder is authorised to use are actuated.

10.15.3 Signalling for flip-flop

Signalling from the reader in the SREL3 ADV system does not indicate whether the door is open or closed in flip-flop mode. Even so, users can see whether the door is open or closed. To do so, the relay output is also used to help activate the power supply for signalling. If an electric strike opens when electric current is applied, for example, the power supply is activated by the relay. The same (activated) power supply can be also used for any signalling system, such an LED or light bulb.



It is even possible to signal an actuator (electric strike) closing when an electric current is applied. In doing so, use is made of the fact that the relay in the controller features both an NC and an NO contact. The positive terminal on the power supply for the electric strike is connected to the common contact; the positive terminal for the actuator is connected to the NC contact. The signalling positive terminal is connected to the NO contact. If the relay switches, the actuator on the NC contact is now longer supplied with power and the door opens. The NO contact closes at the same time and supplies power to the signalling.



11. Signal

You can configure signalling (see *Signal settings [▸ 116]*). You can make use of the relay if you wish to display the opening status in flip-flop mode (see *Signalling for flip-flop [▸ 152]*).

The following table describes the firmware signalling > 1.1.296.

Configuration: Gateway and relay

	Relay authorised	Relay not authorised
Gateway active	💡 🟨🟩 🟩 open 🟩	💡 🟨🟩
	🔊 ⬛ ⬛ open ⬛	🔊 ⬛
Gateway active, transmission error	💡 🟨🟥	💡 🟨🟥
	🔊 ⬛	🔊 ⬛
Gateway inactive	💡 🟩 🟩 open 🟩	💡 🟥
	🔊 ⬛ ⬛ open ⬛	🔊 ⬛

12. Maintenance

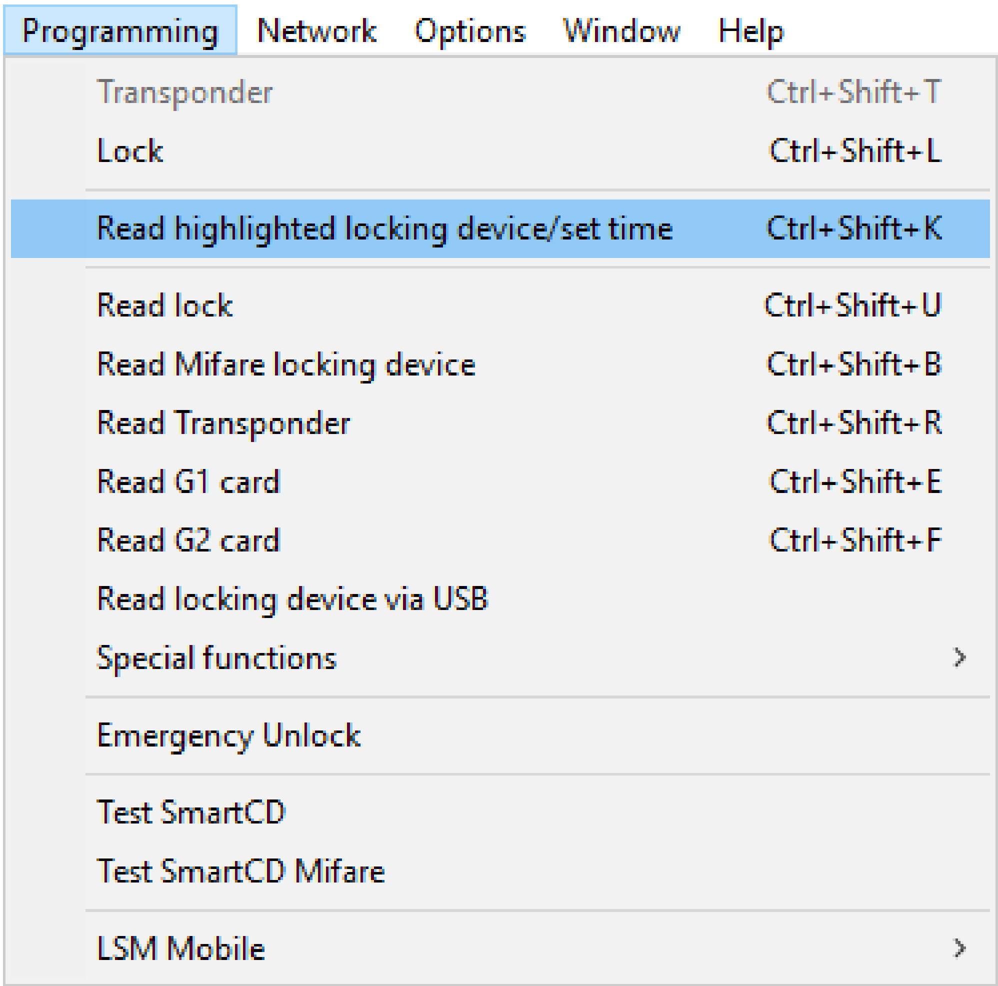
12.1 Battery warning

The built-in back-up battery in the controller continues to power the real time clock in the event that power supply fails. If the back-up battery is empty, the real time clock stops still if the power supply should fail. This can cause malfunctions and problems. Consequently, the battery should be checked on a regular basis. You can read the battery level via a USB connection or the network.

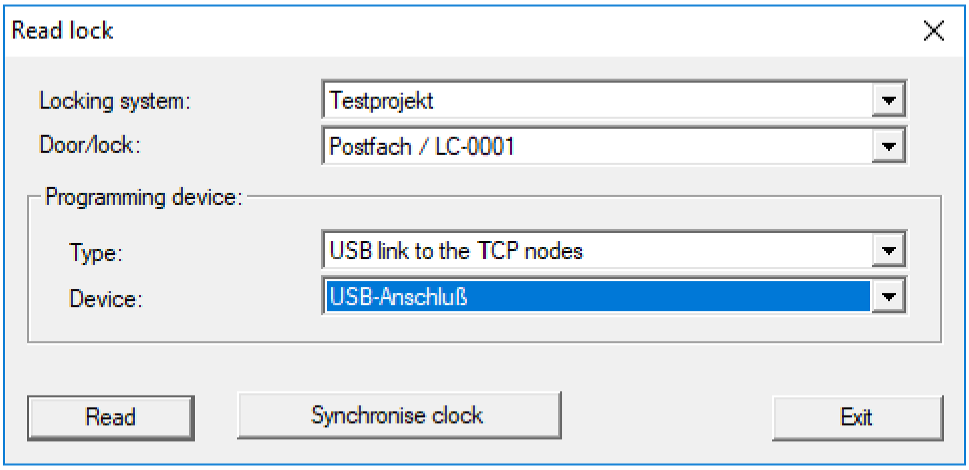
12.1.1 Reading the battery level with USB cable

- ✓ Components connected to power.
- ✓ Controller connected to computer with USB cable.
- ✓ Battery to be checked inserted.

1. Mark the entry on the SmartRelay 3 controller in the matrix.
2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile

↳ The "Read lock" window will open.



Read lock

Locking system: Testprojekt

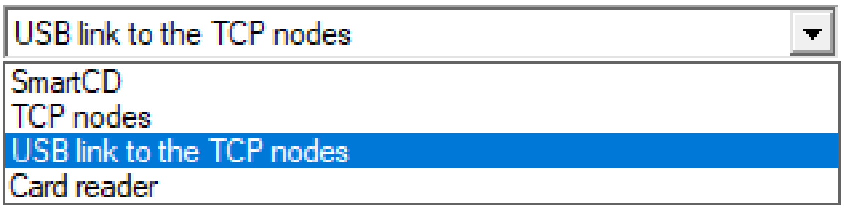
Door/lock: Postfach / LC-0001

Programming device:

Type: USB link to the TCP nodes

Device: USB-Anschluß

3. Open the ▼ **Type** drop-down menu.
4. Select the "USB link to the TCP nodes" item.



5. Click on the Read button.
   - ↳ Locking device is read.

↳ Battery level is displayed in the "State" section.

↳ Battery level is displayed in the "State during last read-out" section in the [State] tab in properties.

12.1.2 Reading the battery level over network

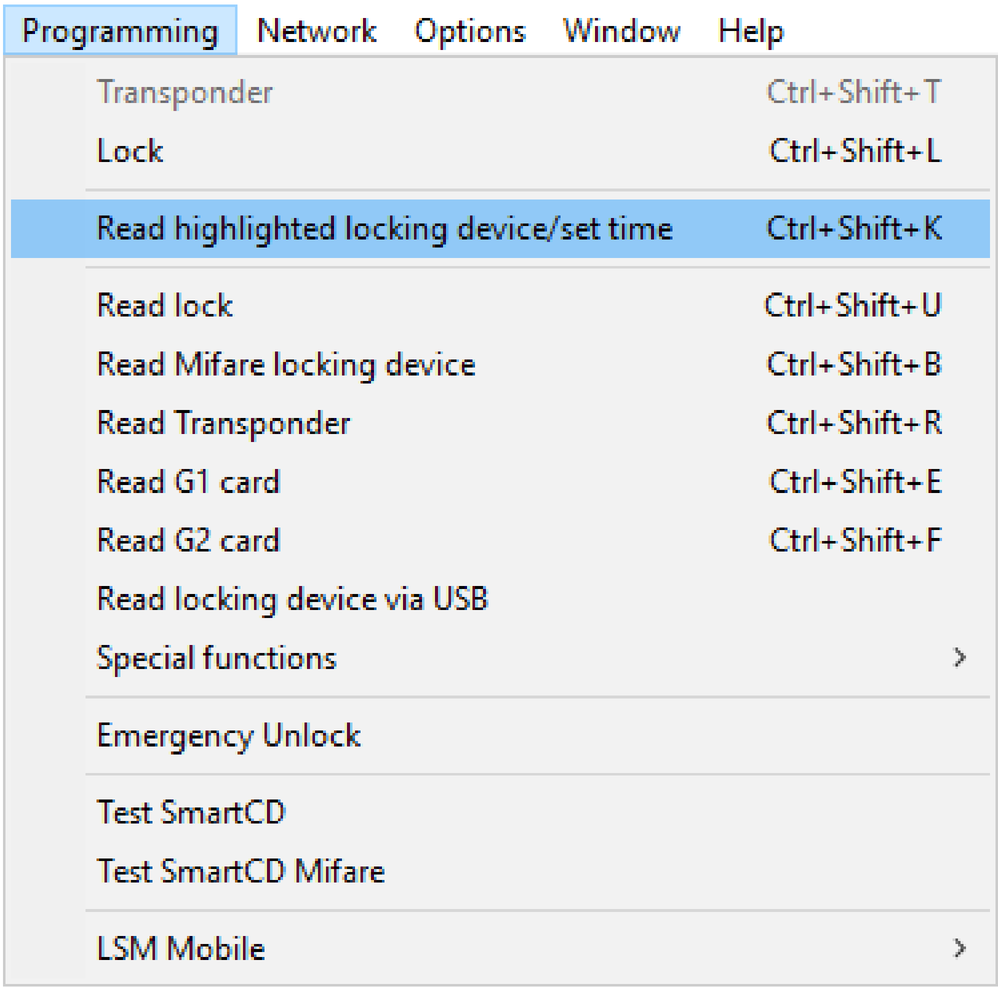
✓ Components connected to power.

✓ Controller connected to computer via network.

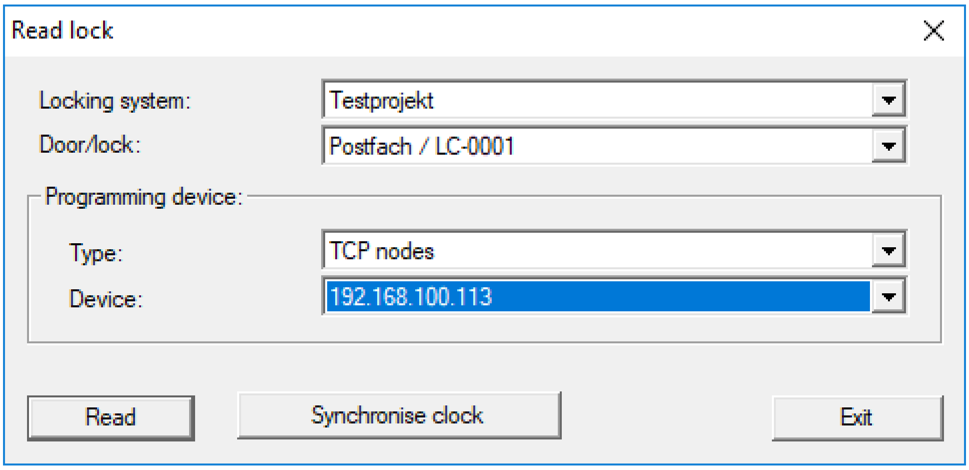
✓ Battery to be checked inserted.

1. Mark the entry on the SmartRelay 3 controller in the matrix.

2. Use | Programming | to select the Read highlighted locking device/set time item.


Programming
Network
Options
Window
Help
Transponder Ctrl+Shift+T
Lock Ctrl+Shift+L
Read highlighted locking device/set time Ctrl+Shift+K
Read lock Ctrl+Shift+U
Read Mifare locking device Ctrl+Shift+B
Read Transponder Ctrl+Shift+R
Read G1 card Ctrl+Shift+E
Read G2 card Ctrl+Shift+F
Read locking device via USB
Special functions
Emergency Unlock
Test SmartCD
Test SmartCD Mifare
LSM Mobile

↳ The "Read lock" window will open.


Read lock

Locking system: Testprojekt

Door/lock: Postfach / LC-0001

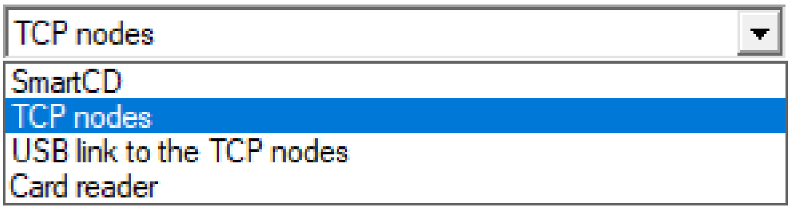
Programming device:

Type: TCP nodes

Device: 192.168.100.113

3. Open the ▼ **Type** drop-down menu.

4. Select the "TCP nodes" item.



TCP nodes

SmartCD
TCP nodes
USB link to the TCP nodes
Card reader

5. Click on the Read button.
   ↳ Locking device is read.

↳ Battery level is displayed in the "State" section.

↳ Battery level is displayed in the "State during last read-out" section in the [State] tab in properties.

12.2 Battery replacement

NOTE

Shorter battery life due to poor contact

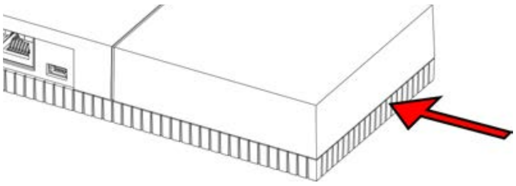
Skin oil impairs contact between the battery and the battery holder.

1. Do not touch the contacts on new batteries with your hands when replacing old ones.
2. Use clean cotton gloves free of fat or grease.

Dispose of the batteries as per local and country-specific regulations.

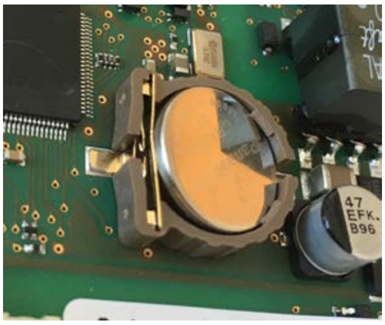
✓ Controller disconnected from power supply.

1. Press in the controller housing at the indicated point and lift the lid.

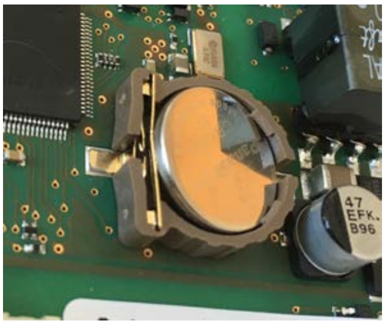


   ↳ Housing is open.

2. Use a screwdriver to press the battery locking mechanism to one side until it releases.



   ↳ Battery is now loose in its holder.
3. Remove the battery.
4. Insert a suitable new battery on the holder (see *Controller [▸ 166]*).



5. Carefully push the battery downwards until it snaps into position.
   ↳ Battery is inserted.
6. Put the housing lid on again.
7. Carefully push the housing lid downwards until it snaps into position.

↳ Battery has now been replaced.

New batteries may not function correctly (due to age, faulty batch or similar). You can view the battery level in LSM after you change the battery (see *Battery warning [▸ 156]*).

IMPORTANT

Interruption in the power supply to the RTC

If the battery and the normal power supply are disconnected, the internal real time clock (RTC) is no longer powered. The clock time will no longer be correct when the power supply is restored and the authorisations added to the time zone plans will not be active at the specified times.

- Implement programming for the controller (see *Programming [▸ 29]*).

13. Fault rectification

13.1 Resetting components

You can reset the controller (see *Resetting the controller [▸ 33]*).

NOTE

Only the hardware settings and access lists on the controller are reset. The IP setting remains unchanged

You can reset the software in LSM (see *Software reset [▸ 137]*).

13.2 Broadcast error

Unavailable service

A frequent cause of transmission errors in programming is an unavailable or ended service. Check whether the service is running.

- If you use a virtual network, the VN host server must be operation.
- If you use the SmartRelay in a network and evaluate inputs, the CommNode server must be in operation.

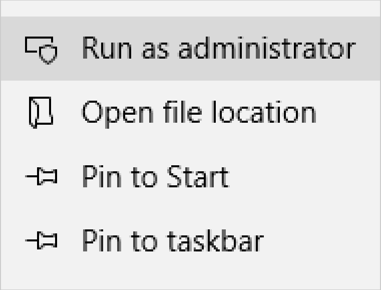
If you are not sure, check both services:

✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

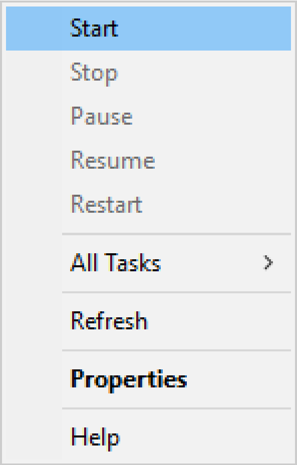
✓ Components connected to power.

1. Press the Windows key.
2. Enter *services*.
3. Right-click on the displayed entry to open the context menu.
4. Select the Run as administrator item.



5. Enter your user name and your password if necessary.
   ↳ The Windows "Services" window will open.
6. Look for the following services: SimonsVoss CommNode Server and/or SimonsVoss VNHost Server.

7. Export the status of the services.
8. If the services are not implemented, right-click to open the services' context menu.
9. Select the Start item.



↳ Service is launched.

10. Execute programming (see *Programming [▸ 29]*).

↳ Controller is programmed.

IP configuration error

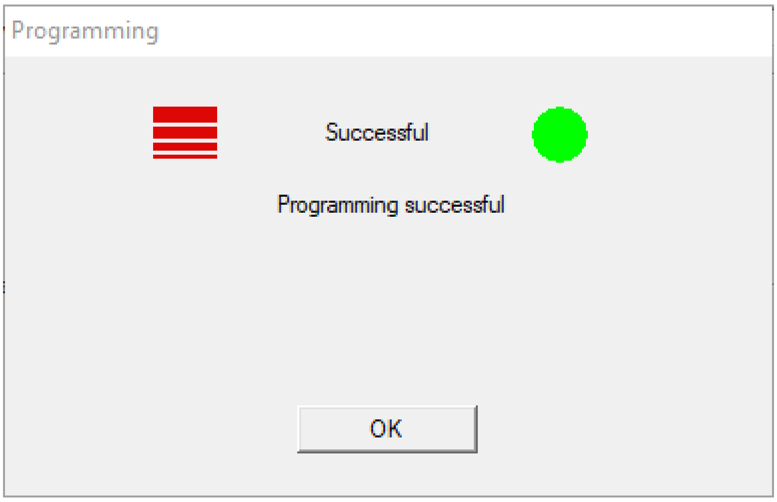
Another possible cause of transmission errors during programming is an error in the IP configuration in the SmartRelay (takes a very long time trying to read before displaying error message).

In such a case, please issue a new IP address in LSM and execute programming with a USB cable.

✓ LSM launched.
✓ Controller connected to computer with USB cable.
✓ Components wired correctly (see *wiring [▸ 58]*).
✓ Components connected to power.

1. Double-click on the SmartRelay 3 entry in the matrix to open the settings.
2. Change to the [IP settings] tab.
3. Enter a different free IP address (see *Establishing IP settings [▸ 28]* on how to detect a free IP address).
4. Click on the Apply button.
5. Click on the Exit button.
6. Execute programming with a USB cable (see *Programming [▸ 29]*).

   ↳ "Programming successful" window is displayed.


Programming

Successful

Programming successful

↳ IP configuration error has been eliminated.

13.3 Permanent relay switching in the SmartOutput module

A possible cause of permanently closed relay contacts in the SmartOutput module may be the use of time zone control for time change-over.

IMPORTANT

Unintentional opening due to use with SmartOutput module

The opening behaviour with a SmartOutput module in conjunction with time zone control deviates from the opening behaviour without the SmartOutput module.

All relays in the SmartOutput module are switched.

- See the sections on *Extended configuration with SmartOutput modules [▸ 140]* and *Extended configuration without SmartOutput module [▸ 139]*.

1. Deactivate time change-over.
2. Execute programming (see *Programming [▸ 29]*).

13.4 Problems with inputs or network readout/programming

If the controller or LSM do not respond to inputs or readout and programming over the network fails, it may be that services are not running correctly. Proceed as follows in this case:

Restart services

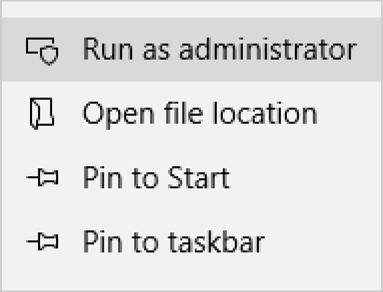
✓ Controller has already been programmed.

✓ Components wired correctly (see *wiring [▸ 58]*).

✓ Components connected to power.

1. Press the Windows key.

2. Enter *services*.
3. Right-click on the displayed entry to open the context menu.
4. Select the Run as administrator item.



5. Enter your user name and your password if necessary.
   ↳ The Windows "Services" window will open.
6. Look for the following services: *SimonsVoss CommNode Server* and/or *SimonsVoss VNHost Server*.
7. Right-click to open the services' context menu.
8. Select the Restart item.

Re-writing config files

You may need to re-write config files. To do so, open the corresponding communication node in LSM and re-write the config files.

13.5 Time change-over does not respond to change

If the time change-over does not respond to changes to the time zone plan, it may be that the changes have not been made in Group 5 or another time zone plan has been assigned.

1. Ensure that you have been editing the time zone plan assigned to the SREL3 ADV system.
2. Ensure that you have been editing Group 5.

14. Technical specifications

14.1 Order numbers

Controller

SREL3.CTR.ADV.G2	Controller for the SREL3 ADV system (standard version)
SREL3.CTR.ADV.ZK.G2	Controller for the SREL3 ADV system (version with time zone management and event logging)

LED reader

SREL3.EXT2.G2.GY	LED reader for the SREL3-ADV-System (anthracite, standard version)
SREL3.EXT2.G2.GY.COVER	LED reader for the SREL3-ADV-System (anthracite, standard version with vandalism protection frame)
SREL3.EXT2.G2.GY.WP	LED reader for the SREL3-ADV-System (anthracite, version with splash protection)
SREL3.EXT2.G2.GY.WP.COVER	LED reader for the SREL3-ADV-System (anthracite, version with splash water protection and vandalism protection frame)
SREL3.EXT2.G2.W	LED reader for the SREL3-ADV-System (white, standard version)
SREL3.EXT2.G2.W.COVER	LED reader for the SREL3-ADV-System (white, standard version with vandalism protection frame)
SREL3.EXT2.G2.W.WP	LED reader for the SREL3-ADV-System (white, splash-proof version)
SREL3.EXT2.G2.W.WP.COVER	LED reader for the SREL3-ADV-System (white, version with splash water protection and vandalism protection frame)

Reader

SREL3.EXT.G2.W	Reader for the SREL3 ADV system (standard version)

SREL3.EXT.G2.W.WP	Reader for the SREL3 ADV system (version with splash water protection)

SmartOutput module

MOD.SOM8	SmartOutput module (standard version)

Accessories

POWER.SUPPLY.2	Power supply unit (12 V_{DC}, 500 mA)
SREL2.COVER1	Vandalism protection housing
SREL3.COVER.GY	Vandalism protection frame for LED reader, anthracite
SREL3.COVER.W	Vandalism protection frame for LED reader, white

14.2 Properties

14.2.1 Controller

Housing	
Material	ABS plastic, UV-stable
Colour	Same as RAL 9016 (traffic white)
Standard protection rating	IP20
Wiring to device	■ Flush mounting ■ Surface mounting
Power supply (only one power supply must be connected)	
Screw terminals	■ V_{IN}: 9 V_{DC} – 32 V_{DC} ■ Power input: max. 3 W ■ Reverse voltage protection: yes The max. current depends on the supply voltage and the activity of the controller.

Pin connector	■ V_{IN}: 9 V_{DC} – 32 V_{DC} (Power supply must be limited to 15 W) ■ Power input: max. 3 W ■ Size: ≥ 2.0 mm inner Ø (recommended: 2.1 mm or 2.5 mm) and ≤ 5.5 mm Outer-Ø (recommended: 5.5 mm) The max. current depends on the supply voltage and the activity of the controller.
Power over Ethernet (PoE)	■ IEEE 802.3af compliant ■ Fully insulated ■ V_{IN}: 36 V_{DC} to 57 V_{DC} ■ PoE budget to be provided: max. 10 W (includes up to three readers powered by the controller) ■ indicated by red LED The PoE supply voltage is reduced to 13 V_{DC} by a voltage transformer. If you apply a supply voltage higher than 13 V_{DC} to the screw terminals or the round plug, the controller is not supplied with voltage via the PoE interface, but via the voltage supply input with the highest applied voltage.
Outputs	3 outputs to supply external reader (V_{OUT} = V_{IN} – 1 V_{DC})*
Battery	
Type	1x lithium cell CR1220 (3 V, 40 mAh) Manufacturers: Duracell, Murata, Panasonic, Varta. Batteries coated with bitter substances are not suitable.
Exchangeable	Yes
Duration	■ > 10 years (inactive) ■ > 2 years (active) Battery status can be called up via LSM. Battery is not used as long as controller is connected to power supply.
Real-time clock (RTC)	
Accuracy	max. ± 20 ppm (≈ 10 minutes per year)
Ambient conditions	

Temperature range	-25 ºC to +60 ºC (operation) 0 ºC to +30 ºC (in storage > 1 week)
Humidity	Max. 90%, non-condensing
Interfaces	
TCP/IP	Features: HP Auto_MDIX, DHCP Client, IPv4 10Base-T-/100Base-T-Standard TCP server: 1x each on port 9760 and 9770 IP address freely programmable, preset: 169.254.1.1 Connection: RJ45
USB	High-Speed USB Vendor ID: 0x2AC8, Product ID: 0x101 Device HID class Connection: Mini-B
RS485	Serves as interface to external readers (SREL3.EXT.*) and other bus devices. Connections: 3 Baud rate: 1 MBd Length: ≤ 150 m, abs. max. 300 m (depending on firmware and cable)
Signal	
LED	1 RGB 1 red
Programming	
Interfaces	TCP/IP USB External reader (support depends on firmware) LNI (support depends on firmware)
Memory	SD card (memory: ≥ 2 GB. SD card may not be removed or exchanged!)
Entries in the access list	Max. 1499 accesses
Relay	

Quantity	2x, independently programmable (support of second relay firmware dependent)
Switch modes	Programmable. - Monoflop - Flip-flop
Switching time	Programmable from 0 s to 25 s.
Contact mode	- 1x NO - 1x NC
Switching voltage	30 V_{DC} (resistive load), 24 VAC
Switching current	max. 200 mA (resistive load)
Digital inputs	
Quantity	4
Level	- Low: 0 V_{DC} to 0.5 V_{DC} - High: 4 V_{DC} to max. 30 V_{DC}
External contact	Used for the connection of external devices. A potential-free contact can be connected between the inputs (I1, I2 or I3) and the I+ connection.
Digital outputs	
Quantity	4
Type	Open drain
Switching voltage	30 V (resistive load)
Switching current	max. 200 mA (resistive load)
Power supply	The O+ connection is available for the power supply. An external pull-up resistor (approx. 1-10 kΩ) can be connected between the digital outputs (O1, O2, O3 or O4) and O+.
Serial ZK interface	

Supported protocols	■ Wiegand, 33 bit ■ Wiegand, 26 bit ■ Primion ■ Siemens Cerpass ■ Kaba Benzing ■ Gantner Legic ■ Isgus
Electrical specifications	See digital outputs

IMPORTANT

***) Undervoltage at the reader with PoE supply**

When the controller is powered via PoE, a voltage converter reduces the PoE supply voltage to 13V. This voltage is available for supplying the connected readers and may not be sufficient for long cables or too small cross-sections to ensure trouble-free operation of the reader (see also *Information on cabling [▸ 176]*). Take one of the following actions:

1. Use an external power supply for the reader.
2. Use an external power supply for the controller, whose voltage significantly exceeds 13 V_{DC} to increase the internal supply voltage. This also increases the supply voltage for the reader and the voltage drop on the line no longer has any effect.
3. Shorten the cable length.
4. Increase the cable cross-section.

14.2.2 Reader

Housing	
Material	ABS plastic, UV-stable
Colour	Same as RAL 9016 (traffic white)
Standard protection rating	IP20
	IP65 with WP variant
	Vandalism-resistant housing available
Wiring to device	Flush mounting
Power supply	

Screw terminals	- V_{IN}: 9 V_{DC} – 32 V_{DC} (Power supply must be limited to 15 W) - Power input: max. 3 W - Reverse voltage protection: yes The max. current depends on the supply voltage and the activity of the reader.
Controller powered	Supply via looped-through controller supply voltage The max. current depends on the supply voltage and the activity of the reader.
Ambient conditions	
Temperature range	- -25 °C to +60 °C (operation) - 0 °C to +30 °C (in storage > 1 week)
Humidity	Max. 90%, non-condensing
Interfaces	
RS485	Serves as an interface to the controller of the SREL3-ADV system. - Number of ports: 1 - Length: ≤ 150 m, abs. max. 300 m (depending on firmware and cable)
RFID	- 13.56 MHz - Read range: 0 mm to 15 mm (depending on card format) - Supported cards: Mifare Classic, Mifare DESFire EV1/EV2)
B-field	Interface to SimonsVoss transponders. - Read range (approx.): 5 cm to 60 cm (☐ Close-up range mode, ☑ Gateway) - Read range (approx.): 5 cm to 100 cm (☐ Close-up range mode, ☐ Gateway)
Signal	
LED	1 RGB
Audio signal	1 piezo buzzer
Programming	

Interfaces	The reader is programmed exclusively via controller. Interfaces of the controller: ■ USB ■ TCP/IP For details, see controller.

Radio emissions

15.24 kHz - 72.03 kHz Only for item numbers: SREL3.EXT.*, SREL3.EXT2.*	10 dBµA/m (3 m distance)
13.560006 MHz - 13.560780 MHz Only for item numbers: SREL3.EXT.*, SREL3.EXT2.*	1.04 dBµA/m (3 m distance)

14.2.3 LED reader

Housing	
Material	PA6 plastic (50% glass fiber reinforced, UV stable)
Colour	■ Dark gray, similar to RAL 7021 or ■ White, similar to RAL 9016
Standard protection rating	IP20
	IP65 with WP variant
	Anti-vandalism frame available
Wiring to device	Flush mounting
Power supply	
Screw terminals	■ V_{IN}: 9 V_{DC} – 32 V_{DC} (Power supply must be limited to 15 W) ■ Power input: max. 3 W ■ Reverse voltage protection: yes The max. current depends on the supply voltage and the activity of the reader.

Controller powered	Supply via looped-through controller supply voltage The max. current depends on the supply voltage and the activity of the reader.
Ambient conditions	
Temperature range	- -25 °C to +60 °C (operation) - 0 °C to +30 °C (in storage > 1 week)
Humidity	Max. 90%, non-condensing
Interfaces	
RS485	Serves as an interface to the controller of the SREL3-ADV system. - Number of ports: 1 - Length: ≤ 150 m, abs. max. 300 m (depending on firmware and cable)
RFID	- 13.56 MHz - Read range: 0 mm to 15 mm (depending on card format) - Supported cards: Mifare Classic, Mifare DESFire EV1/EV2)
B-field	Interface to SimonsVoss transponders. - Read range (approx.): 5 cm to 60 cm (☐ Close-up range mode, ☑ Gateway) - Read range (approx.): 5 cm to 100 cm (☐ Close-up range mode, ☐ Gateway)
Signal	
Visually	3 LEDs (red, green, yellow)
Audio signal	1 piezo buzzer
Programming	
Interfaces	The reader is programmed exclusively via controller. Interfaces of the controller: - USB - TCP/IP For details, see controller.

Radio emissions

15.24 kHz - 72.03 kHz Only for item numbers: SREL3.EXT.*, SREL3.EXT2.*	10 dBµA/m (3 m distance)
13.560006 MHz - 13.560780 MHz Only for item numbers: SREL3.EXT.*, SREL3.EXT2.*	1.04 dBµA/m (3 m distance)

14.2.4 SmartOutput module

Housing	
Material	Housing: Polycarbonate plastic, fibre-reinforced Cover: Polycarbonate plastic
Colour	Housing: green similar to RAL 6021 (pale green) Cover: transparent
Standard protection rating	IP20
Weight	~ 170 g (without packaging)
Installation	DIN rail (37 mm × 15 mm)
Power supply	
Screw terminals	V_{IN}: 12 V_{DC} (11 V_{DC}–15 V_{DC}) Standby current: < 120 mA Max. current: < 150 mA Reverse voltage protection: yes
Ambient conditions	
Temperature range	0 °C to +60 °C (operation) 0 °C to +70 °C (in storage > 1 week)
Humidity	Max. 90%, non-condensing
Interfaces	

RS485	Acts as an interface to the SREL3 ADV system controller. - Number of ports: 1 - Length: ≤ 150 m, max. distance 300 m (depending on firmware and cabling)
Signal	
LED	1 RGB
	8 green
Relay	
Quantity	8x, programmable separately from one another
Switching modes	Monoflop
Switching interval	Programmable between 1 s and 25 s (except 0 s, as on controller).
Contact type	1x NO
Contact material	AgNi+Au
Service life (electrics)	12 V_{DC} / 10 mA: typ. 5 × 10^7 switching cycles
Service life (mechanical)	Typically 100 × 10^6 switching cycles
Bounce time	Typically 1 ms, max. 3 ms
Vibrations	15 G for 11 ms, 6 shocks as per IEC 68-2-27; not tested for permanent operation under vibration
AUX relay switching voltage	Max. 24 V
AUX relay switching current	- Max. 1 A permanent current - Max. 2 A switching current
Switching voltage in outputs	Max. 24 V
Switching current in outputs	Max. 200 mA
OUT switching current	Max. 1 A
OUTPUT switching voltage	Max. 24 V

OUTPUT switching power	Max. 1 VA
OUT switching behaviour for low voltage	$U_V < 10.5 \pm 0.5$ V corresponds to off

14.2.5 Information on cabling

Lines with data transmission	Cat 5 or installation cable for telecommunications systems (e.g. F-YAY 2x2x0.6)
Lines with data transmission and power supply	Cat 5 or installation cable for telecommunications systems (e.g. F-YAY 2x2x0.6)
Lines for power supply only	Any line (e.g. F-YAY 2x2x0.6)

IMPORTANT

Take voltage drop into account

The resistance in copper produces a voltage drop, the size of which depends on the cable gauge, current flow and cable length. The power supply lines must be adequately dimensioned.

1. Ensure that the cable gauge in lines is adequate for power supply. Use another suitable cable where necessary.
2. If required, merge wire pairs to increase the cable gauge.
3. Use a power source located closer to the SmartOutput module if needed.
4. If possible, increase the supply voltage (observe technical specifications).

IMPORTANT

Malfunctions due to interference

Sources of interference may impair functional reliability.

1. Observe the installation instructions (see *Installation [▸ 98]*).
2. Use shielded twisted pair cables.
3. Connect the cable shielding to the earth potential.

*) Undervoltage at the reader with PoE supply

When the controller is powered via PoE, a voltage converter reduces the PoE supply voltage to 13V. This voltage is available for supplying the connected readers and may not be sufficient for long cables or too small cross-sections to ensure trouble-free operation of the reader (see also *Information on cabling [▸ 176]*). Take one of the following actions:

1. Use an external power supply for the reader.
2. Use an external power supply for the controller, whose voltage significantly exceeds 13 V_{DC} to increase the internal supply voltage. This also increases the supply voltage for the reader and the voltage drop on the line no longer has any effect.
3. Shorten the cable length.
4. Increase the cable cross-section.

You can use the form to calculate sparkover for copper cabling. The form takes into account the maximum length which is calculated based on the voltage drop. It does not check any other sources of interference such as transfer resistances or electromagnetic interference fields, which limit the maximum cable length to 300 m. The following formula is used:

$$L_{Customer's\ cable\ (copper)} = \frac{1}{2} * A_{Customer's\ cable} * \frac{\frac{V_{IN\ (customer\ power\ supply)} - 8{,}5V}{0{,}334A}}{1{,}75 * 10^{-2}\,\frac{\Omega * mm^2}{m}}$$

The result is the maximum length, which is calculated based on the voltage drop. This length comprises a forward and return path. You should use an own power supply unit to increase operational reliability if the cable is more than 75% of the maximum calculated length.

Enter the following values into this form:

Value	Explanation
Supply voltage V_{IN} [V]	Voltage in the connected power supply unit. Read the value on the power supply unit or ask the electrician responsible. Use 13 V if you supply the controller via PoE. Enter the number without the unit and use a decimal point if necessary (e.g. 13.5)
Cable gauge A [mm²]	Cross-section of the installed or projected cable. Read the value on the cable or ask the electrician responsible. Enter the number without the unit and use a decimal point (e.g. 0.5).

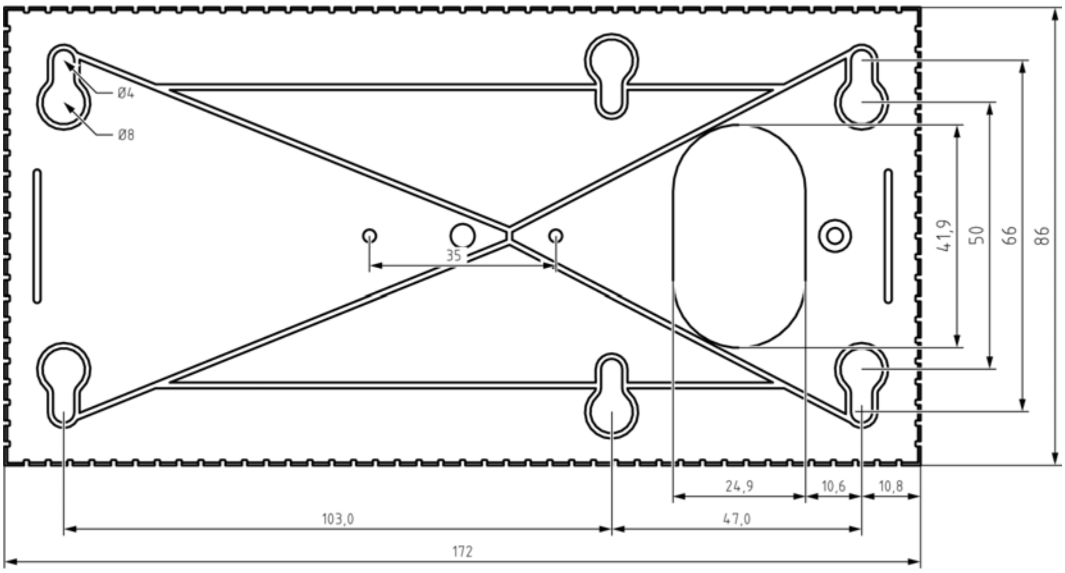
Supply voltage: ______ V
Cable section: ______ mm²
Cable length (max.) 0 m

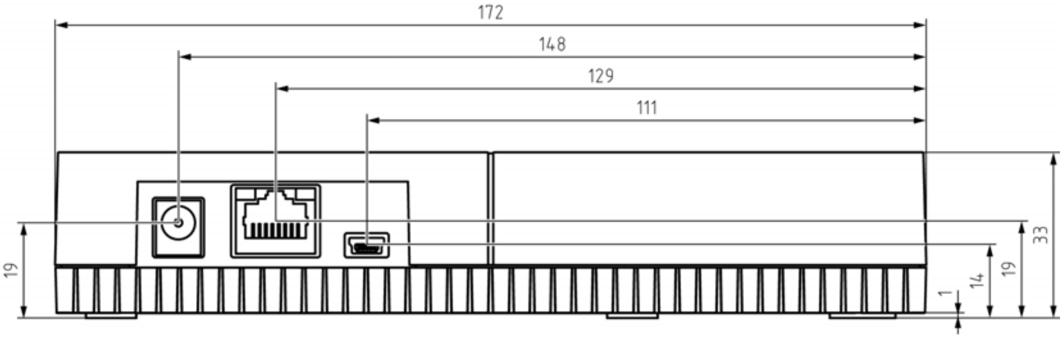
The following table contains the maximum lengths for frequently used cable gauges and supply voltages.

	0.1022 mm² (=AWG27)	0.14 mm²	0.2 mm²	0.6 mm²
PoE	39 m	53 m	76 m	230 m
9 V	4 m	5 m	8 m	25 m
12 V	30 m	41 m	59 m	179 m
24 V	135 m	185 m	265 m	300 m
32 V	205 m	281 m	300 m	300 m

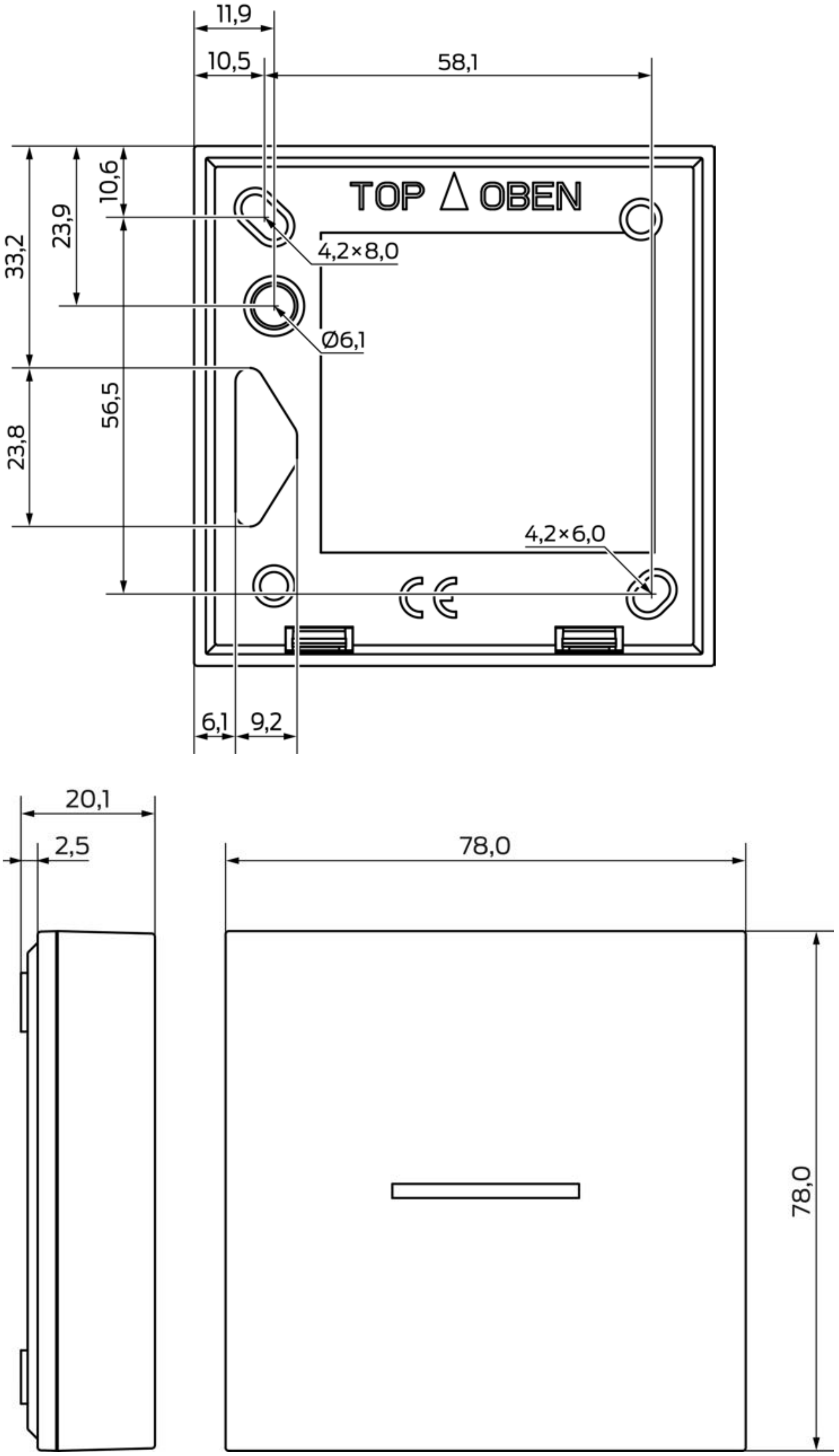
14.3 Dimensions

14.3.1 Controller

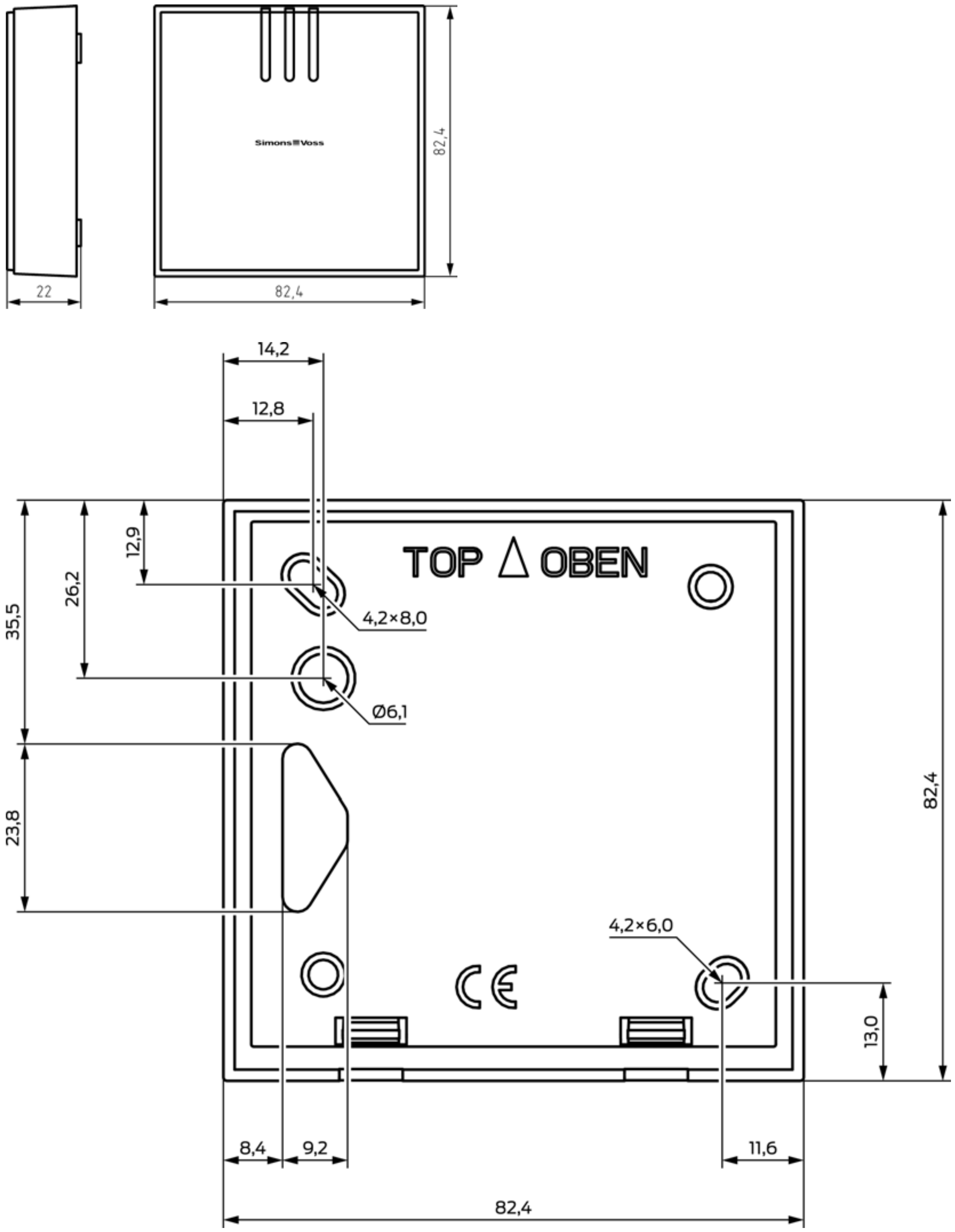




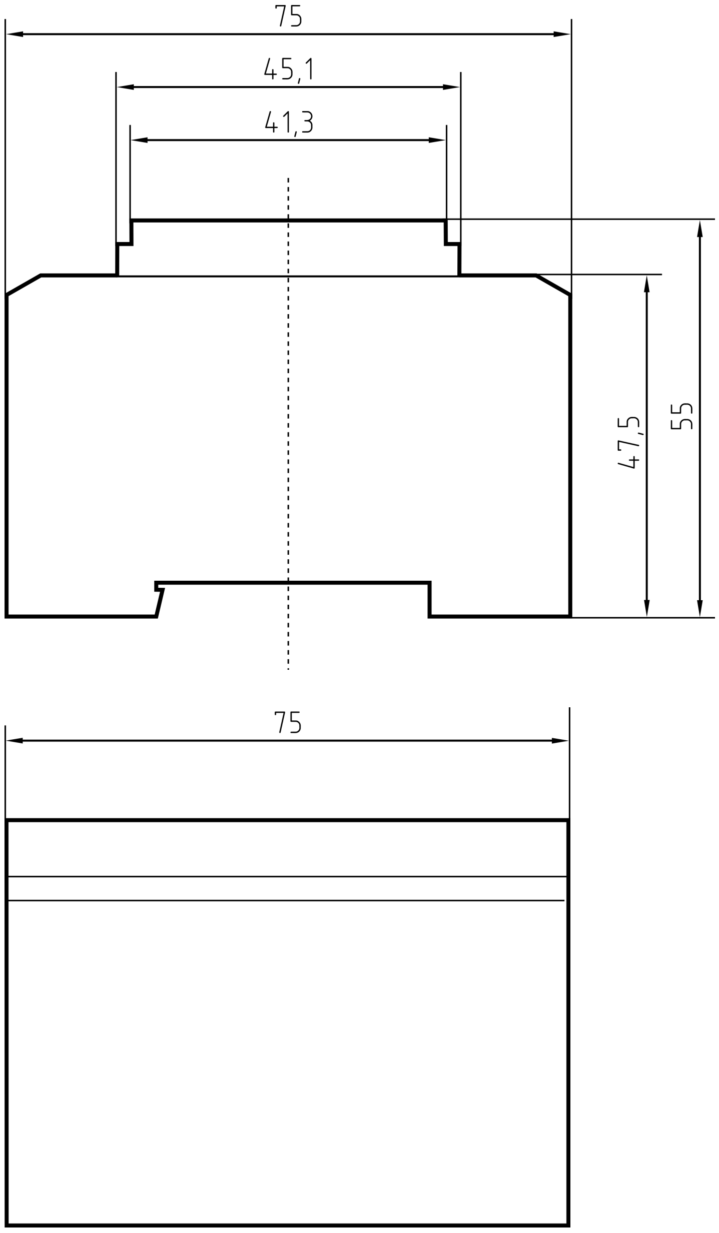
14.3.2 Reader


11,9
10,5
58,1
33,2
23,9
10,6
23,8
56,5
TOP △ OBEN
4,2×8,0
Ø6,1
4,2×6,0
CE
6,1
9,2
20,1
2,5
78,0
78,0

14.3.3 LED reader



14.3.4 SmartOutput module



14.4 Drilling templates

The drilling template scale is 1:1. You can print and the drilling templates in A4 format.

NOTE

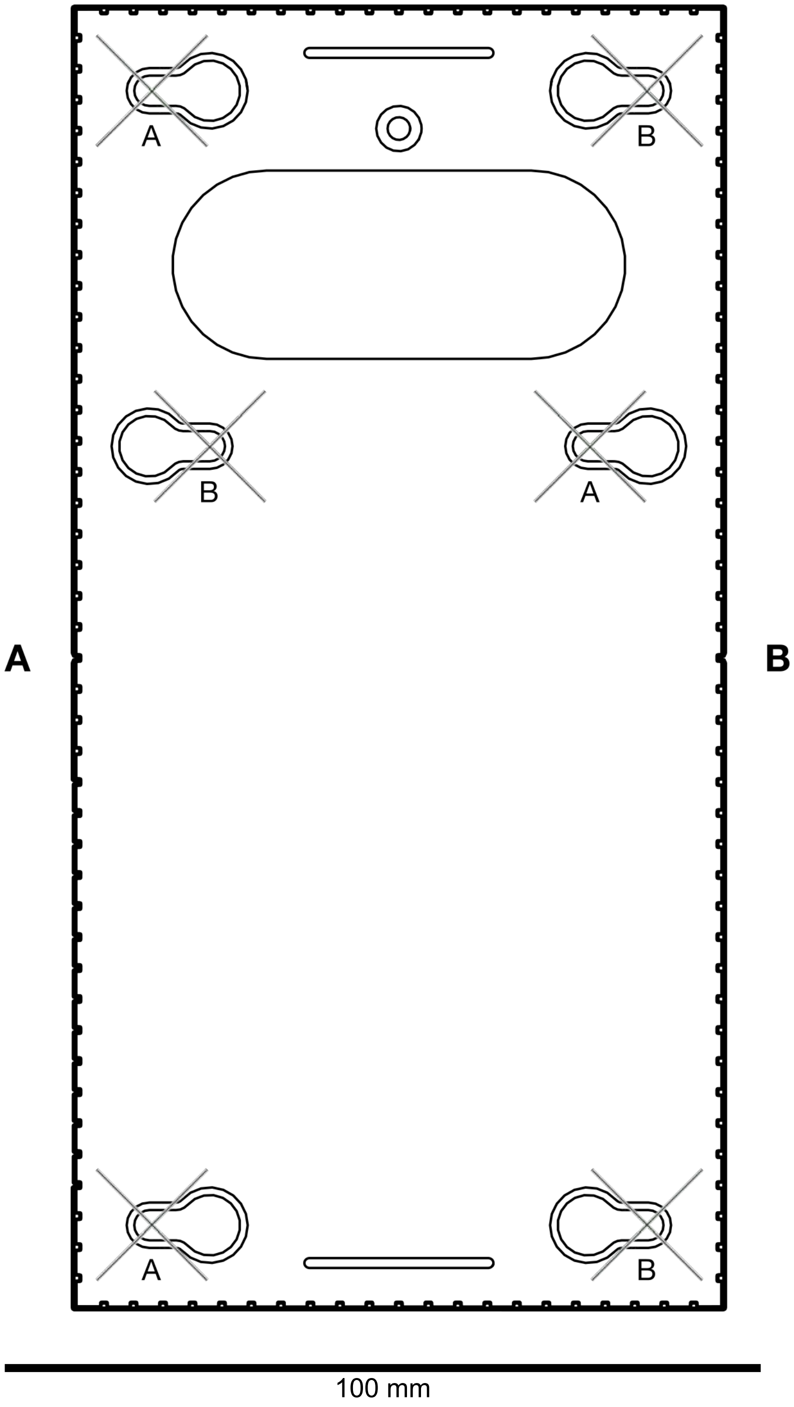
Ensure that the print settings are not set to reduce or enlarge. Use the lines under the drawings to check scale is correct.

14.4.1 Controller

IMPORTANT

Only three drill holes are required to mount the controller.

1. If you fit the controller with Side A facing upwards, drill the holes marked "A".
2. If you fit the controller with Side B facing upwards, drill the holes marked "B".

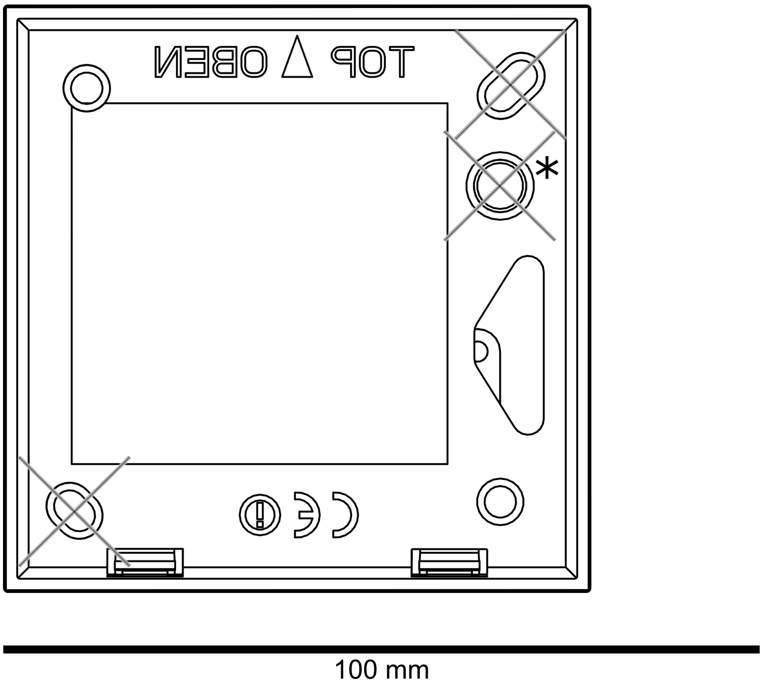


14.4.2 Reader

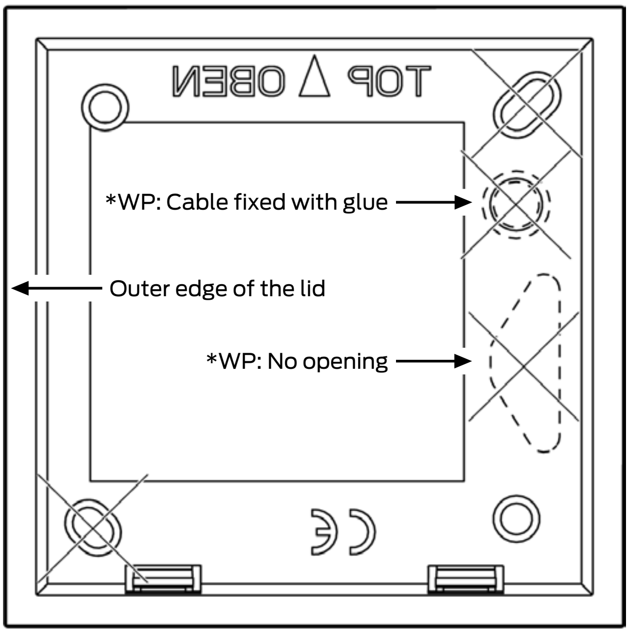
IMPORTANT

The asterisk marks an optional drill hole. It is not required to fasten the reader, but it can be used to feed the cable in the WP variant.

- Only drill this hole if you wish to use the hole as a cable feed-through for the WP variant.



14.4.3 SREL3 LED/LR reader drilling template



15. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

https://www.simons-voss.com/en/documents.html

Software and drivers

Software and drivers can be found on the website:

https://www.simons-voss.com/en/service/software-downloads.html

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

https://www.simons-voss.com/en/certificates.html

Information on disposal

- Do not dispose the device (SREL3.CTR.*, SREL3.EXT.*, SREL3.EXT2.*) in the household waste. Dispose of it at a collection point for electronic waste as per European Directive 2012/19/EU.
- Recycle defective or used batteries in line with European Directive 2006/66/EC.
- Observe local regulations on separate disposal of batteries.
- Take the packaging to an environmentally responsible recycling point.

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

https://faq.simons-voss.com/otrs/public.pl

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany

This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

SimonsVoss
technologies

Made in Germany

A BRAND OF
ALLEGION™