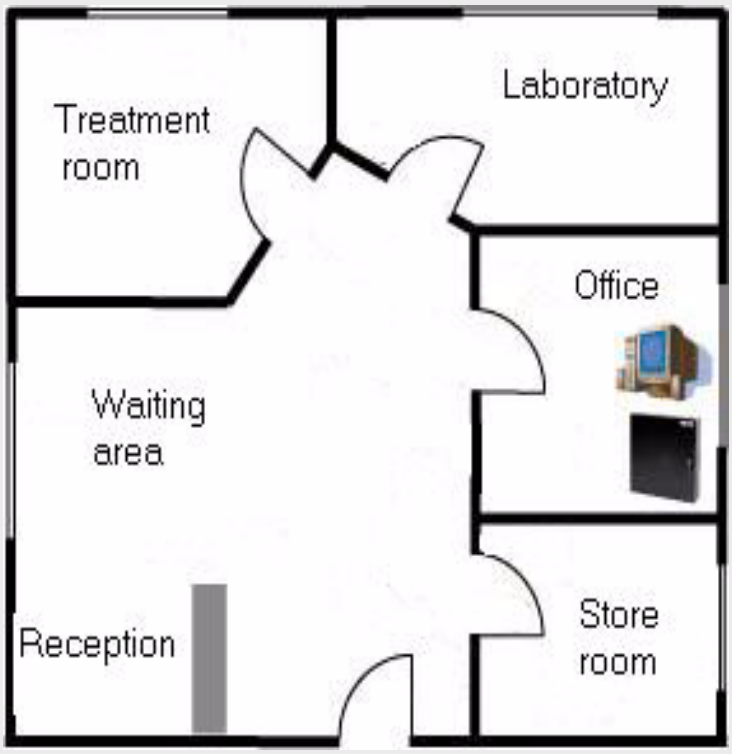


Access Control by Example

ACCBYEG

BOSCH

en Introductory Guide

Table of Contents

1 Introduction

Purpose of this document

Based on a simple example, which nevertheless contains most of the common kinds of door control, this document provides an introduction to installing a small access control system. Its intention is to steer beginners safely past some of the common dangers and pitfalls.

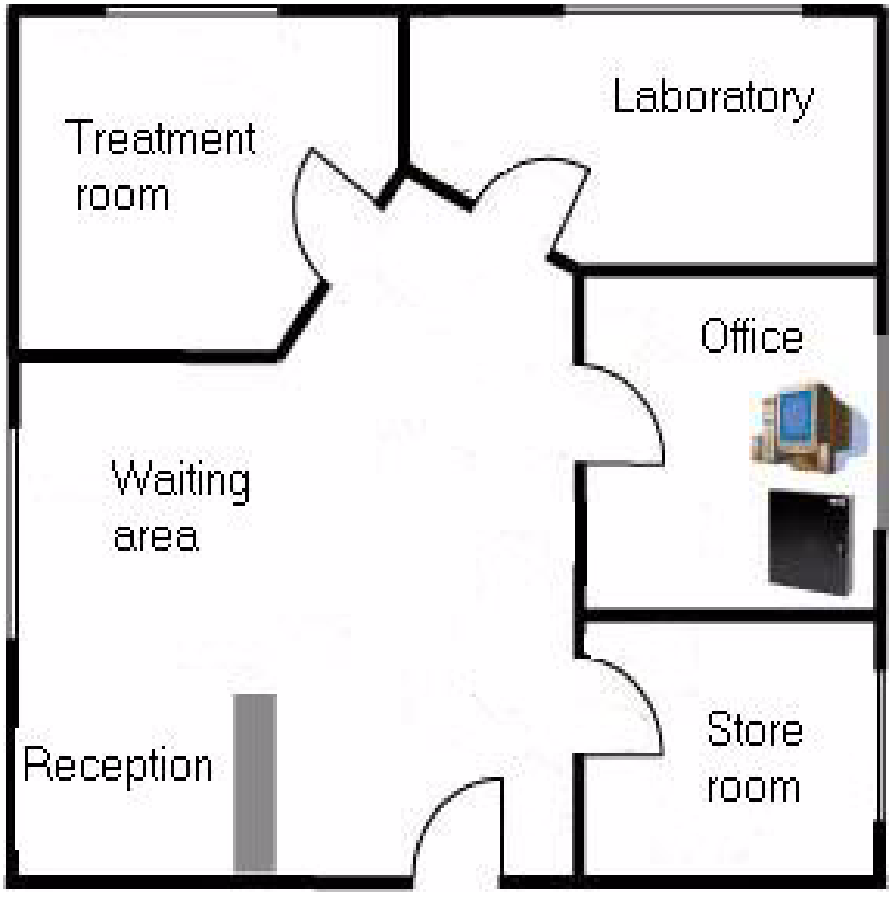
Intended audience

This document is intended for persons who will be involved, perhaps for the first time, in physically implementing an access control system, and wish to gain a quick understanding of the main concepts and tasks involved.

1.1 The example

Dr. Jones has a small but busy medical practice in an inner-city area. In it there are five rooms:

1. A waiting room with reception area and public access between the hours of 9.00 and 16.00.
2. A general Storeroom, opening off the reception area, where bandages, crutches, office supplies and non-hazardous stock items are kept.
3. A laboratory and secure Storeroom, opening off the reception area, where prescription drugs, sharps and potentially hazardous materials are kept.
4. An office opening off the reception area, where a computer and patients' records are kept.
5. A treatment room, opening off the waiting area.



The access control requirements of the rooms are as follows:

Table 1.1

Room	Access for whom	Access control requirements
1. Waiting Room with reception area	Anybody between 09:00 and 16:00	Door should be unlocked at 9:00, locked at 16:00 and requires a card outside of those hours.
2. General Storeroom	Doctor, lab technician, receptionist	Access control to prevent theft.
3. Laboratory	Doctor, lab technician	Strict access control to prevent theft and reduce danger to persons from hazardous materials and equipment.
4. Office	Doctor, receptionist	Strict access control to prevent misuse or theft of medical records and other sensitive data.
5. Treatment room	Anybody, anytime, as admitted by the doctor.	No access control as no valuables are present, and patients are always accompanied by the doctor.

2 Materials Planning

The following section contains a rough analysis of the requirements, and helps you to select the parts required in the quantities you need. It is useful to think in terms of three tiers: The electrical components, the access controller and the host system. These tiers are covered in more detail below.

2.1 Planning the doors

For each of the doors mentioned in *Section 1.1 The example, page 4* we need to decide in general what functionality is required:

- The easiest case is the treatment room - it does not need to be locked and does not require any access control hardware.
- The main entrance to the practice will be unlocked during opening hours, and require a card outside those hours. The arrival of the first member of staff at the card reader in the morning should put the door into unlocked mode for the duration of opening hours.
- All the doors with card readers will require a REX (Request to EXit) unit. Its purpose is to provide an alarm-free exit without the need for a card. A REX signal comes typically from a push button or a motion detector inside the room, or is embedded in the door's own handle. Here we have decided on REX by motion detector.
- All access-controlled doors will require magnetic contacts in order to trigger an alarm if the door is opened by force.

2.2 Low tier: Electrical components

From these considerations we create a table of the doors and the electrical components each requires.

Room	Access control hardware
1. Waiting Room with reception area	Card Reader, e.g. Bosch Delta 1000 Electric door opener, e.g. Bosch Universal Electric Door Opener REX by motion detector, e.g. Bosch DS150i Magnetic contact, e.g. Bosch ISN-C devices
2. General Storeroom	Card reader Electric door opener REX by motion detector Magnetic contact
3. Laboratory	Card reader Electric door opener REX by motion detector Magnetic contact

Room	Access control hardware
4. Office	Card reader Electric door opener REX by motion detector Magnetic contact **Note**:This secured room, which already houses the computer, is the obvious place to put the access controller itself.
5. Treatment room	Nothing

2.2.1 Card reader technologies

Card readers differ in two important respects: scan frequency and protocol.

Scan Frequency: 125kHz vs. 13.56MHz

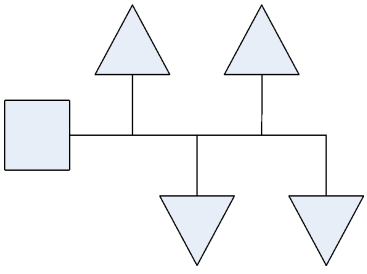
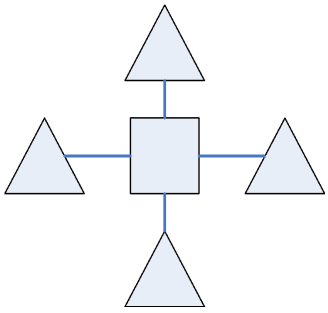
The most common scan frequencies for readers are 125kHz and 13.56 MHz.

125kHz is proven technology prevalent in the USA and in Eastern Europe. The cards and readers tend to be lower priced.

13.56 MHz is newer, more secure technology prevalent in EMEA and increasingly in APAC countries. Hardware is currently priced somewhat higher.

RS-485 vs Wiegand:

Decide early whether to use Wiegand or RS-485 technology for the readers; each has its own advantages and disadvantages. Maximum cable length and wiring topology are different, as the following table shows.

	RS-485 Readers	Wiegand Readers
Wiring topology	bus, (“chain”) 	star 
Maximum cable length	1200m	100m
Number of wires needed for the reader	4	10 (The slightly lower cost of Wiegand readers is offset by higher wiring costs and potential for wiring errors).

2.2.2 Credentials technology

Decide on the credentials technology you wish to use. For Wiegand readers the choice includes e.g. iCLASS (3.56MHz) and EM (125kHz) cards. For RS-485 readers there is a wide choice: MIFARE, HITEC or LEGIC. These credentials types are available in different physical formats: Most common are the classic credit-card sized identity cards, and the smaller tokens

and key fobs which usually carry no printed personal information.

2.2.3 Wiring for non-reader components

Depending on its manufacturer and model, each of these electrical components will require a certain number of wires to control its operation. Typical values for number of wires per component can be found in the table below.

Electrical component	Typical number of wires	Notes/explanation
Door opener	2	Power only
Magnetic contact	2	2 wires for power, but often extra wires for tamper detection
REX with push button	2	E.g. so that the receptionist can open the main entrance from her desk.
REX with motion detector	6	Highly variable depending on manufacturer: 2 wires for power, 2 to the magnetic contacts
Burglar alarm	4	(not used in this example)
Emergency exit	4	(not used in this example)

If you know the total number of wires a door (with all its electrical components) requires, and if you have access to the site during the building phase, then you can influence the kinds of cable which are laid to the doors.

Cables differ both in the number and the thickness of their wires (also known as “cores”). For distances under 25m, as in our example; a wire thickness of AWG18 or 1mm² will be sufficient. For longer distances and stronger currents correspondingly thicker wires will be required. The AMC2 tolerates a maximum 2V drop from AMC to the devices. Voltage drop is calculated by electricians according to standard formulae.
It is advisable to use a spreadsheet to track the sum and thickness of wires required per door.

NOTICE! Remember, although RS-485 readers can be wired together in a bus topology, other components are wired to the controller directly, i.e. in a star topology.
Although some RS-485 readers do provide limited connections for REX and/or magnetic contacts, we do not use that specialized functionality in this example.

2.3 Middle tier: Access Controllers

An access controller is an electronic device which handles input and output signals from and to the peripheral components (readers, door controllers, REX units, magnetic contacts etc). It is an interface through which the access control software communicates with these components, but the controller is able to handle some signal events on its own if it temporarily loses its connection to the software.
Examples are the Access Modular Controller AMC2 and the Access Easy Controller from Bosch Security Systems. The Access Easy Controller is controller hardware with a resident access control application. The AMC2 is software/host/reader neutral and provides variants to handle either RS-485 or Wiegand readers.

2.4 High tier: Hosting the software for the final system

Bosch offers a wide range of software products for configuring access control systems, depending on the size of the installation. For our small example one of two products would be suitable:

- **Access Professional Edition**: (Access PE)
  This product installs on a standard PC. It controls doors via hardware modules called Access Modular Controllers (e.g. the AMC2 4R4).
- **Access Easy Controller**: (AEC)
  The access control software is resident on the door controller itself (i.e. middle and high tiers are combined) and is operated over the network from a standard PC. It uses a web-browser for its user interface.

For the sake of example the following chapters describe two typical combinations:

- RS-485 technology, AMC2 controller and Access Professional Edition software
- Wiegand technology with Access Easy Controller hardware and software

Note: An installation of Access PE / AMC2 with Wiegand technology (a combination not covered in detail in this document) would proceed similarly to the Access PE chapter, but with each of the 4 readers connected directly to the access controller rather than “daisy-chained” to other readers. A suitable AMC2 variant would be the AMC2 4W.

NOTICE! The combination Access PE & AMC2 supports **both** RS-485 and Wiegand reader technology through deployment of corresponding variants of the AMC2 controller (e.g. AMC2 4R4 and AMC2 4W).
AEC supports only Wiegand.

3 Installation with RS-485, AMC and Access PE

This chapter describes the installation of our example access control system using **RS-485 communication to the readers, an AMC2 as access controller hardware and Access Professional Edition as the configuration software**. We will assume that all the components decided upon in *Section 2.2 Low tier: Electrical components, page 6* have been ordered from and delivered by the hardware vendor of your choice. The installation is basically a 6 stage process:

1. Mounting the access controller and associated hardware, see *3.1*
2. Installing the wiring, see *3.2*
3. Mounting the peripheral components, see *3.3*
4. Connecting the peripheral components to the wiring, see *3.4*
5. Connecting the AMC to the wiring from the peripheral components, see *3.5.2*
6. Connecting the AMC to the computer and configuring the software, see *3.5.3*

3.1 Mounting the access controller and associated hardware

The obvious room in which to locate the access controller, the power supply and the configuration PC is the **office**. In it the hardware and software will be protected from unauthorized access. The office is also situated centrally with regard to the doors. The controllers should be housed in a lockable metal enclosure or cabinet for extra security. The enclosure should also contain a battery to provide an uninterruptible power supply (UPS).

3.2 Installing the wiring

Lay the cables decided upon in *Section 2.2.3 Wiring for non-reader components, page 8* from the office to the respective doors. Aesthetically it is always preferable to hide cabling beneath floors, above ceilings or underneath wall plaster, but this is not always practical. Note - junction boxes are commonly used near doors; we leave them out of this example only for the sake of simplicity.
Make sure that cables carrying data (e.g. from the reader) are shielded, see *3.4.2*
Make sure that there is enough length to reach both components above the door (e.g. REX with motion detector, magnetic contacts) and components at handle height (e.g. reader, door opener).

3.2.1 RS-485 bus topology for readers

Readers in an RS-485 environment are connected in a bus topology, i.e. a reader is either connected directly to the controller and to the next reader, or it is connected to the previous and possibly the next reader as part of a chain with a maximum length of 4 readers. See *Section 2.2.1 Card reader technologies, page 7*.
With readers it is very important to follow the manufacturer's instructions as regards grounding (earthing) the device and its cable shielding. See also *Section Figure 3.3 Avoiding a ground loop, page 12*

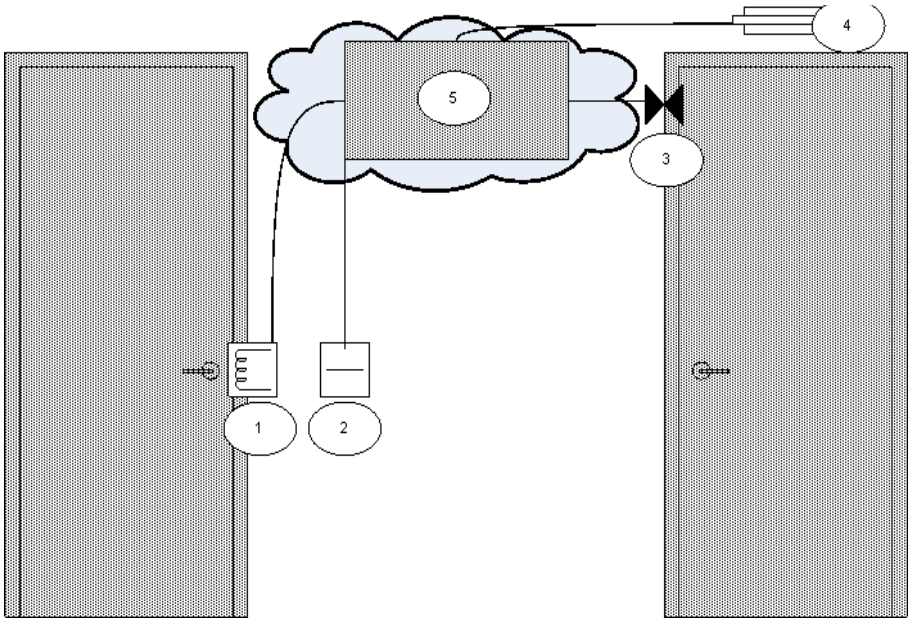
3.2.2 RS-485 star topology for all other components

Every other component in an RS-485 environment is connected directly to its respective controller in a star topology.

3.3 Mounting the peripheral components

Electrical components must always be mounted (i.e. attached to walls, racks, doors and door-frames) as per the manufacturer's instructions.

The following illustration shows typical locations of electrical components with respect to a door. Note that the access controller (5) should always be in a secured area to prevent tampering, preferably in a locked cabinet which has space for the power supply and backup battery to ensure an uninterruptible power supply.



Door from the outside	Same door from the inside
1: Door opener - 2 wires	3: Magnetic contact - 2 wires
2: Reader - 4 wires	4: REX with motion detector - 2 wires
5: Access controller. **NOTE: This should not be near the doors themselves, but should always be located in a secured area** (here represented by the cloud).	

3.4 Connecting the peripheral components to the wiring

Electrical components must always be connected as per the manufacturer's instructions. Nevertheless there are certain basic rules and pitfalls which should be well understood by every installer of access control devices. Please read the following sections carefully.

3.4.1 Protective diodes

A door opener typically locks or unlocks a door by means of a magnet which is subjected to an electric current. When this power is switched off a high voltage is induced in the magnetic coil, which needs to be dissipated to prevent damage to other components. This is generally done by means of a protective diode.

CAUTION!

If the door opener (or other magnetic component, e.g. a door holding magnet) does not have an inbuilt protective diode, be sure to connect such a diode electrically in parallel with it. See illustration below. *Section Figure 3.2 Position of the protective diode, page 12*. Install protective diodes wherever excess voltage can be induced by magnetic fields. Suitable diodes are generally included in the hardware delivery.

Figure 3.1 A diode (Note the colored ring)

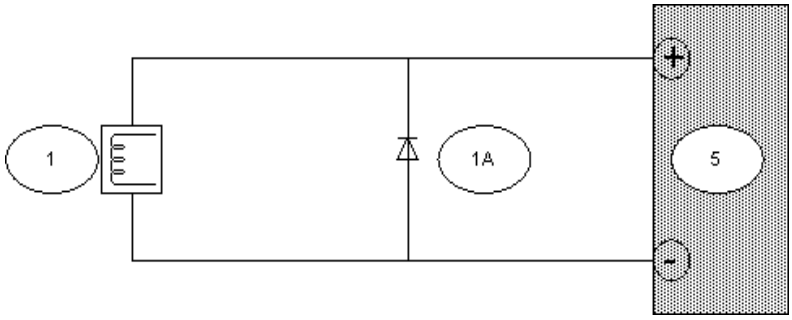


Figure 3.2 Position of the protective diode

Key: 1: Door opener, 1A: Protective diode, 5: Access controller

The colored ring corresponds to the crossbar in the diode symbol.

3.4.2 Shielding data cables and avoiding ground loops

Cables with cores that carry data have a conducting wrapper, accompanied by a naked grounding wire, between the cores and the outer plastic casing. When the naked wire is grounded properly this wrapper “shields” the cores from electrical interference. Without shielding, the integrity of the data signals is threatened.

A common installation error (particularly in cases where the reader-end and the controller-end of the cable are handled by different persons) is to ground the shielding at **both ends**. If the two grounds are not of identical potential, there is a possibility of current flow through the shielding, which can disrupt the signals in unpredictable ways, cause malfunctions in the access control hardware and even masquerade as software errors. This phenomenon is known as a **ground loop**.

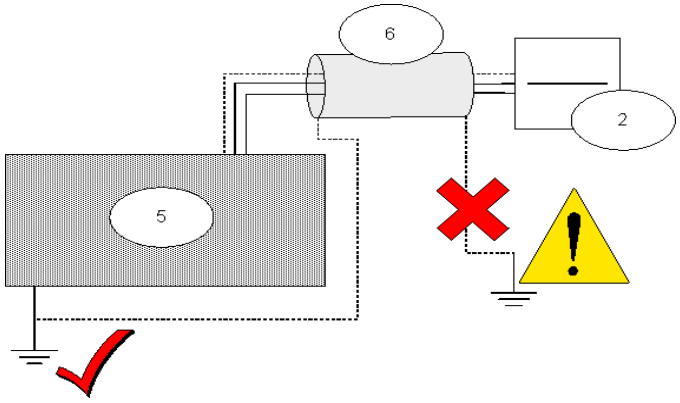


Figure 3.3 Avoiding a ground loop

5: Access controller	6: Shielding around cable	2: Reader

CAUTION!

To avoid ground loops, be sure to ground cable shields only ONCE.

CAUTION!

Follow carefully the grounding instructions for the reader and other sensitive components. Failure to ground components correctly can result in damage to those components and to malfunction of the access control hardware, which can masquerade as a software error.

3.5 Connecting the AMC2 (Access Modular Controller)

The following is an illustration of a typical AMC2. Here the AMC2 4W.

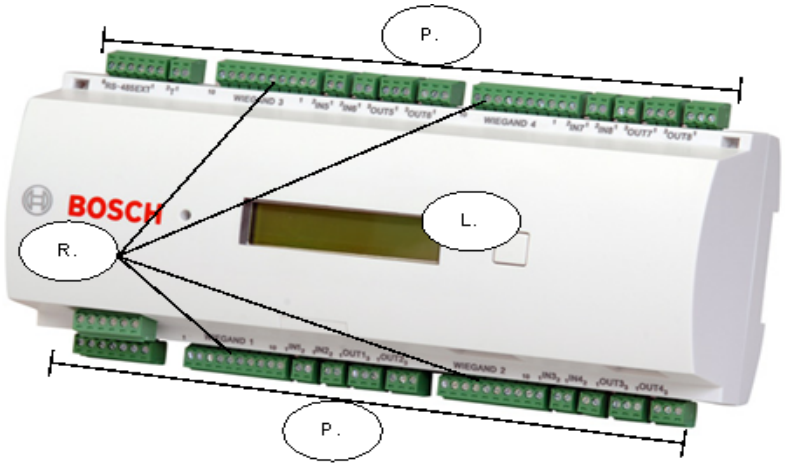


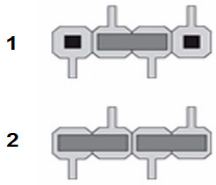
Figure 3.4 An AMC2 access controller

R: Reader connections	P: Pluggable screw terminals	L: LC Display

Space restrictions do not permit a detailed treatment of the AMC2 controller hardware, of which there are several variants. Always consult the installation guide of the controller you are using. For our example we have chosen the **AMC2 4R4**. The relevant installation guide, along with all the other documentation referenced below, is available in PDF format from the Bosch Security Systems internet site, see *Section 5 Resources and further reading, page 27*
As we only need to control 4 doors, one AMC2 device will be sufficient. For connection to the access control software we will use an ethernet crossover cable aka “null modem” (alternatively you could use normal ethernet cables and place a hub or a “switch” between computer and access controller). Other possibilities for the software connection are RS232 (serial) and RS-485 bus). For the power supply we will use the standard Bosch **PBC-60** which also charges the UPS backup battery.

3.5.1 Preparatory steps on PBC-60 power supply, AMC2 and computer

Step no.	Where	Step description	Illustrations / Reference
1	PBC	**Make sure the PBC-60 is not plugged in (under power)**, then use the switch on the side of the PBC-60 to set which voltage is to be fed to the AMC2. In our example we require only 12V for a simple door opener. Certain peripheral devices, especially some readers and powerful door openers, require 24V.	PBC-60 Datasheet.
2	PBC	Connect the battery temperature sensor to the RTH socket, even if no UPS battery is being used. If a battery is used then sensing end should be placed near the battery. This sensor is supplied with the PBC-60	PBC-60 Datasheet.
3	AMC	Remove pluggable screw terminals and open the AMC casing to gain access to internal jumpers and DIL switches.	AMC2-4R4 installation guide “Opening the case”

Step no.	Where	Step description	Illustrations / Reference
4	AMC	On the underside of the AMC's circuit board, set the relay output jumpers for the relay outputs to "wet mode" i.e. the AMC2 should provide a voltage to our door openers. In the illustration opposite... jumper setting 1 shows "dry" (voltage free) mode, and setting 2 shows "wet" (voltage provided) mode.	AMC2-4R4 installation guide "Connecting relay outputs" 
5	AMC	Ensure that the DIL switch number one is set ON and the rest are off, to identify this AMC to the software as device number one via the ethernet connection.	AMC2-4R4 installation guide "DIL switch selector"
6	AMC	Close the AMC casing and replace the pluggable screw terminals.	AMC2-4R4 installation guide "Closing the case"
7	AMC	Short circuit the tamper contact at S13, see *Figure 3.5*. This connection exists to provide protection against tampering with the AMC device. For our simple example we do not require it, and rely instead upon the security of the office itself.	AMC2-4R4 installation guide "Tamper protection"
8	Computer	Install Access Professional Edition on the computer which is to be used to configure this access control system.	Access Professional Edition - Installation manual

CAUTION!
Note: To use door openers or other devices **with their own external power supplies** you must ensure the relay output jumpers are set to the factory-default "dry mode" position, i.e. providing **no** voltage to the relay outputs.

3.5.2 Connecting the peripheral components to the AMC2

The AMC2 possesses 23 connectors of the pluggable screw terminal type. Wires can be fastened with holding screws to the terminals, and these terminals can be plugged and unplugged at the AMC2.

We will use nearly all the available connections, as shown in *Section Figure 3.5 The AMC2 connections used in the 4-room surgery example., page 15*. The numbering scheme S1-S23 is taken from the AMC2-4R4 installation guide.

We will connect 2 readers (Main entrance and Laboratory) in a bus topology to connection S2, and 2 readers (Storeroom and Office) to connection S7. **Note**: S2 and S7 are both connectors to the same RS-485 bus, and this bus may only have a total of 8 readers. The two reader connectors on the upper edge of the AMC2 4R4 (S14 and S19) are not used.

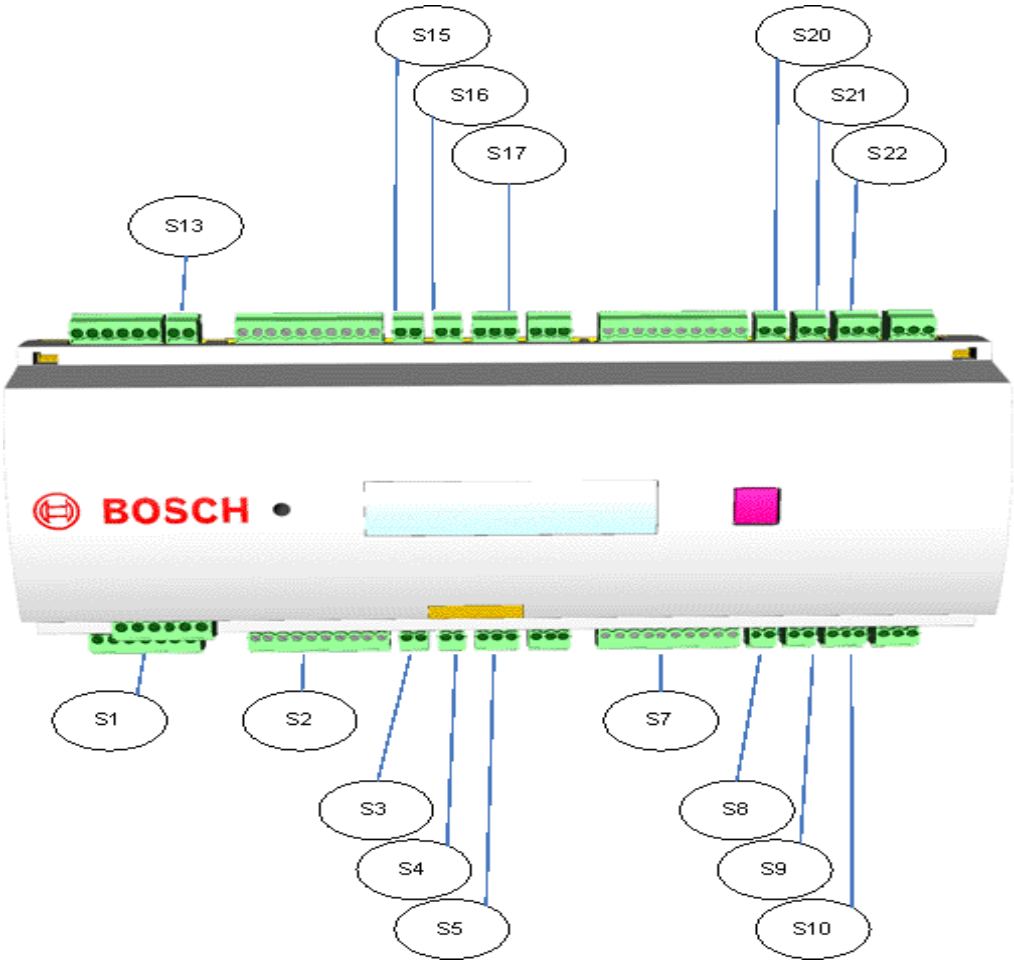


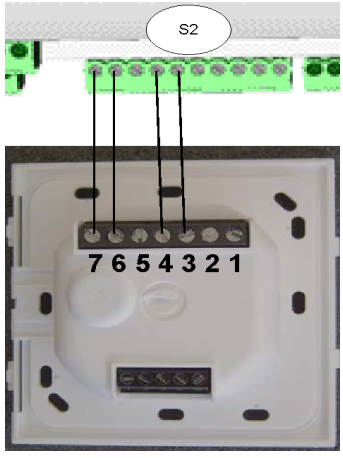
Figure 3.5 The AMC2 connections used in the 4-room surgery example.

Connector	used for...		Connector	used for...
S1 PSU	Power input		S10 Output 3	Storeroom Opener
S2 Reader port 1	Main Ent. and Lab card readers		S13 Tamper contact	(to be shorted as not in use)
S3 Input 1	Main Ent. REX		S15 Input 5	Lab. REX
S4 Input 2	Main Ent. MC		S16 Input 6	Lab. MC
S5 Output 1	Main Ent. Opener		S17 Output 5	Lab. Opener
S7 Reader port 2	Store and Office card readers		S20 Input 7	Office REX
S8 Input 3	Storeroom REX		S21 Input 8	Office MC
S9 Input 4	Storeroom MC		S22 Output 7	Office Opener

CAUTION!

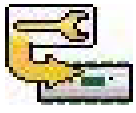
Verify that the voltage specified for your chosen reader and peripheral components corresponds to the voltage delivered by the power supply. If not then adjust the power supply output voltage, see *Section 3.5.1 Preparatory steps on PBC-60 power supply, AMC2 and computer, page 13*

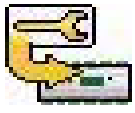
Otherwise you risk damaging both the AMC and the connected components.

Step no.	Where	Step description	Illustrations / Reference
1	AMC:S1	Connect the power supply to S1	
2	All readers	The factory default bus address of readers is usually 1. In order to distinguish between readers on the same bus, each requires a unique address. To do this open each of the readers and set the DIP switch (or equivalent, according to the reader's own documentation) for each of the 4 readers. It is now crucial that we set the reader addresses exactly as we will define them in the software, namely: Main Entrance=1, Lab=2, Storeroom=3, Office=4. see *Section 3.5.3 Setting up the connection between AMC2 and the software, page 17* **Tip**: Write the address settings on the outside of the readers, so that you do not mix them up later!	DIP (DIL) switches inside a DELTA 1000 reader 
3	AMC:S2 and both readers	Connect the reader with address 1 (Main entrance) to the pluggable screw terminal for connection S2 as per the installation instructions for the chosen reader. For instance, for the Bosch DELTA 1000 proximity reader connect the power wires to connectors 7(+) and 6(Ground) and the data wires to connectors 4(Data "A") and 5 (Data "B"). As the data signal is generated only by the voltage **difference** between these wires, their order is unimportant. To connect the reader with address 2 (Laboratory) into this configuration (i.e. into the RS-485 bus) simply extend the wiring from pin 7 of the first reader to pin 7 of the next, and so on.	Back of a DELTA 1000 reader and S2 connector of the AMC2 
4	AMC:S3	Connect the REX unit to S3. In our example we use a DS150 PIR (passive infrared) motion detector. As this is the main entrance the customer may prefer instead to connect a simple push button here, to be operated by the receptionist from her desk.	Documentation included with the REX unit.
5	AMC:S4	Connect the MC (magnetic contact) unit to S4. Note: in this example we use only the power wires. Any tamper detection wires can be left unconnected.	Documentation included with the MC unit.
6	AMC:S5	Connect the door opener to the relay output S5. IMPORTANT: Make sure a protective diode is included in parallel, see *Section 3.4 Connecting the peripheral components to the wiring, page 11*	Documentation included with the door opener unit.
7	AMC:S7	Connect S7 (the second RS-485 reader connector) analogously to S2 above. Use the readers whose addresses you set to 3 (Storeroom) and 4 (Office) above.	

Step no.	Where	Step description	Illustrations / Reference
8	AMC:S8, S15, S20	Connect the REX units for the Storeroom (S8), Lab(S15) and Office (S20) analogously to S3. REX by motion detector is useful but push buttons are very common for cost reasons.	
9	AMC:S9, S16, S21	Connect the MC units for the Storeroom (S9), Lab(S16) and Office (S21) analogously to S4.	
10	AMCS10, S17, S22	Connect the door openers for the Storeroom (S10), Lab(S17) and Office (S22) analogously to S5.	

3.5.3 Setting up the connection between AMC2 and the software

Step no.	Where	Step description	Illustrations / Reference
1	AMC and Computer	Using a crossover cable (aka “null modem”) connect the AMC’s ethernet port to an ethernet port on the computer.	AMC2-4R4 installation guide “Ethernet interface”
2	Computer	Run the Access PE application AmcIPConfig to scan the network for AMC devices and find the AMC which we have connected. In AmcIPConfig assign an unused IP address to the AMC and make a note of this address. The address chosen should be in the same range as that of the Access PE workstation.	Access Professional Edition - Configurator: “Controllers”
3	Computer	Define the AMC/LAC in Access PE. In our example we use an Ethernet connection, so enter Protocol UDP, Address 1 and Remote IP Address as defined in the previous step.	Access Professional Edition - Configurator: “Controllers: defining and modifying new controllers”
4	Computer	In the Access PE main window click the “download settings” button to download the latest firmware from Access PE to the AMC device (here generically known as a LAC or “Local Access Controller”)	 (The download settings button)
5	Computer	For the Main entrance define a **Time Model** for public visiting hours between 9:00 and 16:00.	Access Professional Edition - Configurator: “Time models > Create and modify”
6	Computer	Use the Access PE configurator application to configure all 4 of the doors described above. Each door in our example will be of door model 01b and will require: – A reader of type RS-485 with an address of 1-4. E.g. Main Entrance=1, Lab=2, Storeroom=3, Office=4. – Two analog inputs, one for the REX and one for the magnetic contact. – One relay output to the door opener.	Access Professional Edition - Configurator: “Entrances” and “Signals”
7	Computer	Set the Main Entrance to be dependent on the time model defined above, and for this to come into effect upon first use of the door.	Access Professional Edition - Configurator: “Entrances”

Step no.	Where	Step description	Illustrations / Reference
8	Computer	Assign authorization groups to the individual doors, e.g: – All_Staff (for Main entrance and Storeroom) – Doctor_And_Technician (for Laboratory) – Doctor_And_Receptionist (for Office)	Access Professional Edition - Configurator: “Access Authorizations”
9	Computer	Create the users of the access control system in Access PE, e.g. Doctor, Receptionist, Lab technician. Assign the appropriate authorization groups to each user, i.e: – Receptionist: All_Staff and Doctor_And_Receptionist. – Technician: All_Staff and Doctor_And_Technician. – Doctor: <all three authorization groups>	Access Professional Edition - Personnel Management: “User rights”
10	Computer	Assign the numbers of the credentials (card, token or key fob) to the personnel records of their respective users.	Access Professional Edition - Personnel Management: “User rights”
11	Computer	Click the “download settings” button (see Step 3 above) to update the AMC with the changes.	

4 Installation with Wiegand and Access Easy Controller (AEC)

This chapter describes the installation of our example access control system using **Wiegand communication to the readers. AEC is an access control system that uses Wiegand communication.** We will assume that all the components decided upon in *Section 2.2 Low tier: Electrical components, page 6* have been ordered from and delivered by the hardware vendor of your choice. The installation is basically a 6 stage process:

1. Mounting the access controller, see *4.1*
2. Installing the wiring, see *4.2*
3. Mounting the peripheral components, see *4.3*
4. Connecting the peripheral components to the wiring and AEC, see *4.4* to *4.5.1*
5. Configuring the AEC hardware and network, see *4.5.2*
6. Configuring the AEC software, see *4.5.3*

4.1 Mounting the access controller

The obvious room in which to locate the access controller and power supply is the **office**. In it the hardware will be protected from unauthorized access. The office is also situated centrally with regard to the doors. The enclosure should contain a battery to provide an uninterruptible power supply (UPS).
The backup battery is optional and is not provided with the standard package.

4.2 Installing the wiring

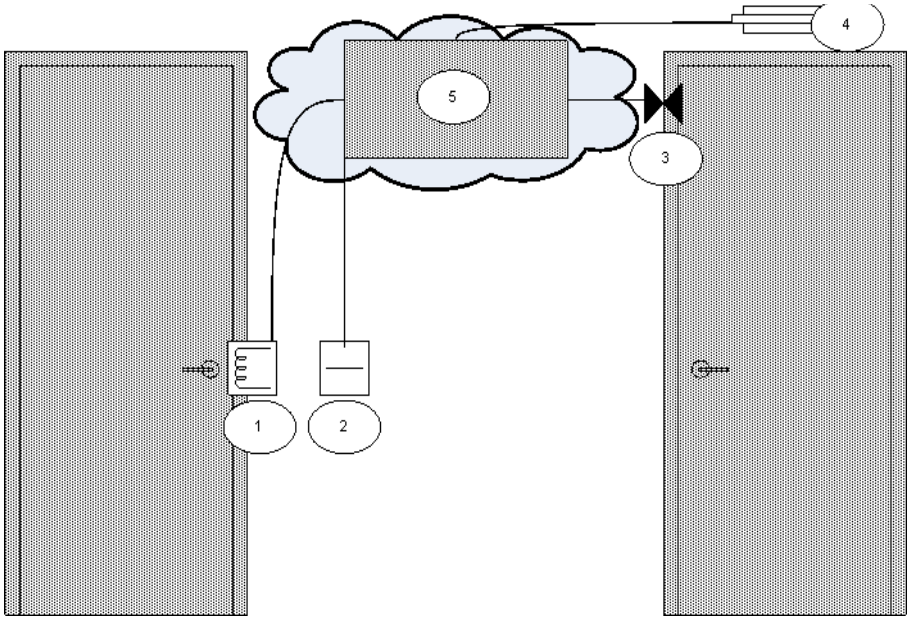
Lay the cables decided upon in *Section 2.2.3 Wiring for non-reader components, page 8* from the office to the respective doors. Aesthetically it is always preferable to hide cabling beneath floors, above ceilings or underneath wall plaster, but this is not always practical. Note - junction boxes are commonly used near doors; we leave them out of this example only for the sake of simplicity.
Make sure that cables carrying data (e.g. from the reader) are shielded, see *4.4.2*
Make sure that there is enough length to reach both components above the door (e.g. REX with motion detector, magnetic contacts) and components at handle height (e.g. reader, door opener).

4.2.1 Wiegand star topology for readers

Readers in a wiegand environment are connected in a star topology, i.e. a reader is connected directly to the controller. See *Section 2.2.1 Card reader technologies, page 7*.
With readers it is very important to follow the manufacturer's instructions as regards grounding (earthing) the device and its cable shielding.

4.3 Mounting the peripheral components

Electrical components must always be mounted (i.e. attached to walls, racks, doors and door-frames) as per the manufacturer's instructions.
The following illustration shows typical locations of electrical components with respect to a door. Note that the access controller (5) should always be in a secured area to prevent tampering.



Door from the outside	**Same door from the inside**
1: Door opener - 2 wires	3: Magnetic contact - 2 wires
2: Reader - 4 wires	4: REX with motion detector - 2 wires
5: Access controller. **NOTE: This should not be near the doors themselves, but should always be located in a secured area** (here represented by the cloud).	

4.4 Connecting the peripheral components to the wiring

Electrical components must always be connected as per the manufacturer's instructions. Nevertheless there are certain basic rules and pitfalls which should be well understood by every installer of access control devices. Please read the following sections carefully:

4.4.1 Protective diodes

A door opener typically locks or unlocks a door by means of a magnet which is subjected to an electric current. When this current is switched off a high voltage is induced in the magnetic coil, which needs to be dissipated to prevent damage to other components. This is generally done by means of a protective diode.

CAUTION!

If the door opener (or other magnetic component, e.g. a door holding magnet) does not have an inbuilt protective diode, be sure to connect such a diode electrically in parallel with it. See illustration below. *Section Figure 4.2 Position of the protective diode, page 21*. Install protective diodes wherever excess voltage can be induced by magnetic fields.

Figure 4.1 A diode

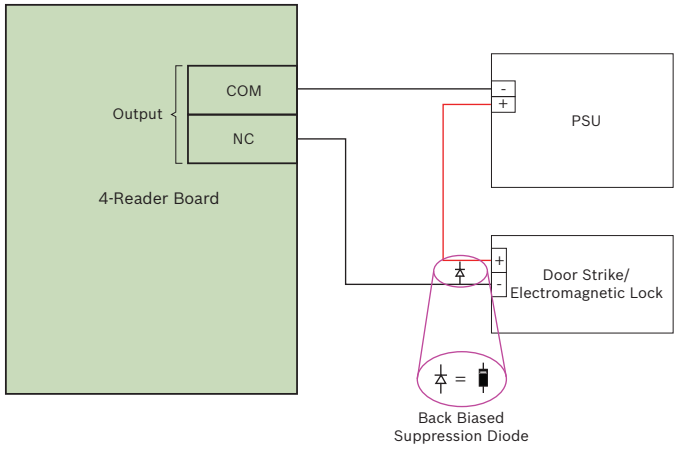


Figure 4.2 Position of the protective diode

4.4.2 Shielding data cables and avoiding ground loops

Cables with cores that carry data have a conducting wrapper, accompanied by a naked grounding wire, between the cores and the outer plastic casing. When the naked wire is grounded properly this wrapper “shields” the cores from electrical interference. Without shielding, the integrity of the data signals is threatened.

A common installation error (particularly in cases where the reader-end and the controller-end of the cable are handled by different persons) is to ground the shielding at **both ends**. If the two grounds are not of identical potential, there is a possibility of current flow through the shielding, which can disrupt the signals in unpredictable ways, cause malfunctions in the access control hardware and even masquerade as software errors. This phenomenon is known as a **ground loop**.

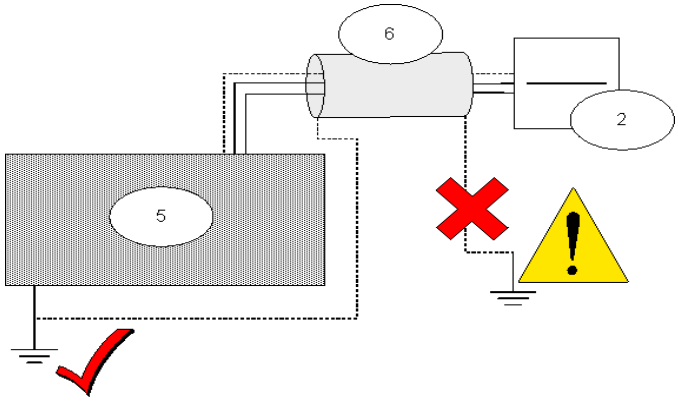


Figure 4.3 Avoiding a ground loop

5: Access controller	6: Shielding around cable	2: Reader

CAUTION!
To avoid ground loops, be sure to ground cable shields only ONCE.

CAUTION!
Follow carefully the grounding instructions for the reader and other sensitive components. Failure to ground components correctly can result in damage to those components and to malfunction of the access control hardware, which can masquerade as a software error.

4.5 Connecting the AEC (Access Easy Controller)

The following is an illustration of an AEC2.1 unit

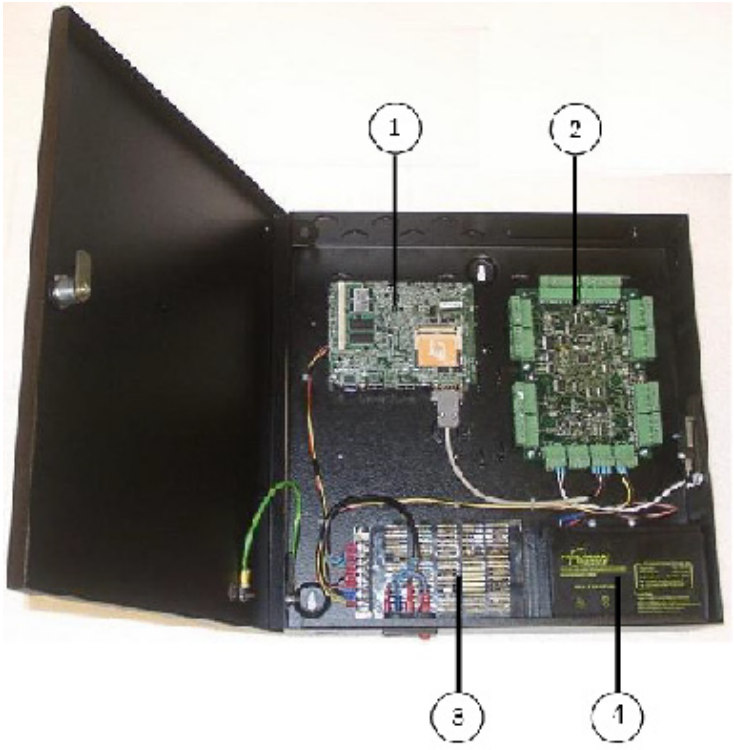


Figure 4.4 An AEC2.1 access controller

1: CPU Board	2: 4 Reader Board	3: Power Supply Unit	4: Backup Battery
Note: AEC2.1 does not come with the 12 VDC standby battery.			

Space restrictions do not permit a detailed treatment of the AEC2.1 controller hardware, of which there are several variants. Always consult the hardware manual of the controller you are using. The relevant hardware manual, along with all the other documentation referenced below, is available in PDF format from the Bosch Security Systems internet site, see *Section 5 Resources and further reading, page 27*.

As we only need to control 4 doors, one AEC2.1 device will be sufficient. For connection to the access control software we will use an ethernet crossover cable aka “null modem” (alternatively you could use normal ethernet cables and place a hub or a “switch” between computer and access controller). For the power supply we will use the standard power cable (100~240 VAC) which also charges the UPS backup battery.

4.5.1 Connecting the peripheral components to the AEC

The AEC2.1 possesses connectors of the pluggable screw terminal type. Wires can be fastened with holding screws to the terminals, and these terminals can be plugged and unplugged at the AEC2.1.

We will connect 4 readers (Main entrance, Laboratory, Storeroom and Office) in a star topology i.e. all the readers are connected to the controller.

Figure 4.5 below shows an example with one door connected to the controller.

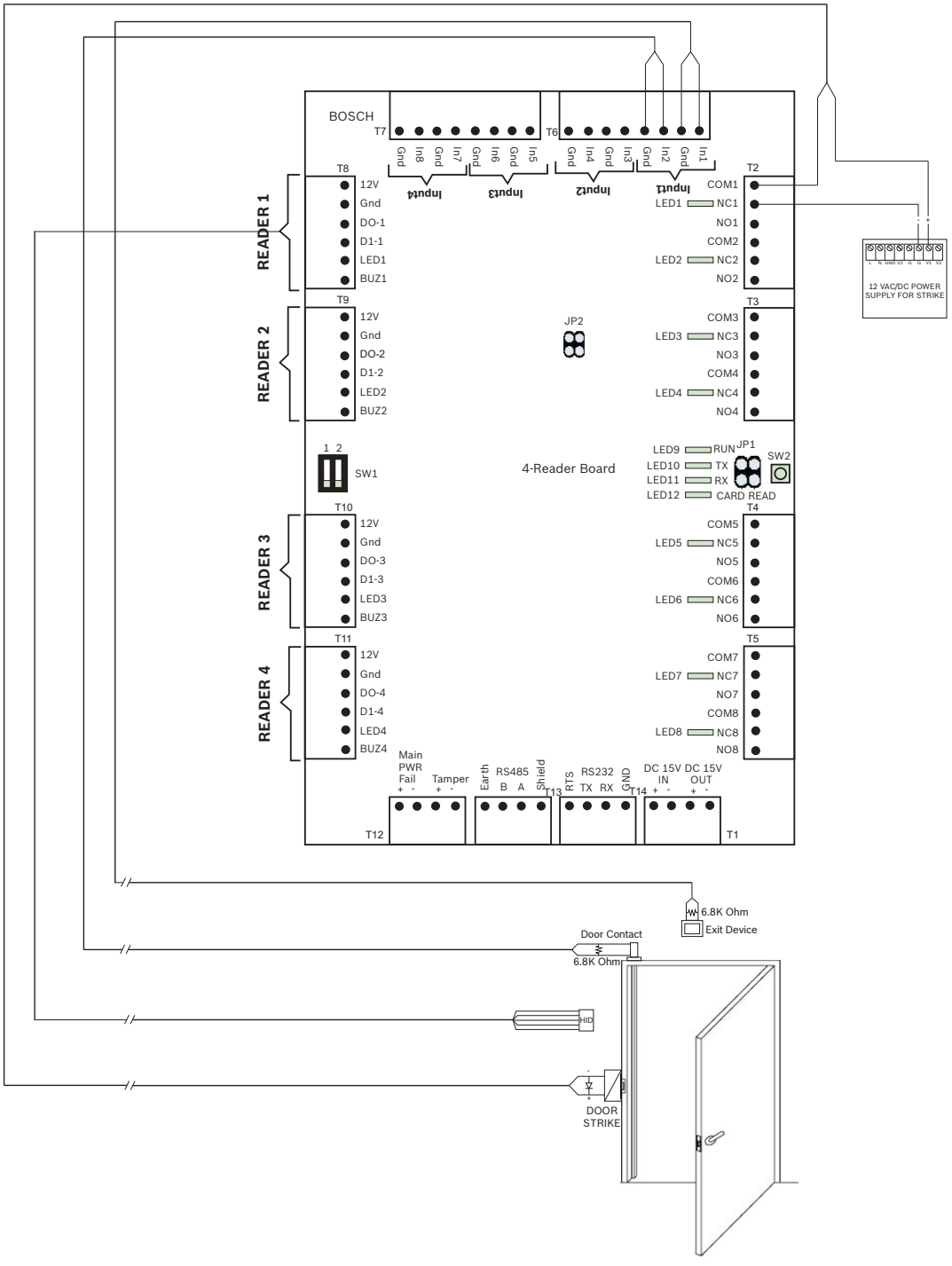


Figure 4.5 The AEC2.1 connections showing one of the door connections.

CAUTION!

Verify that the voltage specified for your chosen reader and peripheral components corresponds to the voltage delivered by the power supply. If not then adjust the power supply output voltage.

Otherwise you risk damaging both the AEC and the connected components.

Step no.	Where	Step description	Illustrations / Reference
1	AEC2.1	Connect the power supply to the power cord in the controller.	
2	AEC2.1	Connect the Main Entrance reader to the pluggable screw terminal Reader1 for connection. Connect the Laboratory reader to the pluggable screw terminal Reader2 for connection. Connect the Storeroom reader to the pluggable screw terminal Reader3 for connection. Connect the Office reader to the pluggable screw terminal Reader4 for connection.	
3	AEC2.1	Connect the REX unit to the terminal **In1** and **Gnd** in **Input1** point. In our example we use a motion detector. As this is the main entrance the customer may prefer instead to connect a simple push button here, to be operated by the receptionist from her desk. IMPORTANT: Install 6.8K ohm end-of-line resistors at each device. The resistor should be wired in parallel (across) normally open devices and in series with normally closed devices.	Documentation included with the REX unit.
4	AEC2.1	Connect the MC (magnetic contact) unit to the terminal **In2** and **Gnd** in Input1 point. Any tamper detection wires can be left unconnected. IMPORTANT: Install 6.8K ohm end-of-line resistors at each devices. The resistor should be wired in parallel (across) normally open devices and in series with normally closed devices.	Documentation included with the MC unit.
5	AEC2.1	Connect the door opener to the relay output **COM1** and **NC1** in **T2**. NOTE: Door openers typically require their own power supplies, in which case the AEC connection must be in “dry mode”, i.e. providing no voltage. IMPORTANT: Make sure a protective diode is included in parallel, see *Section 4.4 Connecting the peripheral components to the wiring, page 20*.	Documentation included with the door opener unit.
6	AEC2.1	Connect an external battery to provide power for the door opener.	
7	AEC2.1	Connect the Laboratory, Storeroom and Office readers as above.	
8	AEC2.1	Connect the REX units for the Storeroom (**In3** and **Gnd** in **Input2** terminal), Lab (**In5** and **Gnd** in **Input3** terminal) and Office (**In7** and **Gnd** in **Input4** terminal). REX by motion detector is useful but push buttons are very common for cost reasons.	

Step no.	Where	Step description	Illustrations / Reference
9	AEC2.1	Connect the MC units for the Storeroom (**In4** and **Gnd** in **Input2** terminal), Lab (**In6** and **Gnd** in **Input3** terminal) and Office (**In8** and **Gnd** in **Input4** terminal).	
10	AEC2.1	Connect the door openers for the Storeroom (**COM3** and **NC3** in **T3**), Lab (**COM5** and **NC5** in **T4**) and Office (**COM7** and **NC7** in **T5**).	

4.5.2 Configuring the AEC hardware and network

Step no.	Where	Step description	Illustrations / Reference
1	Power cable	Connect the power cable (100~240 VAC) to the AEC2.1 power socket, but do not switch on the power.	
2	AEC2.1	Unlock the enclosure door with the keys provided. Open the enclosure to gain access to the internal CPU, 4 reader board and PSU.	AEC2.1 Hardware Manual
3	AEC2.1	Check all circuit board mounting screws for snugness. Verify that socket mounted components are secure. Verify jumper and switch settings of all boards.	AEC2.1 Hardware Manual
4	CPU	Insert Compact Flash onto the AEC2.1 CPU.	AEC2.1 Hardware Manual
5	CPU	Connect an ethernet crossover cable from the computer to the AEC2.1 CPU network port.	AEC2.1 Hardware Manual
6	Computer	Connect a computer running the Windows operating system to the AEC using the crossover network cable. Configure the computer's IP address on the same 192.168.0 network as the default IP address of the controller (192.168.0.41).	
7	AEC2.1	Power up the controller at this time. The CPU board will perform a power-up self-test. This test takes about 90 seconds to complete. The system will take approximately 7 mins to 10 mins to launch the back end programs when the system is booted up for the first time.	
8	Computer	Open a Web browser application (Internet Explorer 7.0 and above) and enter the controller's IP address. The factory default IP address is **192.168.0.41**.	
9	Computer	Login to AEC2.1 using the user name “**user1**” and password “**8088**”. Select the desired language for the software interface from the dropdown list. Click the Login button.	AEC2.1 Software Manual
10	Computer	From the home page, select **System** > **Network Settings**. Modify the Controller's IP Address, Subnet mask, and Gateway to fit into the customer's network configuration.	AEC2.1 Software Manual
11	Computer	From the home page, select **System** > **Advance Settings** > **System Maintenance** > **Reboot** to reboot the controller. After rebooting, the controller will begin responding to its new address.	

4.5.3 Configuring the AEC software

Step no.	Where	Step description	Illustrations / Reference
1	AEC and Computer	Use a normal network cable to connect the AEC's ethernet port to an ethernet port in the network hub.	AEC2.1 Hardware Manual and AEC2.1 Software Manual
2	Computer	Open a Web browser application (Internet Explorer 7.0 and later) and enter the controller's default IP address **192.168.0.41**. If you have changed the IP address enter the new IP address.	AEC2.1 Hardware Manual and AEC2.1 Software Manual.
3	Computer	From the main page select **Configuration** > **Device** > **Door**. Edit the description of the existing door configuration as Main_Entrance, Lab, Storeroom and Office.	AEC2.1 Software Manual
4	Computer	For the Main entrance define a **Schedule** for public visiting hours between 9:00 and 16:00.	AEC2.1 Software Interface: Configuration > Schedules
5	Computer	Assign the above defined schedule to the Main Entrance and set the schedule to unlock the door.	AEC2.1 Software Interface - Configurator: Configuration > Device > Door > Scheduling Options
6	Computer	Assign Access groups to the individual doors, e.g: – All_Staff (for Main entrance and Storeroom) – Doctor (for Office and Laboratory) – Receptionist (for Office) – Technician (for Laboratory)	AEC2.1 Software Interface - Configurator: Card > Access Groups
7	Computer	Create the users e.g. Doctor, Receptionist, Lab Technician and assign individual card numbers to access the doors. Assign the appropriate access groups to each user, i.e: – Receptionist: All_Staff and Receptionist. – Technician: All_Staff and Technician. – Doctor: All Staff and Doctor	AEC2.1 Software Interface - Configurator: Card > Card Administration

5 Resources and further reading

Links to literature, websites etc.

Document	Location / Link
Bosch Security Systems: Product information	http://products.boschsecuritysystems.eu/en/
Bosch Access Control Products: Information and downloadable documentation:	http://products.boschsecuritysystems.eu/en/EMEA/products/bxp/CATM5addb76fb1a3ee8977d108b6d43d16f5
AMC2 4R4 Installation Guide	http://resource.boschsecurity.com/documents/AMC2-AccessModu_InstallationGuide_AMC24R4_enUS_T4443037323.pdf
Miscellaneous AMC2 hardware and extensions	http://products.boschsecuritysystems.eu/en/EMEA/products/bxp/CATM23980e086f5b3df3a8cbc6c804a471bb
Access Professional Edition V2.0	http://products.boschsecuritysystems.eu/en/EMEA/products/bxp/SKUPFT6355205515.P1.F.01U.127.354-CATM8d3152ce9e0ab66b2810c85db614c882
AEC2.1 Hardware Manual	http://products.boschsecuritysystems.eu/en/EMEA/products/bxp/CATM5addb76fb1a3ee8977d108b6d43d16f5
AEC2.1 Software Manual	http://products.boschsecuritysystems.eu/en/EMEA/products/bxp/CATM5addb76fb1a3ee8977d108b6d43d16f5
AEC2.1 Utilities Manual	http://resource.boschsecurity.com/documents/AccessEasyContr_InstructionBook_UtilitiesProgrammManual_enUS_T6385916427.pdf

Glossary

A

Access control	Protecting resources from misuse by unauthorized persons whilst facilitating their legitimate use by authorized persons.
Access PE	Access Professional Edition - access control software sold by Bosch Security Systems for mid-range access control installations.
AEC	Access Easy Controller - an access controller sold by Bosch Security Systems with a browser based user interface for small to mid-range access control installations.
Alarm	An event that draws attention to a situation requiring human intervention. An alarm can trigger further events such as live video, video playback, the display of action plans/maps etc.
AMC2	Access Modular Controller - an access controller module (HW + firmware) sold by Bosch Security Systems for any size of access control installations.

C

Credentials	Objects carried by an individual person in order to identify that person to access control systems or to other persons. Typical forms of credentials are cards and key fobs.

D

DIL or DIP switch	A bank of small binary switches used for configuring hardware at installation time, but not involved in user interaction.
Door model	One of a set of standard door configurations defined in the access control software. Using door models accelerates the software configuration process.

G

Ground loop	Unwanted electrical current through a conductor caused by its being grounded at more than one point, with these points having different electric potentials.

J

Jumper	A small component used to connect two pins thus making a binary switch. Like DIL switches jumpers are used for configuring hardware at installation time but are not involved in user interaction.

L

LAC	Local Access Controller. A generic term for access controllers, found in the Access PE GUI and documentation. The AMC2 is a kind of LAC.

M

MC	Magnetic contact. A component which detects whether a door is open or not. In combination with other components it can be used to raise an alarm if the door is forced open.

Mode wet/dry	An AMC connection is in “wet mode” when the AMC provides a voltage to the peripheral device via that connection. “Dry mode” is the opposite, i.e. no voltage is provided via the connection. The mode is determined by a jumper setting inside the AMC unit. It is important that devices with their own power supplies be connected only in dry mode.

P

Protective diode	A small component wired in parallel with a magnetic component in order to dissipate any harmful excess voltage induced by powering off the magnet.

R

REX	A Request to EXit device. An electronic device, typically a push button or a motion detector, which signals the need to unlock a door to allow exit.
RS-485	A digital communications standard which is especially effective over long distances and in electrically “noisy” environments. Here it is an alternative communication medium to Wiegand for connecting readers to access controlers. RS-485 uses a bus topology and has a longer range than Wiegand.

T

Tier	An access control system can be considered as consisting of three tiers: the electrical components (low tier), the access controllers (middle tier) and the software host system (high tier).
Time model	A structure of hours of the day which is defined by administrators as a named entity in an access control system. System administrators can control, for instance, the opening times of a door, or the valid attendance times of a person based on such time models, thus accelerating the software configuration process.

W

Wiegand	The Wiegand interface is a common wiring standard for card readers

Index

Bosch Security Systems
Robert-Koch-Straße 100
D-85521 Ottobrunn
Germany
Telefon 089 6290-0
Fax 089 6290-1020
www.boschsecurity.com