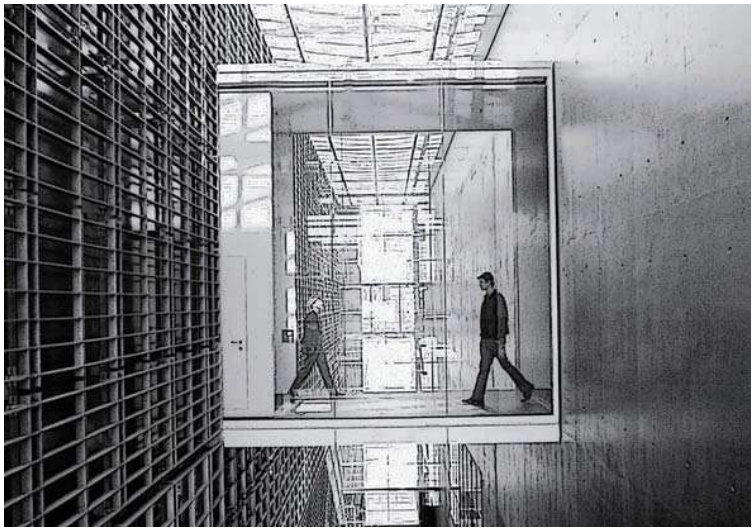
SIEMENS



Access Control

Granta to SiPass Migration Guide

Siemens AB

Security Products

Contents

1 Summary

SiPass Integrated, MP2.6 SP1 Supports the Granta Hardware providing a possible upgrade path from Granta to SiPass Integrated. The purpose of this document is to highlight the differences between Granta and SiPass and provide basic setup instruction for the most common Granta configurations.

Please see section 3 “Upgrading MKIII to ACC firmware” for migration steps.

2 Configuring Granta Devices

SiPass Integrated, MP2.6 SP1 provides support for the configuration of Granta devices through the FLN Configurator. Granta specific features for SiPass Integrated are:

:

- Mapping the plug in modules expansion bus to FLN 4.
- Mapping the plug in module handler (backboard) to device 11
- Searching the Granta FLN Bus 4 for plug in modules.
- Saving the plug in modules to the database.
- Downloading firmware upgrades to the Backboard on the Granta bus.
- Configuring Monitored/Unmonitored inputs.
- Configuring Reader Technology on the Cotag and Swipe modules.
- Configuring Parity Check & Enhanced Read for Cotag read heads
- Configuring Repeat Transaction Delay and Hold off time for Cotag readers.

NOTE: The Granta system will need to remain online while configuring the devices in the FLN Configuration dialog, in order to read and set the values.

2.1 Expansion bus and Modules

The plug-in expansion bus is mapped to FLN 4 in SiPass Integrated.

Plug in modules are mapped to odd numbers, starting from 1, and step up in increments of 2. i.e. 1, 3, 5, 7, 9 are the valid addresses of plug-in modules on the Granta Expansion bus. Even numbers are not allowed.

NOTE: In Granta, a single plug-in module was considered to be 2 devices on an even and odd address. This no longer applies – all plug-in modules are treated as a single device. E.g. a Cotag module occupying slot 0 and 1 would appear in SiPass as a 2 reader device on address 1.

The FLN Configurator allows the Expansion bus to be searched, showing what devices are present. Each discovered device can be saved, after assigning a unique name.

The Backboard device is on address 11. The Backboard device manages all the plug-in modules, as well as the Cotag card reading process. The firmware on the backboard device can be upgraded by right clicking on the backboard device and selecting “Flash with Latest Firmware”, “Flash with Embedded Firmware”, “Flash with Selected Firmware” or “Flash with Specific Firmware”.

2.2 Supported Card Formats

The following Cotag card formats are supported by SiPass:

- Format 0 – 16 bit card, 16 bit facility.
- Format 1 – 24 bit card, 16 bit facility.
- Format 2 – 30 bit card, 16 bit facility.
- Format 3 – 31 bit card, 16 bit facility.
- Format 4 – 48 bit card, no facility.

The following Wiegand card formats are supported by SiPass:

- 300 – 26 bit HID Prox format – 16 bit card, 8 bit facility, 2 bits of parity.
- 301 – 32 bits of data – 16 bit card, 16 bit facility.
- 302 – 34 bits of data – 16 bit card, 16 bit facility, 2 bits of parity.
- 303 – 48 bits of data – Cotag format 3 over wiegand.
- 304 – 34 bits of data in CardKey format.
- 305 – 48 bits of data – Cotag format 4 over wiegand.

The following SiPass specific card formats are also available:

- CSN32 – 32 bits of data – 32 bit card number.
- CSN40 – 40 bits of data – as above but with an 8 bit checksum.
- ASCO 36 bit – legacy ASCO specific card.
- Proximity Corporate 1000 – legacy HID Prox format, 35 bits total.
- SALTO Wiegand – 34 bit or 58 bits of data, with either a 32 bit of 56 bit card.
- Custom Wiegand – user configurable format. Set the reader to Raw Card (Wiegand) to be able to use the Custom Card dialogue in the FLN Configurator.

The following Magstripe formats are supported by SiPass:

- Granta formats 350 to 361.
- The following SiPass specific formats are also available:
- Siemens Reader Clk/Data – 10 to 16 digits of card number.
- Siemens Reader Clk/Data Extended – up to 21 digits of card number.
- Magstripe Credit – last 5 digits of a credit card.
- Magstripe Encrypted – legacy ASCO format.
- Magstripe Facility – 12 digits total length, 5 digit card, 6 digit facility.
- Magstripe 37.
- Argina Clk/Data – legacy format.

NOTE: - SiPass does not support the Issue number on cards (Revision Number in SiPass)
- SiPass does not support bit swapping.

2.3 Monitored/Unmonitored inputs

A Radio Button Selection in the FLN Configurator dialogue for the Swipe, Cotag and IO modules allows the choice of Monitored or Unmonitored inputs.

This selection sets the characteristics for **all** inputs. This means that it is not possible to have some inputs unmonitored and some monitored on the same board.

Perform the following steps to set the input to Monitored or Unmonitored:

1. Click on the **System** Menu and choose **FLN Configuration**. The *FLN Configuration Dialogue* will appear.
2. Select the Swipe, Cotag or IO module from the device tree and Click on the "Configuration" tab.
3. Click **Monitored** or **Unmonitored** in the Inputs radio button selection.

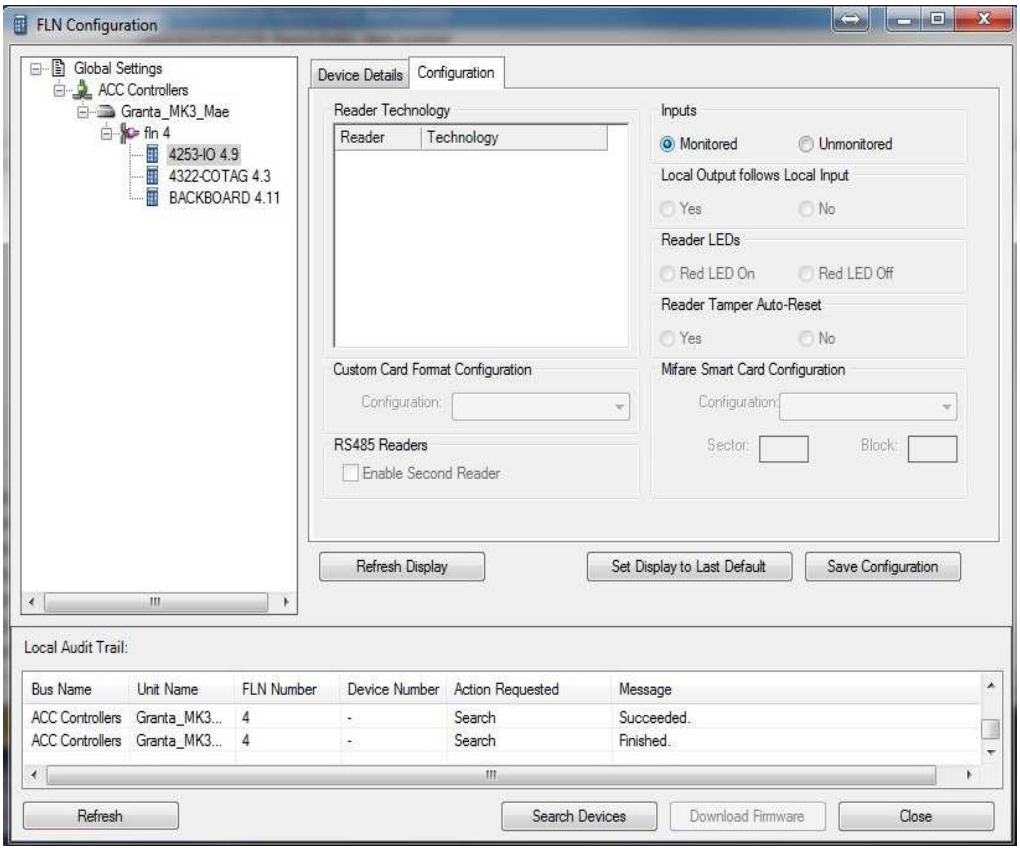


Fig.1. FLN Configuration - IO, Swipe and Cotag

4. Click **Save Configuration**.

The inputs can be wired to be either monitored or unmonitored; the setting only changes the reporting of the inputs. For example: an input with monitoring resistors is set to unmonitored – the firmware will treat an open circuit Tamper as an Alarm, and short circuit Tamper as Normal.

2.4 Parity Check & Enhanced Read on Cotag Read Heads.

These settings are present on the Baseboard device on address 11, since it applies to all Cotag read heads.

A tick box enables/disables whether a parity check on Cotag cards will be performed. Cards that were not encoded with Parity will not be readable after this is enabled.

Enhanced Read, when enabled via a tick box, causes the card to be read twice before a card number is reported. This ensures reliable reading in high noise environments.

Perform the following steps to set the Parity check and/or the Enhanced Read on the Backboard Device in the FLN Configuration:

1. Click on the **System** Menu and choose **FLN Configuration**. The *FLN Configuration Dialogue* will appear.
2. Select the Backboard module from the device tree and Click on the “Configuration” tab.
3. Click the **Enhanced Read** and/or the **Parity Check (DPIC)** Tick Box.

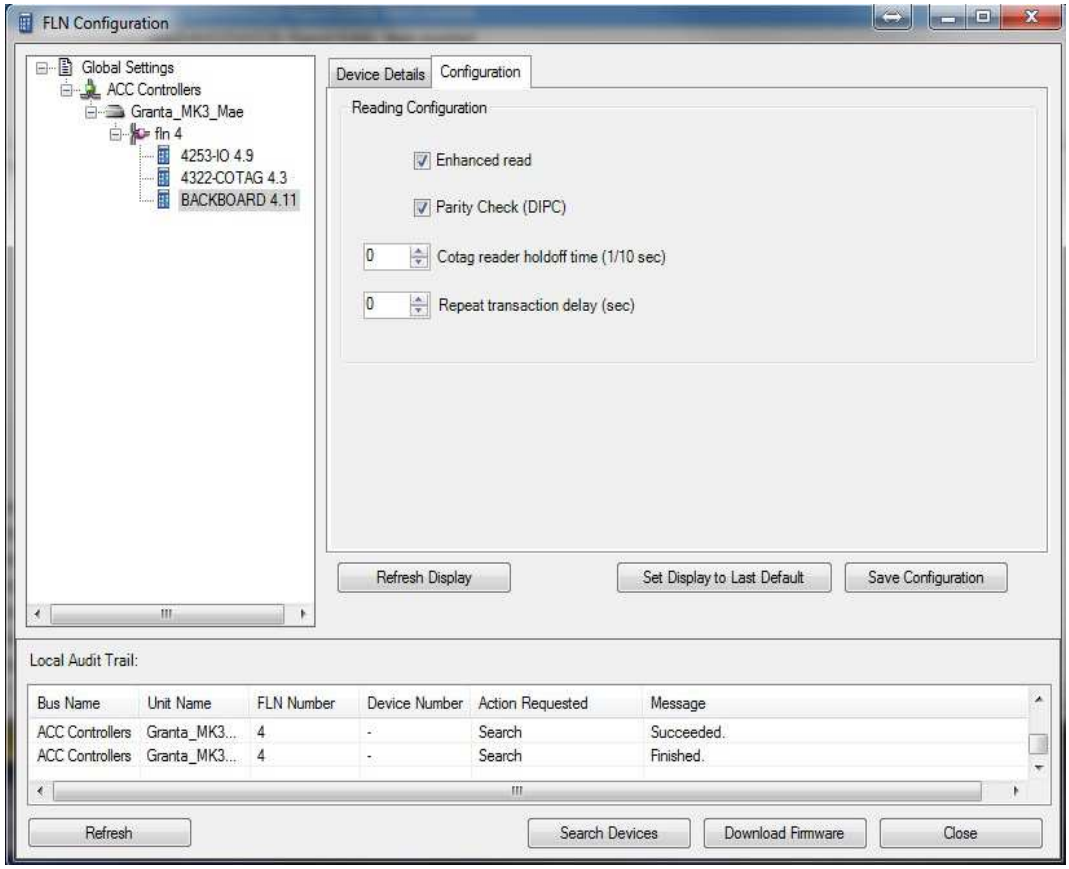


Fig.2. FLN Configuration – Backboard Device

4. Click **Save Configuration**.

2.5 Hold off Time for Cotag Read Heads

These settings are present on the Baseboard device on address 11, since it applies to all Cotag read heads.

Hold Off time, also known as Aerial hold off time, prevents the Cotag read head from reading again for the allotted time. The value range that can be set is between 0-255 and it is measured in tenths of a second (1/10 sec).

Perform the following steps to set the Hold off time:

1. Click on the **System** Menu and choose **FLN Configuration**. The *FLN Configuration Dialogue* will appear.
2. Select the Backboard module from the device tree and Click on the "Configuration" tab.
3. Enter the Hold off time into the **Cotag Reader Hold off Time** Field. *(See Fig 2 in section 2.1.4 above)*
4. Click **Save Configuration**.

2.6 Repeat Transaction Delay for Cotag Read Heads

These settings are present on the Baseboard device on address 11, since it applies to all Cotag read heads.

A Repeat Transaction Delay (in seconds) is applied to Cotag read heads. The value range that can be set is between 0 – 255. It is most useful in AntiPassBack (APB) where an IN reader may be located close to an OUT reader, and it is not desirable for a card holder to accidently trigger the OUT reader when entering a door.

Perform the following steps to set the Repeat Transaction Delay:

1. Click on the **System** Menu and choose **FLN Configuration**. The *FLN Configuration Dialogue* will appear.
2. Select the Backboard module from the device tree and Click on the "Configuration" tab.
3. Enter the delay time into the **Repeat Transaction delay** Field. *(See Fig 2 in section 2.1.4 above)*
4. Click **Save Configuration**.

2.7 Learning a Distributor Code

SiPass 2.6 SP1 incorporates support for both the learnt distributor code and the Siemens distributor code (dual distributor code).

The procedure to set the Distributor Code is as follows:

1. Power up the controller and wait around 15 seconds for the unit to be functional.
2. Place a link on Jumper on the **LEARN** link. Verify that the **CONFIG LED** is now blinking rapidly.
3. Badge the specific Cotag card to be learnt on the **RF** coils, or on any Cotag read head.

4. Verify that the **CONFIG LED** has turned solid green. If it is still blinking, wait a few seconds and try again, until the **CONFIG LED** turns solid green
5. Remove the jumper from the **LEARN** mode link.

2.8 Licensed Card Technologies

There are 2 new card technologies which are licensable in SiPass 2.6 SP1 to allow for Granta Migration. These are:

- **Siemens Granta Vendor Specific**
  This card technology is “vendor specific”, which is defined together with the learn-mode jumper and a config card.

- **Siemens Granta Generic** This applies to cards with the generic distributor code. The Siemens generic code also allows a vendor specific code to be entered as described above. This means that the Siemens generic card tech caters for customers using both vendor specific and Siemens distributor codes.

There are several scenarios when migrating a site from the original Granta system using Cotag cards to a SiPass Integrated system.

1. All cards have a non-Siemens distributor code.
The site is using cards that all have a vendor specific distributor code. In this situation the site needs a Siemens Granta Vendor Specific licence, with a facility number matching the majority of the cards on site. Extra facility numbers for cards with the same Distributor Code can be added free of charge in the Credential Profile dialogue.

2. All cards have a Siemens Distributor Code.
The site needs a Siemens Granta Generic licence with a facility number matching the majority of cards on site. Extra facility numbers for cards with the Siemens Distributor Code can be added free of charge.

3. Dual Mode: Siemens Distributor Code and a Specific Distributor Code.
The site needs a licence matching the majority population of card types – either Vendor Specific or Generic. Extra facility numbers are available free for the base licence, but there will be a charge for facilities in the other card technology.

4. Swipe modules and readers are in use.
The site is using Swipe modules, either exclusively or in addition to Cotag cards and readers. Cards badged at a Swipe module will require a Siemens Granta Generic licence, either as a base licence or as an additional Facility.

5. Adding SiPass door controllers and card readers.
The site is using swipe modules and wants to add new readers on SiPass door controllers e.g. DESfire cards and readers on a DRI. In this situation, the site needs a Granta Generic licence, with a facility matching the majority of cards on site. In addition, they need to add a Credential Profile of type Siemens Reader, for which a charge will apply. Any new DESfire cards added will have to be as additional cards to a base card technology.

3 Upgrading Granta MK3 to ACC firmware

Granta-MK3 Firmware Migration Procedure:

- Prerequisite: A name brand micro SD card of at least 32 MB in size. SanDisk and Lexar have been tested and found to be reliable. SDHC cards are not supported.

This procedure will work on the latest revision of the Granta MK3 hardware. This procedure can also work on earlier revisions, but place a jumper on X-992, and remove the jumper when complete.

1. Use the SDFormater V3.0 software to format the micro SD card.
2. Copy the supplied files to the micro SD card, and verify that the file boot.bin is in the root directory (along with other files and folders).
3. Make a note of any relevant information about the controller to be migrated, e.g. IP address, subnet mask, etc, and then power down the controller.
4. Place the micro SD card into the micro SD socket, and slide the socket shut.
5. Place a jumper on **X-992** and power up the controller. *(See Fig.3 Below for X-992 jumper location)*.

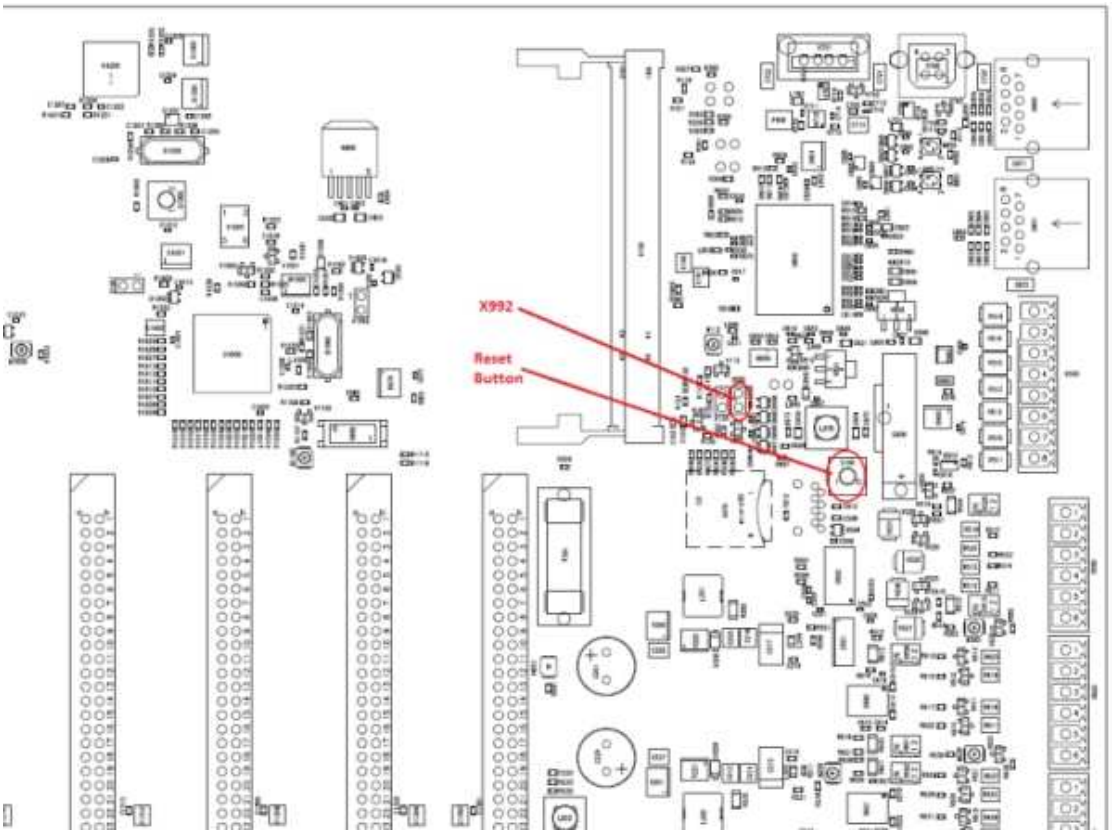


Fig.3 – Backboard Diagram.

6. Watch the **LEDs** near the FLN 1, 2 and 3 connectors.
   - The **LEDs** will begin flashing in a repeating cycle while the board is being programmed.
   - The **LEDs** will stop flashing when programming is complete.
   - Note: if the **LEDs** never start cycling, try pressing the **Reset button** once *(See Fig.3 above for Reset button location)*, and watch the **LEDs** closely.
7. Power down the board, remove jumper **X-992** and the micro SD card.

Now that the Granta-MK3 controller is running SiPass Integrated firmware, be sure to use SiPass to perform all further firmware updates.

4 Feature Comparison

The table below highlights the main differences between SiPass Integrated and Granta.

Feature	Granta	SiPass Integrated
Cards		
Card Format	Allows an individual card format to be set per reader.	Allows one card format per module (2 readers).
Bit Swapping	Bit Swapping configuration for shuffling portions of a card bit stream around.	Bit Swapping not supported.
Custom Magstripe	Custom Magstripe	Custom Magstripe not supported.
Time Schedules		
Holidays	Supports 7 different holiday sets	Supports 2 different holiday sets
Time Schedules	Granta can evaluate a time schedule.	SiPass cannot evaluate a time schedule however a time schedule can control whether a program can run.
Access Points		
Shunting	Shunting (disabling) of an arbitrary door frame contact (to cater for a dual reader door)	SiPass supports Door Sets, which binds 2 readers into a single door, so no shunting required. Unused inputs & outputs are available for other uses.
Manual Commands	Can disable Manual Commands on an Access Point.	Not supported, but SiPass can restrict access to points via Operator Privileges.
Latch time/auto relock	Allows the configuration of a fixed period of time for the door latch, or to auto relock when the door closes.	SiPass always locks the door when the door closes, unless the door frame input is disabled. **Note:** that a CBET could be programmed to temporarily disable the door frame contact, but this will add a lot of extra audit messages to the

		audit trail (which cannot be hidden).
Door Forced/Open Alarms	Can enable Door Forced and Door Open alarms separately, with a choice of Alarm or Warning.	Door Forced is always generated unless the Door Frame contact is disabled. Alarms in Si-Pass are fully configur-able
Tamper monitoring	Tamper Monitoring can be enabled/disabled on a per point basis.	Configurable only on a per module basis.
AntiPassBack	Granta allows for simple configuration of local antipassback on the access point	SiPass requires an APB area to be created.
CLIC event from PIN	Granta allows for triggering a CLIC program from a specific PIN on a specific keypad.	Not Supported.
Access Levels	Allows for merging two Access Levels together	Not Supported.
AntiPassBack		
AntiPassBack	In Granta a collection of doors is reffered to as a Zone.	In SiPass a collection of doors is reffered to as an Area.
Local AntiPassBack	Granta supports a Local mode of AntiPassBack, restricted to a single controller.	Requires a Cluster to be defined (as 1 controller) and then an area to be defined.
AntiPassBack Entry/ exit	APB is either on Entry or Exit, but not both	SiPass always checks on both entry and exit
Hard/Soft AntiPassBack		2 basic modes of APB – hard and soft. Hard APB prohibits entry or exit if there is any problem; Soft APB just generates a warning.
Other		
ASP/CLIC	CLIC is a PLC style programming interface. It is run on a periodic basis and applies PLC rules to execution.	ASP is an Event driven script language. It allows for more complex pro-grams to be constructed, with larger numbers of flags, counters and pro-grams, but care is re-quired with the sequence of programs being exe-cuted.
Intrusion	Can be partially achieved with CLIC	Intrusion (Native and External) supported.
Dual Custody		Dual Custody supported.
Door Interlocking	Can be partially achieved with CLIC	Door Interlocking supported.
Elevators	Can be achieved with CLIC on a small scale	Elevators (Low and High Level) supported

Issued by
Siemens AB

Infrastructure & Cities
Security Products
International Headquarters
Englundavägen 7
SE-171 24 Solna
Tel. +46 8 629 0300

www.siemens.com/securityproducts

Document no. A6V10366553
Edition 05.2012