

tyco

*Fire &
Security*

Siteguard Access Control Catalogue Issue 4



a vital part of your world

Introduction

Welcome to the latest edition of Tyco Fire & Security's access product catalogue specifically for Siteguard Access (SGA). This catalogue contains only Siteguard Access and is aimed at simplifying the design and promotion of a 'typical' system for this low, mid, and high-end access product.

You will find additional information including data sheets, presentation material, independent product test results and detailed technical information on our web site all of which will help enhance quotations and customer documentation.

Our goal is to despatch your Siteguard Access product, backed by our warranty and service returns policy on the same day that we receive your order. We recognise that your business is dependent on excellence in customer service and to further promote this we offer extended warranty and credit on a "No Question – No Fuss" basis for any new in-warranty product returned to the distribution centre.



For further information about Siteguard Access or any issue related to this catalogue contact our telephone Help Lines on :

Letchworth Customer Services on :-
+ 44 (0) 1462 66 77 00

TFS Technical Support Call Centre :-
Direct +31 475 352 722
Fax +31 475 352 725
Hours 09:00 - 19:00 CET
08:00 - 18:00 GMT
07:00 - 17:00 EET
UK only 08701 238 787

Toll Free: 0800 CALL TYCO or (0800 22 55 89 26)
E-Mail: TSPEuropeSupport@tycoint.com



Our web site can be found at www.tycoemea.com/English/Products/access.asp

This page is left intentionally blank

CONTENTS

Table of Contents

Chapter 01 - Siteguard Access Overview	
Introduction	5
System Connectivity RS485 via USB Converter	6
System Connectivity RS485 via Ethernet Converter	6
System Connectivity TCP/IP (eSeries)	6
Chapter 02 - Siteguard System Hardware	
SGA Site Controller	7
Intelligent Access Controller (IAC)	8
Input / Output Controller (IOC)	9
IAC Two Door Configuration	10
I/O Multiplexer	10
USB Converter	11
Ethernet Converter	11
5-Way Enclosure Cabinet	12
Basic Blade for 5-Way Enclosure	12
Blade c/w Ethernet Switch	13
5-Way Enclosure -Supporting Products	13
Galvanically Isolated Line Driver	14
Volt Free Relay Lock Interface	14
Chapter 03 - Siteguard Cards & Readers	
Indala Proximity Readers	15
Storm Vandal Resistant Keypad	17
Storm Keypad Interface	17
Grosvenor Format Wiegand Pulse Stretcher	18
Indala FlexCard Proximity Card	19
Indala FlexISO Proximity Card	20
Indala FlexKey Proximity Tag	21
Chapter 04 - Siteguard ID Card Printing	
Magicard MC200 Printer & Consumables	23
Chapter 05 - Siteguard Core Software	
SGA Core Software	25
SGA ID Badging	26
SGA Graphics	27
Chapter 06 - Siteguard Extended Software	
SGA Network / Client PC Licence	29
SGA Pictures	30
SGA Guard Tour	31
SGA Event Relay and Event Relay Plug-ins	32
SGA Vari-Time Manager - Time Zone Plug-in	33
SGA Queued Report Writer	33
SGA Kone Elevator/Lift Interface	34
SGA ThyssenKrupps Elevator/Lift Interface	34
SGA Bag Search	35
SGA Galaxy Dimension Intruder Interface	35
AnywhereUSB Hub	36
USB to Serial Adaptor	36
Chapter 07 - Siteguard Enterprise	
SGA Enterprise	37
Chapter 08 - Siteguard Access Software Support Agreement	
SSA	38
Appendix	
SGA Design Flow Chart	40
Glossary	
Glossary of Terms for Access Control	41



This page is left intentionally blank

Introduction

Siteguard Access uses modular components and distributed intelligence throughout the system from 1 door to more than 1,000, making it the most powerful and feature rich system available.



Wide Ranging

Backed by our policy of evolving with technology whilst maintaining backwards compatibility Siteguard Access is the chosen system for a wide range of industries including:

- Armed forces
- Banking and insurance
- Broadcasting
- Commercial and retail
- Defence industry
- Pharmaceutical manufacturing
- Public utilities
- State buildings
- Technology companies
- Transport
- Universities

Siteguard Access

Windows Based PC Access Control

Siteguard has long been recognised as a market leader serving entry, mid-range and enterprise solutions alike. This has only been possible because :-

- a) the Intelligent Access Controller (IAC) is powerful and flexible enough to be compatible with any IT infrastructure
- b) the suite of software components are compatible throughout the entire Siteguard portfolio

Siteguard is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server (must be 32bit versions).

Flexible and Scalable

Siteguard Access integrates with CCTV switchers, digital and network video recording, time & attendance, intruder and other critical business systems to become the 'hub' or focal point of a company's electronic security.

The basic/standard Siteguard software consists of:

- Access Control
- ID Badging
- Alarm Graphics
- Incident & Engineering Logs
- Archive and Back-Up Applications

Features

- From entry level to enterprise solutions, Siteguard supports a field-upgradeable solution for thousands of card readers, alarm monitoring points and cardholder records
- Control and manage multiple sites
- Seamless integration with other critical business systems e.g. CCTV, fire & intruder
- Serial (RS485) or IP (eSeries) connectivity
- System architecture allows workstations and controllers to be connected to the same network
- Alarm management and site graphics
- Alarm routing by time, day and system mode
- Integrated imaging and ID card production
- ODBC links to third party databases
- Unlimited expansion

Simple to Install

Unlike many access control systems Siteguard Access only uses two types of controller, the Intelligent Access Controller (IAC) and the Input / Output Controller (IOC). Each controller is manufactured with two variants for either serial (RS485) or IP connectivity (eSeries) so that any installation method or specification can be accommodated.

The simplicity of Siteguard allows any system controller to be connected to a Site Controller or main PC/server, either directly on the same LAN/WAN if using IP (eSeries controllers) or via a Comms Line Header if using serial (RS485 controllers).

Every type of intelligent controller installs into the same enclosure which includes a 12v, 2.5A PSU, 2A of which is available for locks making Siteguard a truly simple system to design and install.

Siteguard Access and JANUS Access

Siteguard Access is a leading edge access control system manufactured by Tyco Safety Products under license from Grosvenor Technology.

The design of the system and its feature set are exactly the same as Grosvenor Technology's JANUS system.

Card formats and readers are the same for both products but the controllers and software cannot be mixed because the communication protocols are different.

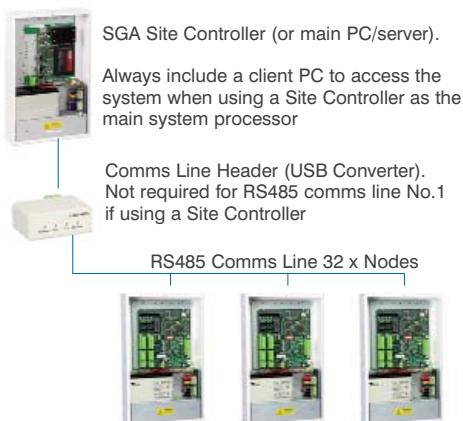
System Connectivity

Siteguard access needs a Site Controller or a main PC/server to hold the core system data which can then be shared with client PC's if they are licensed on the system.

Intelligent Access Controllers (IAC's) and Input/Output Controllers (IOC's) connect to the Site Controller or main PC/server via RS485 or ethernet and communicate system setup and alarm information around the system.

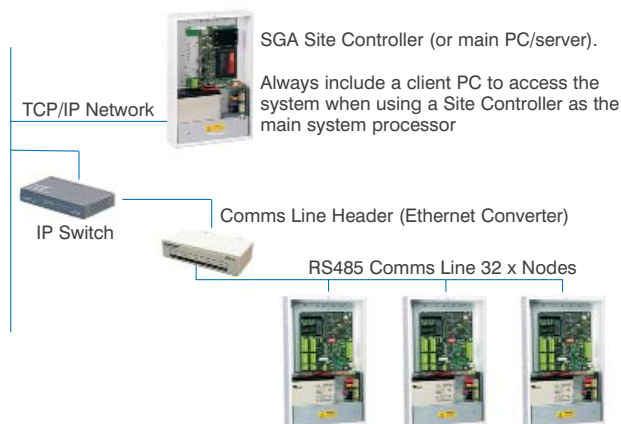
The same system can include different types of connectivity to suit the local requirement and there is no limit to the number of controllers that can be configured.

Typical examples of connectivity are shown here using a Site Controller as the main processor but this could just as easily be a PC (minimum SGA specification required).



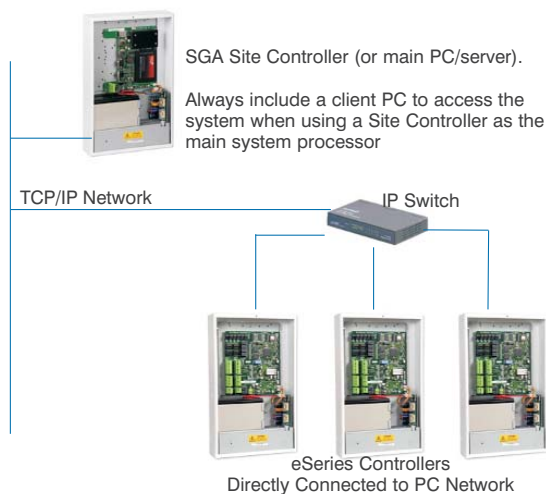
RS485 Comms Line via USB

- 32 x controller nodes per RS485 comms line
- A controller node can be an IAC or IOC (RS485)
- 1,200Mtrs max distance per comms line (measured from the USB converter to last controller node)
- 1-way USB Converter is powered from the USB port. No other PSU is required
- A USB Converter has a unique identity when connected to a Siteguard system. This allows a USB converter and its comms line to be disconnected and reconnected into a different USB port yet still retain the same comms line configuration



RS485 Comms Line via Ethernet

- 32 x controller nodes per RS485 comms line
- A controller node can be an IAC or IOC (RS485)
- 1,200Mtrs max distance per comms line (measured from the ethernet converter to last controller node)
- On ethernet converter requires a separate 12v PSU
- There is no limit to the number of comms lines that can be installed using ethernet converters
- Rijndael highly advanced data encryption (AES) can be set on the ethernet converter to protect against sabotage and malicious attack



TCP/IP Controllers (eSeries)

- eSeries controllers connect directly to the LAN/WAN via a network switch and an RJ45 patch cable
- Line headers are not required when using eSeries IAC/IOC controllers
- Significantly faster down-load times and actions across different controllers
- There is no limit to the number of eSeries boards that can be installed on the same Siteguard system
- Rijndael highly advanced data encryption (AES) can be set at each controller to protect against sabotage and malicious attack
- RS485 and eSeries controllers can be used on the same Siteguard system but not on the same comms line

SGA Site Controller



Main PC Not Required

The SGA Site Controller is a battery backed industrial grade PC that can take the place of a main SGA PC/server. The Site Controller comes pre-loaded with core software for access control, graphics and ID card production.

When using RS485 IAC and IOC controllers the initial SGA comms line connects directly onto the Site Controller board without the need for a comms line header. 1 x RS485 comms line has been included within the on-board circuitry and also includes galvanic isolation for greater reliability even in the most challenging of electrical environments.

For additional RS485 comms lines on a Site Controller, and for all RS485 comms lines when using a main PC/server, a USB or ethernet comms line header is required.

eSeries controllers do not connect directly to the Site Controller / main PC/server, they connect at any point on the same PC network via their on-board ethernet connector, thus negating the need to wire all the way back to the main PC.

Important Note:

Always include a client PC to access the system when using a Site Controller. Alternatively, a monitor, keyboard and mouse can be connected directly to the Site Controller.

Technical Specification

Dimensions (H.W.D):	420 x 265 x 77mm
Weight:	5.3kg (with Enclosure and PSU)
Operating Temp:	0°C to 50°C
Power Requirement:	230Vac, 50hz, 8W
Battery Back-Up:	1 x 12V 7Ah battery, supervised, provides operation for up to 10 hours

Features

- Intel Atom Z510 1.1GHz processor with 400MHz front side bus
- 30Gbyte serial ATA solid state flash drive
- 512Mbyte DDR2 memory
- Opto-isolated RS485 on-board comms line
- 4 x USB2 ports
- Battery backed up to 10 hours
- Intelligent power management for graceful shutdown

Intelligent Power Management

Solid state components including a 30Gbyte Flash hard drive means there are no moving parts in the SGA Site Controller, making for lower maintenance and silent operation

Remarkably low power consumption (typically 8W) allows the Site Controller to be housed in any of the standard SGA enclosures without the need for louvers or forced ventilation

Very low power consumption allows a standard 7Ah battery to maintain the unit for up to ten hours during a power failure

Intelligent power management gracefully shuts down the controller if the battery becomes too low, thus avoiding file corruption and data loss

A monitor, mouse and keyboard can be directly connected but are not necessary for normal operation

With the ability to monitor and manage the board via a remote PC connection it can be discretely positioned anywhere on a site or in an office complex

Product Codes

SGA-SC-IAC25-PSU	SGA Site Controller, enclosure and 2.5A PSU. Pre-loaded with core SGA software for up to 25 IAC's (50 readers)
SGA-SC-IAC50-PSU	SGA Site Controller, enclosure and 2.5A PSU. Pre-loaded with core SGA software for up to 50 IAC's (100 readers)

Intelligent Access Controller (IAC)



Intelligent Access Controller (IAC)

The IAC provides all of the I/O required for 2 x single-reader doors or a single door with dual readers. In addition the IAC offers 6 x additional inputs and 4 x change-over relay outputs for general system use, plus a separate tamper point for the panel enclosure.

Overview

Intelligent Access Controller (IAC-485)

Intelligent Access Controllers (IAC-485's) can be connected together with up to 32 x IAC and/or IOC nodes to form a Siteguard comms line.

2 or 4-wire data-cabling interconnects the RS485 IAC's which in turn connect directly to the SGA Site Controller. There is no need for a comms line header (converter) for the first comms line when using a Site Controller as it is included within the on-board circuitry. For additional RS485 comms lines on a Site Controller, and for all RS485 comms lines when using a main PC/server, a USB or ethernet converter is required to connect the line.

Any number of Siteguard Access RS485 comms lines can be installed and no matter how large or small the system, the comms line header (USB or Ethernet) is the only variant in the system design. USB converters obviously require a USB port of which there are 3 spare on a Site Controller.

Intelligent Access Controller (IACe - eSeries)

The IACe is an ethernet ready controller that does not require a comms line header or interconnecting wiring between the IACe nodes. Each board employs its own TCP/IP address and connects directly onto a LAN or WAN via an IP-switch and the on-board RJ45 ethernet adaptor.

An IACe is exclusively 'tied' to its Siteguard Access system and employs Rijndael advanced data encryption (AES) to protect against sabotage and malicious attack.

PSU and Enclosures

IAC's and IOC's include an enclosure and integral 2.5A PSU (2A available for locks and peripherals). A 5-way enclosure is also available if limited wall space is a site restriction and IAC/IOC boards can be sourced without an enclosure for use in this instance (see page 13).

Features

- Intelligent Access Controller (IAC)(RS485 and TCP/IP versions available)
- 2 x readers with PIN - 1 or 2 door configuration
- Additional 6 x alarm inputs & 4 x relay outputs
- 12,000 card holders at controller (basic memory). 65,000 with ext. memory. (Reduce numbers by half if using User-Defined PIN's)
- Rijndael AES data encryption on eSeries
- Real-time processing at door
- 2.5A power supply with battery back-up
- 1A @12Vdc is available per lock from the IAC
- Local LED and sounder outputs
- Memory buffer whilst off-line (4,000 events)
- Upgrade flash whilst system is working
- Any modern reader technology supported *
- Individual battery back-up
- No system limit for the number of controllers

* Some readers use special protection codes or formats that cannot be used by SGA without the permission and full co-operation of the originator. In these instances contact Grosvenor Technology for assistance. support@gtl.biz

Technical Specification

Dimensions (H.W.D):	420 x 265 x 77mm
Weight:	5.17kg (with Enclosure and PSU)
Operating Temp:	0°C to 50°C
Power Requirement:	230Vac, 50hz, 63va supervised
Battery Back-Up:	1 x 12V 7Ah battery, supervised, provides operation for up to 12 hours for IAC board only or typically up to 4 hours inc. locks and readers
Reader Types:	Most modern day technologies
Reader Power:	5Vdc or 12Vdc
Outputs (LED/Buzzer):	Door forced, door wedged, valid card, invalid card
Auxiliary Inputs:	6 x supervised inputs
Auxiliary Outputs:	4 x 2A max. c/o relay outputs
Internal Lock Power:	12Vdc, NO/NC, 1A ea, supervised, short-circuit protected. External lock power (optional) 24Vac/dc, circuits rated at 3A ea, supervised IAC-485 - 2 or 4-wire RS485/422 IAC-485 - Up to 19.2K baud IACe - RJ45 Ethernet 10/100 BaseT IACe - 10/100Mbps
Communication:	
DHCP:	Supported
Encryption:	IACe only - Rijndael advanced data encryption standard (AES)
Firmware:	Flash memory dual 512Kbit
RAM Memory:	1Mbit expandable to 4Mbit, supported by main battery

Product Codes

636.003.016.10	IAC for RS485 comms, enclosure, tamper and 2.5 Amp PSU. Tyco protocol. 12,000 card holders
636.003.016.10E	IAC for ethernet comms, enclosure, tamper and 2.5 Amp PSU. Tyco protocol. 12,000 card holders
636.003.016.EXM	Plug-in memory expansion to increase IAC board from 12,000 card holders to 65,000

Input / Output Controller (IOC)



Features

- Input / Output Controller (IOC)(RS485 and TCP/IP available)
- Provides a means of connecting any alarm, switch or relay function to Siteguard Access
- 16 x Supervised Alarm Inputs
- 16 x Change-Over Relay Outputs
- Rijndael AES data encryption on eSeries
- Upgrade Flash whilst system is working
- Permissions and time patterns for I/O controls
- Individual battery back-up
- No system limit for the number of controllers

Input / Output Controller (IOC)

The Input / Output Controller (IOC) provides 16 x inputs and 16 x change-over relay outputs for general system use.

Input / Output Controllers and Intelligent Access Controllers (IAC's) can all be used on the same Siteguard system.

Overview

Input / Output Controller (IOC-485)

Input / Output Controllers (IOC-485's) can be connected together with up to 32 x IAC and/or IOC nodes forming a Siteguard Access comms line.

Input/Output Controller (IOCe - eSeries)

The IOCe is an ethernet ready controller that does not require a comms line header or interconnecting wiring between the IOCe nodes.

2 or 4-wire data-cabling interconnects the RS485 IOC's which in turn connect directly to the SGA Site Controller. There is no need for a comms line header (converter) for the first comms line when using a Site Controller as it is included within the on-board circuitry. For additional RS485 comms lines on a Site Controller, and for all RS485 comms lines when using a main PC/server, a USB or ethernet converter is required to connect the line.

Each board employs its own TCP/IP address and connects directly onto a LAN or WAN via an IP-switch and the on-board RJ45 ethernet adaptor.

Any number of Siteguard Access RS485 comms lines can be installed and no matter how large or small the system, the comms line header (USB or Ethernet) is the only variant in the system design. USB converters obviously require a USB port of which there are 3 spare on a Site Controller.

An IOCe is exclusively 'tied' to its Siteguard Access system and employs Rijndael advanced data encryption (AES) to protect against sabotage and malicious attack.

Technical Specification

Dimensions (H.W.D):	420 x 265 x 77mm
Weight:	5.17kg (with Enclosure and PSU)
Operating Temp:	0°C to 50°C
Power Requirement:	230Vac, 50hz, 63va supervised
Battery Back-Up:	1 x 12V 7Ah battery, supervised, Battery duration will vary depending upon relay operations, but typically provides 4 hours local backup
Auxiliary Inputs:	16 x supervised inputs
Auxiliary Outputs:	16 x 2A 30V max, c/o relay outputs
Communication:	IOC-485 - 2 or 4-wire RS485/422 IOC-485 - Up to 19.2K baud IOCe - RJ45 Ethernet 10/100 BaseT IOCe - 10/100Mbps
DHCP:	Supported
Encryption:	IOCe only - Rijndael advanced data encryption standard (AES)
Firmware Flash Memory:	Dual 512Kbit

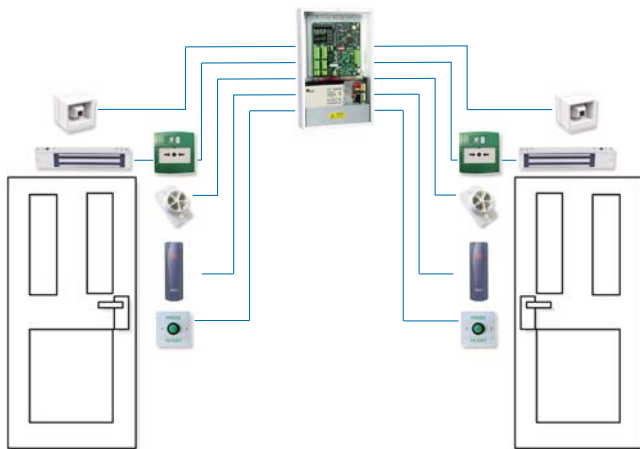
PSU and Enclosures

IAC's and IOC's include an enclosure and integral 2.5A PSU (2A available for locks and peripherals). A 5-way enclosure is also available if limited wall space is a site restriction and IAC/IOC boards can be sourced without an enclosure for use in this instance (see page 13).

Product Codes

636.004.014.16	IOC for RS485 comms, 16 x inputs, 16 x outputs, enclosure, tamper, and 2.5A PSU. Tyco protocol
636.004.014.16E	IOC for TCP/IP comms, 16 x inputs, 16 x outputs, enclosure, tamper, and 2.5A PSU. Tyco protocol

IAC Two Door Configuration



IAC Two Door Configuration

- Each IAC (RS485 & eSeries) can manage 2 x doors with reader IN and egress button OUT or 1 x door with reader IN & OUT
- Once an IAC has been connected to the main PC/server all other connections run from the IAC to the door furniture which may include any combination of:
 - 2 x readers with optional PIN
 - 2 x egress switches
 - 2 x door contacts
 - 2 x locks with optional break-glass unit
 - 2 x local door sounders

SGA Cable Types

Device	Cable Type	Max Length
RS485 Network	2 pair screened Belden #8723	1.2 KMtrs
Card Reader	4 pair screened Belden #9504	50 Mtrs
Door / Lock	Normally 2 core Subject to volt drop use	Subject to volt drop Alarm 4 / 6 / 8 core
Keypad to K/P Interface	12 core screened	2 Mtrs
K/P Interface to IAC	4 Pair Screened Belden #9504	50 Mtrs
Input / Outputs	2 Core per device Use alarm 4 / 6 / 8 core	100 Mtrs
Power	3 Core 0.75mm2	-

Product Codes

2120
610.001.045
2045/2046/2047
610.001.046
610.001.045
2009
2045/2046/2047

I/O Multiplexer



Features

- Extends data signals 1,200Mtrs on a 1-pair wire
- Includes reader, door and lock signals
- Ideal for heritage sites where small cables are a benefit

I/O Mux

The I/O Multiplexer (also known as an I/O Mux) provides a means of transferring reader, door and lock signals over a 2-wire RS485 data connection.

Typical applications include :-

- Readers in a lift car where the IAC is remote from the lift car (long distance)
- Heritage sites where a 1-pair cable would be easier to install (smaller cables to hide)

An I/O Mux is required at each end of a 1-pair cable.

1 pair of I/O Mux caters for a single portal channel therefore if two door/reader sets are required to be extended, 4 x I/O Mux will be required.

Product Code

DVR-IO-MUX

1 x I/O Multiplexer in plastic housing. Requires 12Vdc power supply which can be derived from the IAC. (Should be purchased in pairs).

USB Converter



Features

- USB to RS485 / RS422 converters
- 2 or 4-wire connectivity
- 1-way and 4-way units available
- 1-way units powered via USB from main PC/server
- PRO versions include opto-isolation protection against ground potential variances
- 32 x controller nodes per comms line
- 1,200 Mtrs cable segment supported

USB Converter

Serially connected RS485 controllers must be connected to the Site Controller or the main PC/server via a comms line header. This can be a USB or an ethernet converter.

A USB converter is 'hard-wired' from a USB port and converts Siteguard communications protocol to RS485. A USB converter is suitable for driving up to 1,200Mtrs on 2 or 4-wire copper cable.

Multiple USB converters may be connected to the same Siteguard Access system utilising additional USB2 ports on the Site Controller or the main PC/server.

Product Codes

637.006.048

USB converter and cable. This unit is powered via the USB port on the Site Controller or PC. Supports up to 32 x RS485 2-wire IAC's or IOC's

LH-USB-485-PRO1

USB converter and cable. This unit is powered via the USB port on the Site Controller or PC. Supports up to 32 x RS485 2 and 4-wire IAC's or IOC's and is opto-isolated for greater reliability even in the most challenging electrical environments

Ethernet Converter



Features

- Ethernet to RS485 / RS422 converters
- 2 or 4-wire connectivity
- RJ45 ethernet 10/100 BaseT, DHCP supported
- Enables routing of RS485 and RS422 JANUS comms via a TCP/IP network
- 32 x controller nodes per comms line
- RS485 1,200Mtrs cable segment supported
- No limit to the number of ethernet converters supported on a Siteguard Access system
- Rijndael advanced data encryption (AES)

Ethernet Converter

An ethernet converter connects to the Siteguard LAN / WAN via an on-board RJ45 ethernet adaptor.

Ethernet converters use a unique TCP/IP address which is identified to SGA and converts Siteguard communications protocol from ethernet to RS485 and is suitable for driving up to 1,200Mtrs on a 2 or 4-wire copper cable.

There is no limit to the number of ethernet converters that may be connected to the same Siteguard system.

Product Codes

LH-ENET-485

Ethernet line Header only. Supports up to 32 x controllers. Requires fixed IP address and 12Vdc supply. Ethernet Line Header complete with enclosure and PSU. Requires Fixed IP address and 240Vac supply

637.006.062

5-Way Enclosure Cabinet



Features

- Small footprint saves wall space (Dimensions: 350 x 450 x 300 W, H, Dmm)
- Easily expandable
- Multiple configuration options
- Blades can be individually battery backed (Including the Site Controller and IP switch)
- Ample room for wiring
- Cabinet is empty when ordered. Blades and boards must be ordered separately. Picture shown is when fully populated

5-Way Enclosure Cabinet

The 5-way enclosure allows 5 x SGA IAC/IOC boards to be installed in any combination e.g.

- 5 x RS485 controllers
(10 x readers or 80 x I/O)
- 1 x Site Controller, + 4 x RS485 controllers
(8 x readers or 64 x I/O)
- 1 x Ethernet Switch, + 4 x eSeries controllers
(8 x readers or 64 x I/O)
- 1 x Site Controller, + 1 x ethernet switch,
+ 3 x eSeries controllers (6 x readers or 48 x I/O)

The cabinet and blades are purchased separately to allow for greatest flexibility, and each blade includes its own 2A PSU with battery charging circuits.

Important Note:

Because of the cabinet weight when fully loaded with 5 x 7Ah batteries, the cabinet must always be installed on a uni-strut framework.

Product Code

ENC-5WAY-230V

5-way enclosure. 220V transformer and tamper

Basic Blade for 5-Way Enclosure



Features

- Spare blade suitable for any SGA controller
- Includes 2A PSU with battery charging circuits
- Individual 7Ah battery is required per blade

Basic Blade for 5-Way Enclosure

A standard blade for the 5-way enclosure includes a 2A PSU and battery charging circuits.

Mounting posts and interconnecting cabling for any of the SGA controllers are included.

Product Code

ENC-BLADE-20-PSU

Single blade c/w 2A PSU. Mounting posts for Site Controller or IAC/IOC boards, interconnecting wiring and battery charging circuits are all included.

Blade c/w Ethernet Switch



Features

- Battery backed 12Vdc ethernet switch
- Industrial environment EMC compatible
- 10BASE-T/100BASE-TX compliant
- RoHS compliant
- 4 x patch cables supplied with blade
- Individual 7Ah battery is required per blade

Ethernet Switch

This blade comes complete with a 12Vdc ethernet switch which is powered from the standard PSU. (The switch does not need to be ordered separately).

Being 12Vdc powered it can also be battery backed from the 7Ah battery which would be fitted separately.

The five-way ethernet switch allows for 1 x ethernet feed into the cabinet and 4 x ports to connect to eSeries boards that would be installed into the same cabinet.

Product Code

ENC-BLADE-ENET

Single blade c/w 2A PSU and 5-port ethernet switch. Unit is suitable for 12Vdc and includes battery charging circuits. Also includes 4 x patch cables to connect from switch to IAC/IOC boards inside the 5-way cabinet

5-Way Enclosure - Supporting Products



5-Way Enclosure - Supporting Products

Because the 5-way enclosure can be made up from separate items there is a need to supply individual boards without the 1-way enclosure that they would normally be shipped in. These items are listed here for your convenience.

- Site Controller board only
- IAC - RS485 and eSeries boards
- IOC - RS485 and eSeries boards

Product Codes

SGA-SC-IAC25-000

Site Controller board and system dongle. Pre-loaded with SGA Core software for 25 x IAC's (50 x readers).

SGA-SC-IAC50-000

Site Controller board and system dongle. Pre-loaded with SGA Core software for 50 x IAC's (100 x readers).

SGA-IAC-485

IAC RS485 board only (RS485 comms).

SGA-IAC-E

IACe eSeries board only (ethernet comms).

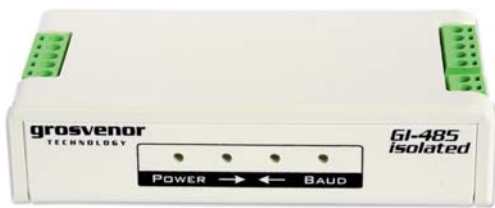
SGA-IOC-485

IOC RS485 board only (RS485 comms)

SGA-IOC-E

IOCe eSeries board only (ethernet comms).

Galvanically Isolated Line Driver



Galvanically Isolated Line Driver

The DVR-GI-485 allows you to extend a SGA comms line by another 1,200Mtrs from the DVR-GI-485 position. It also accepts RS485 2 or 4-wire comms in and RS485 2 or 4-wire comms out. The line in and line out are opto-isolated for greater reliability in challenging electrical environments and this unit should always be used at the point of exit and entry of a building when SGA comms wiring is run externally.

If external wiring is to be run underground the DVR-GI-485 is normally sufficient to protect against extraneously induced voltages. If the wiring is to be run above ground e.g. on a catenary overhead wire, contact Grosvenor Technology for advice on lightning protection - support@gtl.biz

It should be noted that an extended comms line distance does not increase the number of comms line nodes e.g. 32 x IAC's/IOC's.

Features

- Galvanically isolates comms lines when run between different buildings
- Re-generates RS485 comms signals
- Extends comms line distance by 1,200Mtrs
- Includes opto-isolation for greater reliability in challenging electrical environments
- As well as 2-wire in, 2-wire out. 4-wire in, 4-wire out, wiring can be changed from 2-wire in, 4-wire out or vice versa

Product Code

DVR-GI-485

Inline RS485 comms driver, includes galvanic opto-isolation. Requires 12Vdc

Volt Free Relay Lock Interface



Volt Free Relay Lock Interface

The volt free relay lock interface is a plug-in hardware unit that changes the 12Vdc lock output of an IAC into volt free change-over relay contacts. This is useful when operating turnstiles or barriers where 'dry-contacts' are needed rather than an applied voltage.

1 x unit transforms both IAC lock outputs and each pole is rated at 1A.

Note

This unit is only suitable for volt-free operation and is not suitable for switching current.

Features

- 1Amp rated contacts
- Plug-in unit. No tools required
- One unit per IAC (2 x lock output ports)

Product Code

IDC-RLY-LCK-INT

Plug-in volt-free relay lock interface unit.

Indala Proximity Readers



Features

- Uses passive cards (no battery) for long life
- Non-contact for convenience and ease of use
- Small unobtrusive readers
- Maintenance free card reader life
- Cards can be supplied in ISO credit card size with integral mag-stripe for multi-function

HID Indala Proximity

SGA proximity readers are manufactured by HID Indala and programmed exclusively for use with Siteguard Access.



Indala 125 kHz proximity cards and tags feature FlexSecur® technology which provides an additional level of security through a verification process at the reader. Unique to Indala, FlexSecur® screens out unauthorised credentials prior to sending card data to the SGA controller.

This additional verification enhances the security of the card technology in two ways:

- The entire data field of the card / tag is encrypted prior to programming. Therefore, the data on the card cannot be decoded by others. Only the reader is able to decrypt and transmit valid data to the SGA controller.
- Credentials and readers can be uniquely programmed for each site protecting the client against unauthorised entry attempts by using credentials from another facility. This is another unique feature to the Indala product line.

SGA Indala Reader Options

Product Codes

FlexPass Linear Classic		
	Indala FlexPass-Linear reader supplied with black finish. (Classic Format).	
	Read range up to 12cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.	636.002.301FP
FlexPass Linear Mullion (Slim)		
	Indala FlexPass-Linear reader supplied with black finish. (Slim Format)	
	Read range up to 12cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.	636.002.307

Indala Proximity Readers

SGA Indala Reader Options

Product Codes

FlexPass Wave Mullion (Slim)



Indala Flexpass-Wave Mullion reader supplied with Onyx finish. (Slim Format).

636.002.830FP

Read range up to 12cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.

FlexPass Wave Wallswitch

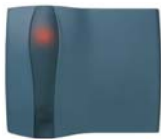


Indala Flexpass-Wave Wallswitch reader supplied with Onyx finish.

636.002.832FP

Read range up to 12cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.

FlexPass Wave (Mid-Range)



Indala Flexpass-Wave reader supplied with Onyx finish. (Mid-Range Format).

636.002.833FP

Read range up to 30cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.

ASK-501 Wallswitch Reader



ASK-501 Wallswitch style prox reader with integral matrix keypad.

636.002.304

Read range up to 10cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.

Indala Legacy Wallswitch Reader



Legacy Wallswitch reader formally known as the ASR-505 Wallswitch reader.

636.002.302

Read range up to 10cm with FlexISO card. Supplied in Grovesnor Format for use with Siteguard Access systems.

Storm Vandal Resistant Keypad



Features

- Vandal resistant (20J BS EN 60068-2-75: 1997)
- Weather, water and dust resistant (IP65)
- All metal keytops and casing
- Permanent, high contrast, engraved keytop graphics

Storm Vandal Resistant Keypad

Attack resistant keypads for use in public environments.

Designed and constructed to ensure rapid and reliable data entry in the most challenging applications, the Storm 1000 Series keypads are field proven and lab tested to survive hard use, abuse and vandalism. Ideal for use in a wide range of industrial, commercial and public applications.

Note

Requires Storm Keypad Interface.

Product Codes

PIN-12-KEY-T	Storm keypad telephone style
PIN-12-KEY-SMBB	Surface mounting back box

Storm Keypad Interface



Features

- Fixes directly onto rear-side of Storm keypad
- Connects to IAC via 4 cores (2-power 2-data)
- Can be wired up to 50Mtrs from IAC

Storm Keypad Interface

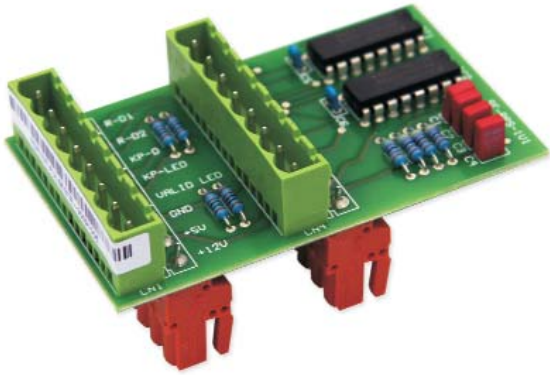
The keypad interface can be fixed directly to the rear-side of the keypad or wired remotely (2Mtrs) if required.

The interface transmits PIN activations to the IAC which can be up to 50Mtrs distance.

Product Code

PIN-INT-12-KEY	PIN interface board only
----------------	--------------------------

Grosvenor Format Wiegand Pulse Stretcher



Features

- Converts standard wiegand into Grosvenor Format
- Plug-in unit. No tools required
- One unit per IAC (2 x reader ports)

Pulse Stretcher

Siteguard access can work with most modern reader types but they should always be Grosvenor Format when using a wiegand output.

The Pulse Stretcher is a plug-in hardware unit that changes a standard wiegand output into Grosvenor Format so that standard wiegand readers can be used with the system.

Readers in this catalogue are manufactured as Grosvenor Format so the Pulse Stretcher is not required.

Product Code

RDR-INT-PULSESTR Plug-in Pulse Stretcher unit.

Indala FlexCard® Proximity Card



Features

- Convenient credit card size can be carried in a purse or wallet
- ABS Construction
- Lightweight - Features bevelled edges and a thickness of only 1.8mm (0.065 inches)
- Vertical Design - Well-suited for badge use

Indala Proximity Clamshell

Exclusive FlexSecur® Security Technology

The Indala FlexCard® is ideally suited to many applications and environments including:

- Warehouse
- Factory
- Universities
- Offices

The Indala FlexCard® clamshell card is "credit card" length and width, features beveled edges, and at a thickness of only 1.8mm (0.065"), is one of the thinnest proximity cards of its kind. Flexible and light enough to be carried in a purse or wallet, the card can also accept photo-flap and direct-print adhesive backed ID badge overlays.

The RF-programmable card is a 125kHz credential featuring high quality and security through the use of FlexSecur® authentication.

Indala's FlexCard can be used interchangeably with other Indala credentials and can be ordered with specified facility codes and ID numbers.

Two Points of Authentication

The reader first authenticates the credential. After validation, the reader passes the credential's information to the host system for authentication. If the reader does not validate the credential, no information is passed on to the host system.

Expanded Credential Information

Use the 172 bits to code employee's office location, grade level, department location, or any other pertinent credential information.

Technical Specification

Dimensions (mm):	86 x 54 x 1.8
Weight (grams):	12
Temperature:	-30° to 65°C
Typical Max Read Range:*	Slim/Wall switch: Up to 12cm Linear Classic Up to 12cm Mid-Range Up to 30cm Long-Range Up to 63cm
Inkjet Marking:	Includes sales order number and ID number matching internal ID
Slot Punch:	Vertical
Description:	125 kHz, Indala logo (front), embossed Indala logo (back), inkjet marking on embossed side (lower right corner with slot to the right), vertical slot punch, no artwork.

Product Codes

636.001.902.SGA	Unbranded Siteguard format Indala clamshell card. No site specific site code supplied unless a special order is placed.
636.001.903.SGA	ADT branded Siteguard format Indala clamshell card. No site specific site code supplied unless a special order is placed.

Indala FlexISO® Proximity Card



Features

- Graphics quality surface - On both sides
- Many systems applications
- Optional magnetic stripe for use with other systems, such as cafeteria vending, copy machines and fuel dispensing
- ISO 7810 compliant

Indala Proximity ISO Card

The Indala FlexISO® card has the ability to contain multiple card technologies in a single credential for systems such as cafeteria vending, copy machines and fuel dispensing.

Digital photos and graphics can be printed directly over the FlexISO's front surface by using a dye-sublimation printer. Bar codes can be imaged onto the card for use with tracking, time and attendance, library systems or job costing systems and the mag stripe can be used for compatible systems requiring magnetic swipe technology.

The RF-programmable card is a 125kHz credential featuring high quality and security through the use of FlexSecur® authentication.

Indala's FlexISO can be used interchangeably with other Indala credentials and can be ordered with specified facility codes and ID numbers.

Two Points of Authentication

The reader first authenticates the credential. After validation, the reader passes the credential's information to the host system for authentication. If the reader does not validate the credential, no information is passed on to the host system.

Expanded Credential Information

Use the 172 bits to code employee's office location, grade level, department location, or any other pertinent credential information.

Technical Specification

Dimensions (mm):	86 x 54 x 0.73 nominal
Weight (grams):	6
Temperature:	0° to 50°C
Typical Maximum Read Range:*	Slim/Wall switch Up to 12cm Linear Classic Up to 12cm Mid-Range Up to 30cm Long-Range Up to 66cm
Inkjet Marking:	Includes sales order number and ID number matching internal ID
Custom Graphics:	Available on FlexISO with customer-supplied artwork.
Slot Punch:	Optional vertical or horizontal (locations indicated on card)
Description:	125 kHz, white glossy finish (front), white glossy finish with Indala logo and mag stripe (back), inkjet marking on standard location, no slot punch, no artwork

Product Code

636.001.904.SGA

Indala ISO prox card suitable for ID printing. Supplied with unencoded magstripe on reverse side. Not site code specific as it is for use with Siteguard Access and will be taken from SGA bureau stock.

Indala FlexKey® Proximity Tag



Indala FlexKey

Exclusive FlexSecur® Security Technology

The rugged Indala FlexKey® is ideally suited for a variety of applications and environments including:

- Holiday resorts
- Locker rooms
- Health spas
- Apartment buildings
- Club houses
- Offices where photo-ID's are not required

The RF-programmable keytag is a 125kHz key fob featuring high quality and security through the use of FlexSecur® authentication.

With up to 172 user-definable bits, FlexKey® permits the encoding of a wide range of data and information.

Technical Specification

Dimensions (mm):	43.8 x 30.4 x 5.46
Weight (grams):	5.4
Temperature:	-30° to 65°C
Typical Max Read Range:	Slim/Wall switch: Up to 5cm Linear Classic Up to 5cm Mid-Range: Up to 17cm Long-Range: Up to 40cm
Inkjet Marking:	Includes sales order number and ID number matching internal ID on printed strip on back side
Outer shell:	Ultrasonic welded polycarbonate
Inner shell:	RF core shielded in epoxy
Packaging:	100 sequential units per container
Description:	125 kHz, printed Indala logo on front side, printed strip for inkjet marking on back side

Features

- Contemporary design
- Easily attached to a keyring, badge clip, or lanyard
- LED Construction
- Built to withstand harsh operating environments
- FlexKey can be customised by including a company logo or motif

Able to withstand harsh environments, the FlexKey® has double-sealed construction. The inner electronics are fully encapsulated and the outer body is ultra-sonically welded polycarbonate material.

Designed to complement the Indala Curve and Wave product lines. The surface can be customised with company logos.

Two Points of Authentication

An Indala reader first authenticates a credential after which it passes the credential's information to the SGA controller for system for authentication. If the reader does not validate the credential, no information is passed to SGA.

Expanded Credential Information

Use the 172 bits to code an employee's office location, grade level, department location, or any other pertinent credential information.

Product Code

636.001.905.SGA Indala prox keyfob - not site code specific as it is for use with SGA and will be taken from SGA bureau stock.



This page is left intentionally blank

Magicaid MC200 Printer & Consumables



Features

- 100 x card feeder and hand-feed card slot provide batch and one-off card printing convenience
- LCD display with simple button menu selections
- USB rev1.1 (USB 2.0 compatible)
- Thermal transfer with solid wax and colour dye sublimation
- Two year factory warranty

Magicaid MC200 Single Sided Printer

MC200 single sided ID printer c/w power lead and selectable UK/EU plugtop. Kit includes printer, YMCKO colour ribbon for up to 300 prints, cleaning kit and 100 plain PVC cards. Printer has 1 year Ultra coverplus warranty and 2nd year return to base.

Technical Specification

Print method	Thermal transfer with solid wax and colour dye sublimation
Magstripe option	ISO 7811 Magstripe encoder
Resolution	High quality 300dpi images
Colour ribbon	5 panel colour dye film - YMCKO - 300 images per roll
Black ribbon	2 panel monochrome dye film - KO 600 images per roll
Print speed	35 seconds (colour) 7 seconds (mono)
Interface	USB rev1.1 (USB 2.0 compatible)
Card capacity	100-card feeder, 30-card stacker
Cleaning kit	Cleaning kit - 10 cards, 1 pen
Cleaning roller kit	Cleaning roller and 5 sleeves
Temperature	Sheltered Office environment 10°C to 30°C (50°F to 85°F)
Weight	5.5kg
Power	External power "brick" for 90-265V 40-60Hz (autoranging)

Product Codes

3633-0003	Ultra single sided ID printer
MA300YMCKO	MC200 colour ribbon
MA600KO	MC200 resin black ribbon
3633-0053	MC200 cleaning kit
3633-0054	MC200 cleaning roller kit



This page is left intentionally blank

SGA Core Software



Siteguard Access Core Software

Siteguard core software is licensed by the number of IAC's and the number of extended software modules that are required. The system can manage any number of readers and card holders without limitation and the starter options for core software include :-

SGA-CORE-IAC25 has the capability to control 25 x IAC's (50 readers), ID card production, graphical alarm screen, incident and engineering logs, archive and reporting. This version includes licensing for 1 x client PC.

SGA-CORE-IAC25 can be installed onto a dedicated SGA Site Controller or a clients own PC (minimum SGA specification required). This PC can be shared with other applications or dedicated to SGA.

SGA-CORE-IAC50 has the capability to control 50 x IAC's (100 readers), ID card production, graphical alarm screen, incident and engineering logs, archive and reporting. This version includes licensing for 3 x concurrent client PC's that are capable of running any of the core applications.

SGA-CORE-IAC50 should be installed onto a dedicated SGA Site Controller or PC (minimum SGA specification required). It is recommended that SGA client PC's are also dedicated to the SGA system.

SGA-CORE-SERVER includes the capability to control 250 x IAC's (500 readers), ID card production, graphical alarm screen, incident and engineering logs, archive and reporting. This version includes licensing for 3 x concurrent client PC's that are capable of running any of the core applications.

SGA-CORE-SERVER should be installed onto a dedicated SGA PC/server (minimum SGA specification required). It is recommended that SGA client PC's are also dedicated to the SGA system.

Input / Output Controllers

Input / Output Controllers (IOC's) are not license restricted and any amount can be installed without license implications.

Siteguard PC Clients

Individual client PCs can be added to the system at any time so that concurrent PC connections to the main PC/server can run and manage the system.

Features

- Access control for unlimited cards and readers
- Three core packages to simplify entry to product
- Dedicated PC not required for smaller systems
- New package to simplify upgrade of older systems
- Integrated ID card production
- Integrated graphical alarm monitoring
- Incident and engineering logs
- Client PC's expandable to unlimited numbers
- Single and multi-sites anywhere in the world
- Microsoft Vista compliant

Siteguard Site Controller

SGA-CORE-IAC25 and SGA-CORE-IAC50 are available as pre-installed systems on the SGA Site Controller with the additional benefits of :-

- Very low power consumption to greatly reduce energy costs and carbon footprint
- Battery backup safeguarding against power glitches and outages whilst maintaining real-time comms
- Graceful shutdown in the event of battery failing safeguarding against corrupt files and applications
- Can be discretely positioned anywhere on a site or office complex
- Includes 1 x comms line header so an RS485 converter is not required for the first 32 x controllers

Siteguard Upgrade Path

New upgrade packages enable existing SGA systems to expand into the new format in a single move. SGA extended software modules previously purchased will also be included within any upgrade.

Technical Specification

Operating System

The latest version, SGA v4.3, is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server. Latest Service packs to be installed.

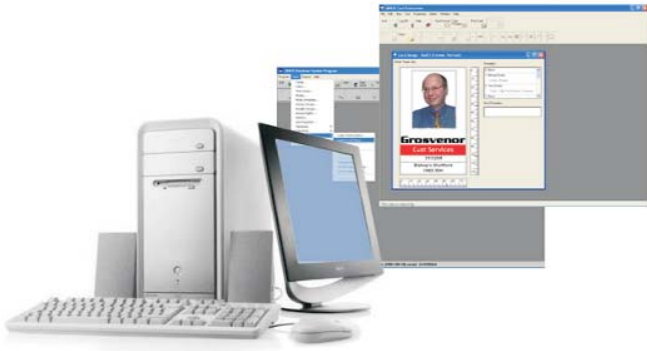
Product Codes

SGA-CORE-IAC25	SGA core software license for 25 x IAC's (50 x readers)
SGA-CORE-IAC50	SGA core software license for 50 x IAC's (100 x readers)
SGA-CORE-SERVER	SGA core software license for 250 x IAC's (500 x readers)
SGA-UPG-IAC25	SGA core software upgrade to take an existing system to 25 x IAC's
SGA-UPG-IAC50	SGA core software upgrade to take an existing system to 50 x IAC's
SGA-UPG-SERVER	SGA core software upgrade to take an existing system to 250 x IAC's

Note

If a system needs to upgrade by a large amount, two packages may need to be purchased.

SGA ID Badging (Included in Core Software)



Features

- Multiple card formats and designs
- Use any data field from Card and User Records (including custom fields)
- User friendly design editor
- Mag Stripe and Smartcard encoding (If supported by the card printer)
- Batch or individual print runs
- Barcode printing supported
- Multiple printer options

ID Badging & Card Production

Siteguard Access Card Production is a fully integrated ID imaging and card production system with powerful features such as:-

- user friendly design editor
- support for multiple graphical formats
- picture cropping with user defined aspect ratio
- copy and export designs to other SGA systems

Photographs, signatures and logos can be utilised from video capture, digital cameras, scanners, signature tablets or import of existing files created by other systems.

Any number of card formats and designs can be created making use of default and user defined fields within the Siteguard Access User and Card records. Designs can be created and modified with landscape and portrait formats including orientation and layout by the system manager and stored with unlimited designs.

Technical Specification

Operating System

Always ensure the printer supports your chosen operating system. Latest service packs must be installed.

Note

Card printing is processor hungry and if run from the same PC as the Guard Screen or comms application it can slow real-time events annunciating by some seconds. If this will be an issue use a separate/remote PC for card printing.

ID pictures stored in the system are utilised throughout SGA for consistency in verification e.g. real-time events reported in the Guard Screen and/or the Pictures application.

Special features such as mag stripe encoding, smartcard encoding and holographic overlays can all be included as long as these features are supported by the card printer.

Product Code

637.007.511

SGA ID badging licence For new systems it will be included within the initial licence.

SGA Graphics (Included in Core Software)



Features

- Dynamically interface with drill-down maps
- Animated icons
- View and acknowledge alarms
- Oversee people and company assets in area
- Include third party systems e.g. intruder system
- Log-On levels per individual user

Graphics Add-On for Guard Screen

Real-Time Graphical Interface

The real-time graphical interface within Siteguard uses digital drawings and photographs of a site and is primarily used to display, monitor and control system activities.

The status and control of doors, barriers, turnstiles, alarm inputs, system outputs, area occupancy and company assets can all be clearly and precisely monitored such that Siteguard graphics quickly becomes a central and integral component of the core Report/Guard Screen.

Monitor System Health

System health and status is supervised within the SGA graphical environment including hardware faults such as controller off-line, tamper and loss of power.

Integration with Other Systems

System interfacing is used to dynamically share Siteguard graphical information with other safety and security systems and annunciate alarms and events for example from SGA Intruder (Galaxy 500). Once interfaced into Siteguard, a third-party event is monitored within the normal graphical Report/Guard screen and transactions are stored in the Siteguard history file for inclusion into standard historical reporting.

Technical Specification

Operating System

The latest version, SGA v4.3, is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server. Latest Service packs to be installed.

Additional Benefits

- No limit to number of maps
- Drill-down features for maps and icons
- Animated icons whilst in alarm state
- Over-ride doors/turnstiles/barriers
- View/acknowledge input/alarm state
- Change output state
- Oversee people and assets in area
- Graphical integration with other alarm panels
- Suitable for touch-screen operation
- Individual log-on controls
- Auto switch option upon alarm
- Monitor company assets
- Cloak healthy icons on busy screens
- Control animation speeds

Product Code

637.007.512

SGA graphics licence
For new systems it will be included within the initial licence.

This page is left intentionally blank

SGA Network / Client PC Licence



Features

- Allows simultaneous access to the system database and/or other SGA applications
- Networked/client PC's are managed and controlled by a user's individual log-on name and password
- Each license is for concurrent system user and not for a specific PC or user name
- Dedicated PC is not required
- Unlimited workstations

Network/PC Client Licence

Network/Client PC license's determine and manage how many SGA Report Screens and SGA Database applications can be running and connected to the SGA Comms program at any one time.

If a Siteguard system has 4 x SGA network/client licenses, in addition to the main PC/server, up to 4 x other instances of the Report / Database applications can be run concurrently. This is not a limit to the number of PC's on the network - only a limit to the number of instances connected and running at any one time.

Technical Specification

Operating System

The latest version, SGA v4.3, is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server. Latest Service packs to be installed.

Product Code

637.007.510

SGA Client PC licence.

SGA Pictures



Pictures

Asset and ID Verification

Pictures is an SGA add-on module that displays previously stored card holder and/or asset images when a transaction is detected at any nominated reader.

Pictures enables ID verification as a card holder attempts to enter an area, protecting against cards improperly acquired. System supervisors can compare the stored image either at the door or via a remote CCTV monitor. Wireless networks and tablet PCs are especially useful for spot checks in times of heightened security.

The same instance of Pictures will display a photograph of an asset should it go into alarm or be seen at a portal protected by an asset reader. When Pictures is used in conjunction with Siteguard Graphics, the authorised location of a static asset is also displayed alongside the image.

Display Options

Pictures provides different display options:

- Detail View - Shows the last transactions with textual detail about the person/asset and the event
- Multiple View - Shows pictures and some transaction detail in a grid format. The size and format of the grid is variable with up to 4 x 4 rows/columns
- History View - Shows line by line historical transactions

Features

- ID and asset verification at point of use
- Complements Siteguard Access Graphics
- Detail, multiple and historical views
- Different readers can report to different screens
- Roaming capability with tablet PCs

Additional Benefits

- ID and asset Picture verification at point of use
- Several instances can cover multiple locations
- Detail, multiple and historical views
- Ideally run with the Report/Guard screen
- Compliments Siteguard Graphics
- Single or groups of readers per instance
- Roaming capability with tablet PC's
- Different readers can report to different screens
- Any SGA reader technology
- Long-Range RFID for Asset Protection

Operating System

The latest version, SGA v4.2, is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server. Latest Service packs to be installed.

Core Software

Must be Siteguard Access 4.3 or later

Product Code

637.007.517

SGA Pictures software licence.

SGA Guard Tour



Features

- Tours can be edited, saved and run
- Monitor Guard Tours for correct tour patterns and time spans
- Generate alarms for tour anomalies
- Tours can use card or system inputs to register arrival at stations*

Guard Tour

Sequenced and Random Tours

Guard Tour is a sub-module of SGA and functions from any SGA networked PC. Multiple tours can be run together on the same or on different client PCs.

Every tour must start and end with a nominated card with the intermediate stations being any mixture of the same card and/or system inputs.

Technical Specification

Operating System

The latest version, SGA v4.2, is supported on Windows XP Professional, Windows Vista (Business or Enterprise), and Windows 2003 Server. Latest Service packs to be installed.

* A guard tour must start and end with a card reader

Core Software

Must be Siteguard Access 4.3 or later

Tailored to your Need

Any active card can undertake a guard tour and can be selected on the fly from the SGA PC. Tours can be Random or Sequenced with readers and system inputs being visited as the descriptions suggest, either randomly over a set time span or in a pre-set sequence over a set time span.

A Guard Tour is managed and monitored by the system in real-time with alarm and event activity being logged for future historical reporting via the standard Siteguard Access report generator. Alarms can be initiated upon tour failures and anomalies.

Product Code

637.007.513

SGA Guardtour software licence.

SGA Event Relay & Event Relay Plug-Ins



Third Party Control with SGA

Event Relay is a one-way communications application that captures Siteguard events and uses them to trigger or prompt multiple third-party systems via a pre-described Event Relay action.

When activated, Event Relay actions pass user definable ASCII or XML commands to a third-party system via a TCP/IP socket or a serial connection.

Depending upon the third-party system capabilities, Event Relay actions can cause a device to switch cameras, change recording speeds, append text to a digitally recorded journal e.g. Intellex 'Smart Search', or send an email etc.

Licensing

Event Relay is deployed on the Site Controller or SGA main PC/server and the basic license includes the capability to send generic ASCII or XML commands to multiple third-party 'target' devices. Other specialist personality 'plug-ins' can be added to the basic application and includes:

- Comms plug-in - allows an Event Relay action to feed back into the SGA Comms to control various SGA system parameters e.g.
 - Change a system mode from an input
 - Activate a sounder upon a valid read
 - Unlock a door/s from an input
- IndigoVision plug-in - allows ER to communicate with the IndigoVision Control Centre software which in turn controls the IndigoVision system
- Email plug-in - the SGA email plug-in allows ER to communicate with an exchange server or SMTP Relay service so that emails can be sent upon given SGA system parameters

Event Relay Actions can use triggers from:

Reader Events:

Invalid PIN	No Access Authority
Valid Access	Wrong Time
Wrong Mode	APB Failed
Duress PIN	No Access Group
Invalid Access	No Reader Group
Valid APB	

Features

- Direct Siteguard events to third-party equipment to control and prompt:
- CCTV Switchers
- Digital Video Recorders
- Intruder Panels
- Building Management Systems
- Works with any third-party system capable of receiving standard ASCII or XML commands
- Works via serial or TCP/IP socket
- Send emails upon given SGA events

Door Events

Wedged	Forced
Closed	Exit Switch
Unlocked	Locked
Suspect Sensor	

Input Events

Activated	Reset
Alarm Enabled	Alarm Isolated
Fault	Fault Cleared
Fault Isolated	Fault Enabled
Tamper	Tamper Cleared
Tamper Enabled	Tamper Isolated
Control Isolated	Control Restored

External Alarm Events

Activated	Reset
-----------	-------

Box Events

Action Fired	APB
Closed	Mains Power Off
Mains Power On	Off Line
On Line	Opened
Reload Required	Started
Type And Version	

Area Events

Area Empty	Area Occupied
Not Single Person	Number OK
Number Too Few	Number Too Many
Single Person	

Asset Events

Battery Low	Battery OK
Comms Lost	Comms OK
Motion Isolate Enabled	Motion Isolate Reset
Motion Started	Motion Stopped
OOA Motion Started	OOA Motion Stopped
Tamper Activated	Tamper OK

Core Software

Must be Siteguard Access 4.3 or later

Notes

The on-site engineer will require additional time to configure a command string code for each event / trigger required. Third-party product protocols must be sourced in advance of the engineer attending site as these can take a little while to source from the manufacturer.

Product Codes

637.007.518	Event Relay software licence.
SGA-EVT-RLY-COMM	Event Relay comms plug-in
SGA-EVT-RLY-EMAL	Event Relay email plug-in
SGA-EVT-RLY-IGVN	Event Relay IndigoVision plug-in

SGA Vari-Time Manager - Time Zone Plug-in



Features

- Dynamic shift patterns for up to 51 weeks ahead
- Graphical views of shift patterns
- Simply move a card holder from one shift to another
- The next 7 days shift patterns are held at each IAC to maintain time zones if the controller go off-line

Vari-Time Manager

Rather than using the standard weekly time zones that are repeated every week, if you need to vary access times from week to week or month to month, the SGA Vari-Time Manager can set variable shift patterns for up to 51 weeks in advance.

Multiple Shift Patterns can be defined so that an employee or a group of employees follow a designated shift pattern that is more akin to a typical T&A shift system, offering tighter operational controls and greater system security.

Technical Specification

Core Software

Must be Siteguard Access 4.3 or later

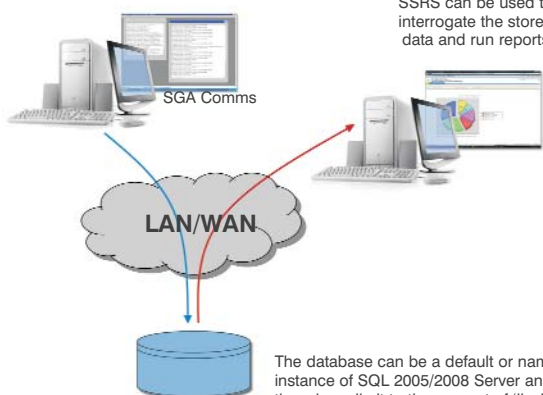
Product Code

SGA-VARI-TIME

SGA Vari-Time Manager license

SGA Queued Report Writer

SGA writes historical events and operator activity onto MSMQ which in turn sends the data to a SQL database. All events are transactional which guarantees delivery



Features

- Graphical and analytical reporting
- No system limit for 'live' immediately available, historical and operator activity data. The only limit is disk space
- Run reports from anywhere via a web browser
- No remote software to install in order to enable the reporting functionality

SGA Queued Report Writer

Queued Report Writer has replaced the now obsolete SGA Head Office Archive & Reporting.

Whilst keeping current history and operator activity always available for reporting, standard SGA archive and reporting requires previously archived history to be restored onto the system before it can be reported upon. This can be time consuming and problematic if different periods need to be appended together.

Queued Report Writer allows you to keep many years of operator activity and historical data live and always available for immediate reporting. It also provides the ability to generate your own extremely powerful graphical and analytical reporting which can be invaluable to other departments within an organisation.

Note

MS SQL licences are not included and should be supplied separately by the client. It is highly recommended that you should include a day for Grosvenor Technology to install.

Contact Grosvenor Technology at customerservices@gtl.biz

Product Code

SGA-QRW

SGA QRW software and licence.

Kone Elevator/Lift Interface



Features

- Automatic floor destination from a card read
- Greater efficiencies for multi-car systems
- Greater control for multi-tenant buildings
- Speedier transit for personnel

Kone Lift Interface

This service is designed to interface with the KONE Polaris Pro lift controllers and act as part of their destination calling feature.

Specific SGA readers e.g. at a turnstile or by a lift call button will be visible in the Kone interface software and can be set to call an elevator/lift and pre-determine its destination dependent upon the department that the cardholder belongs to. After entering the lift car the passenger does not have to activate any additional operations. The passenger reaches his/her destination automatically.

Technical Specification

You must confirm with KONE that the correct equipment is installed or the system will not work.

Core Software

Must be Siteguard Access 4.3 or later

Product Code

NSL

Due to different versions of lift, always get a quotation from Grosvenor Technology

customerservices@gtl.biz

ThyssenKrupp Elevator/Lift Interface



Features

- Automatic floor destination from a card read
- Greater efficiencies for multi-car systems
- Greater control for multi-tenant buildings
- Speedier transit for personnel

ThyssenKrupp Lift Interface

This service is designed to interface with the ThyssenKrupp MX-Board lift controllers and act as part of their destination calling feature.

Specific SGA readers e.g. at a turnstile or by a lift call button will be visible in the ThyssenKrupp interface software and can be set to call an elevator/lift and pre-determine its destination dependent upon the department that the cardholder belongs to. After entering the lift car the passenger does not have to activate any additional operations. The passenger reaches his/her destination automatically.

Technical Specification

You must confirm with ThyssenKrupp that the correct equipment is installed or the system will not work.

Core Software

Must be Siteguard Access 4.3 or later

Product Code

NSL

Due to different versions of lift, always get a quotation from Grosvenor Technology

customerservices@gtl.biz

SGA Bag Search



Features

- Randomly chooses a card holder for bag search
- Include visitors by using an egress button
- Search rate is adjustable e.g. 1 in 10 probability etc.
- Inhibits valid egress until verified
- Works with egress reader, T-REX or both

Bag Search

SGA Bag Search randomly puts cards into an anti-passback area and marks their status as 'Failed Anti-Passback'. This is done at the same time that a valid entry is registered and is determined upon the probability settings that have been pre-defined on the system e.g. 1 in 10, 1 in 20 etc.

Upon an egress attempt by any card in this anti-passback area, the system will prohibit them from leaving and their details will be flagged at a local PC which is monitoring the Bag Search system. Verification at the PC will reset the user's anti-passback status who will then be able to egress in the normal way.

Core Software

Must be Siteguard Access 4.3 or later

Product Code

SGA-BAG-SEARCH SGA Bag Search licence

Galaxy Dimension Intruder Interface



Features

- Allows intruder alarm events to be displayed on any SGA Report / Guard Screen including textual and graphical representations
- Logical rules can be set and used by the system
- Historical / audit reporting of all events and alarms
- Connect panels via ethernet using AnywhereUSB
- Isolate and re-set zones from within SGA

SGA Galaxy Dimension Intruder Interface

The Galaxy Dimension Intruder Interface is a two-way software application that runs on the Site Controller or main PC/server. The SGDI (6620) serial port connects directly to the Site Controller or main PC/server via its serial port but can also connect via USB if using a USB to Serial adaptor.

The Galaxy Dimension interface converts inputs from the SGDI panel (alarm, tamper and fault) into SGA events which can then be displayed on any of the SGA Report / Guard Screens. Once converted, the intruder events are treated in the same manner as a normal SGA input with full alarm monitoring, graphical representation, logical functions and historical reporting being available. In addition, the SGA software can be used to set or unset the SGDI panel.

Core Software

Must be Siteguard Access 4.3 or later

Product Code

637.007.514 SGA GDI software licence

AnywhereUSB Hub



Features

- Network-enabled USB hub
- Connect Galaxy Dimension anywhere on LAN
- USB-to-serial adaptors are also fully compatible

AnywhereUSB Hub

AnywhereUSB is a network-enabled USB hub that delivers the same plug and play user experience as onboard USB ports. Software drivers are loaded onto the SGA Site Controller or the main PC/server enabling remote devices such as Galaxy Dimension panels to communicate with SGA Comms.

Product Code

AE-ANYWHERE-USB AnywhereUSB 5-Way Hub for TCP/IP connection

USB to Serial Adaptor



Features

- Convert USB to RS-232 serial port
- Compatible with Galaxy Dimension panels
- Easy to setup and install
- No external power needed - draws power from the USB connection

USB to Serial Adaptor

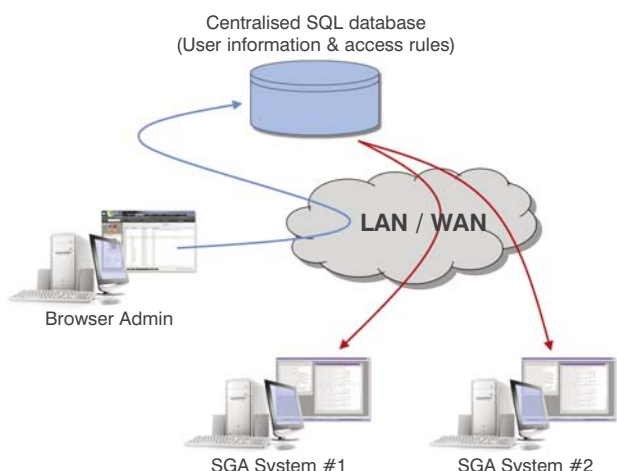
A cost-effective solution that bridges the compatibility gap between USB and serial peripherals such as the Galaxy Dimension intruder panel.

Use this adaptor to connect a Galaxy Dimension panel to a USB port if your point of connection doesn't include a spare serial port e.g. a Site Controller, main SGA PC or a USB Anywhere hub.

Product Code

AE-USB-SER-ADPT USB to Serial Adaptor

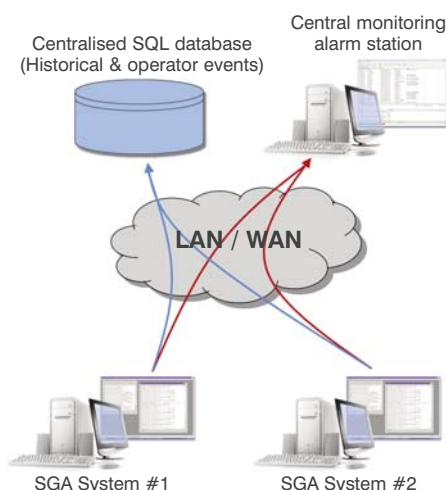
SGA Enterprise



System Admin

- Centralised SQL database
- User specific, database partitioning easily controlled by administrator
- Manage one or more synchronised SGA systems via web browser
- No software to install on admin PC's
- Absolute security

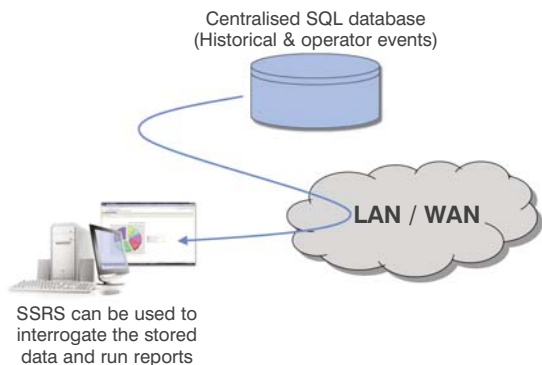
Siteguard Enterprise is the worlds most advanced corporate-wide access solution. One or many Siteguard systems can be controlled and managed via a single SQL database with web browser connections. New SGA systems can be bonded into the scheme from anywhere in the world as long as they are on the same corporate LAN / WAN.



Event Distribution

- Multiple systems monitored by central stations
- Guaranteed message delivery around the system

Historical and operator events can be distributed to one or many centralised SQL databases. Alarms and critical events are directed to central monitoring stations via MSMQ which guarantees message delivery.



Reporting

- Graphical and analytical reporting
- No system limit for 'live' immediately available, historical and operator activity data. The only limit is disk space
- Run reports from anywhere via a web browser
- No remote software to install in order to enable the reporting functionality

Keep many years of operator activity and historical data live and always available for immediate reporting. Generate your own extremely powerful graphical and analytical reporting which can be invaluable for other departments within an organisation.

Siteguard Enterprise is a NSL product. Contact Grosvenor Technology customerservices@gtl.biz for more information



grosvenor
TECHNOLOGY

Features

- Free software upgrades
latest features and functions*
always compatible with the latest/current MS Windows platform
- Free flash and firmware upgrades for existing SGA controllers
- The site system administrator or his/her deputy (registered on SSA certificate) has direct access to the design authority help desk during UK normal working hours for 'reasonable' assistance on how to use the system **
- Free email tracking to an email group of the client's choice for every problem logged
- Certified ADT installation personal have direct access to the design authority help desk during UK normal working hours for 'reasonable' help on maintenance issues (whilst they are on site) ***
- Option of remote diagnostics from the design authority during UK normal working hours ****
- Subsidised day-rate for a design authority engineer to attend site for professional services for example staff re-training, system trouble-shooting, system health-check, assistance in system set-up and/or commissioning new extensions to the system
- Loyalty discount for renewing an SSA within 30 days of expiring SSA

* Features available to the client are also dependant on the firmware installed in the controller

** This does not include system hand-over/user training

*** Non certified engineers may contact Grosvenor's Tech Support team but they reserve the right to refuse assistance if the engineer is not SGA or PC literate

**** Remote system connection must be available

Siteguard Access Software Support Agreement Launch

Sites with a SSA contract will benefit from direct access to Grosvenor's support team. You must ensure that the engineer on site has been trained since Grosvenor cannot assist engineers that have little or no experience of SGA.

The second major benefit is remote support allowing Grosvenor to assist directly with software issues.

Remote Support

Remote support will only be available where the client has given approval for the system to be accessed from outside of their network and where a suitable means of connection is made available at no cost to Grosvenor Technology.

This connectivity gives the engineer on site direct support from one of Grosvenor's Technical Support team.

The main methods of remote connection are:-
WebEx (<http://www.webex.co.uk/>)

Design Authority pays for WebEx services and Site pays for internet connection. This is by far the easiest connection to install and could even be done via an HSPA dongle carried by the engineer]

RDP (Remote Desktop) or similar remote control software
Requires input from site IT department to install and set-up. The end user is responsible for the provision and any costs incurred for the Internet connection and they would have to provide remote control software e.g. Microsoft Terminal Services Client

Chapter 8 - SSA

VPN (Virtual Private Network)

Requires input from site IT department to install and set-up. Could be Windows / CISCO etc.

The end user is responsible for the provision and any costs incurred for Internet connection and Software. They must issue the VPN client to Grosvenor Technology if it is not already available. Once the VPN is established then remote desktop / VNC or similar remote control software is used.

Connection Methods:-

- ADSL (Broadband)
- INTERNET (PC can access WebEx website on internet with no other hardware / software)
- CUSTOMER WAN (if PC can access internet if allowed by customers IT Dept)
- HSDPA (Mobile dongle) with Correct Configuration.

N.B. Grosvenor do not provide Remote Support via Dial-up connections for new systems

Product Codes

Core software SSAs

SSA-SG-IAC025	Any additional software modules must be added to the core software SSA for SSA to be valid
SSA-SG-IAC050	Any additional software modules must be added to the core software SSA for SSA to be valid
SSA-SG-IAC100	SGA software SSA part code for systems Server systems - covers the first 100 x IACs. In addition SSA-SG-IAC100+ must be added in multiples as required to cover additional IACs on the site.
SSA-SG-IAC100+	SSA for Server systems - required for each multiple of 100 etc above SSA-SG-100. Any additional software modules must be added to the core software SSA for SSA to be valid

Version upgrades

As announced in previous bulletins the version upgrade part code will now be made obsolete. Only sites with a valid Software Support Agreement will be able to order the version upgrade CD. This will now be free of charge for the supply of the CD. ADT will need to agree with the client when and how this is to be installed as ADT will need to cover the installation costs etc.

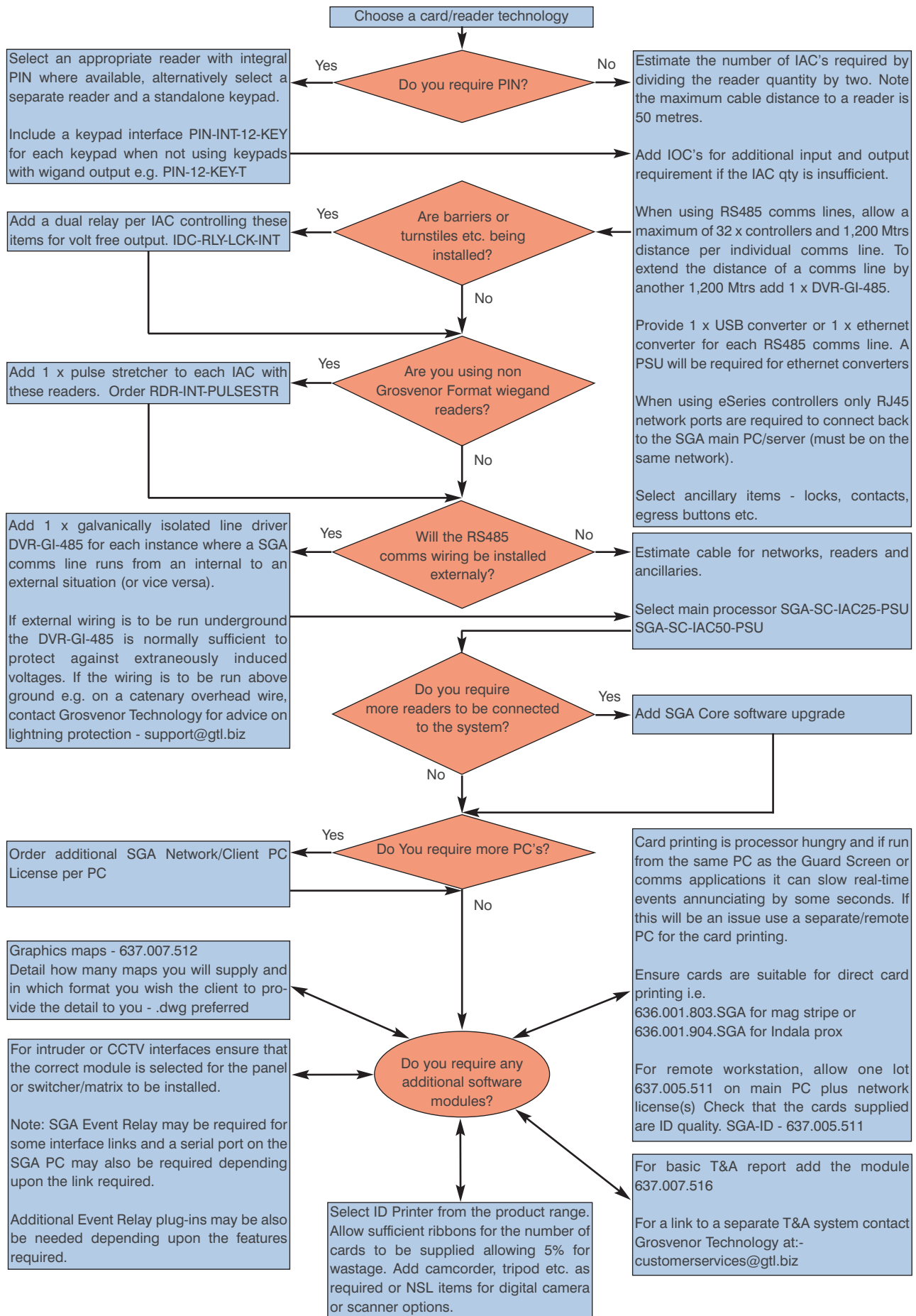
Maintenance Contract.

ADT have decided that only sites with a maintenance contract covering the sites hardware should be offered a SSA. This allows work such as the version upgrade installation to form part of the regular maintenance visit.

Software module SSAs

SSA-SG-BAG-SRCH	Bag search module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-EVT-R-CMS	Event relay Comms module plug-in SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-EVT-R-EML	Event relay module for email feature. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-EVT-R-IVN	IndigoVision integration module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-EVT-RLY	Standard Event Relay module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-GD-TOUR	Guard Tour module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-GXY-DMSN	Galaxy Dimension intruder panel integration module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-PICTURES	Pictures module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-QRW	Queued Report Writer module SSA. Core software SSA must be included with each module SSA for cover to be valid
SSA-SG-VARI-TIME	SGA Vari-Time report SSA. Core software SSA must be included with each module SSA for cover to be valid

SGA Design Flow Chart



Glossary of Terms for Access Control

Access Group Permission programmed into the access control system to allow a cardholder to enter certain doors at specified times.

Active Card An access control proximity card, which is powered by a battery within the card or keyfob. Be aware that batteries have a limited life span and in most cases cannot be replaced - hence the customer will need to budget for replacement within the life expectancy of the system.

Anti-Pass Back (APB) is a facility where card readers are programmed as IN or OUT of a controlled area. Cardholders can enter an area BUT the card cannot be used at any other IN reader to the same area until the card is "seen" by the system to leave the area. This stops duplicate use of a card at controlled points.

Asset Tagging Usually managed by active tags and long range readers/door loops. Asset tagging provides tags, which are suitable for fixing to items such as laptops, projectors etc. Tags can be static (for fixed location items - works of art) or portable. Some have additional features such as tamper, so that the tag cannot be removed whilst within the secure area before the item is taken off site.

Barcode Low cost and low security means of providing access control. Commonly seen in libraries. Two methods of barcode are available - open (as seen in library books) which can be copied and reproduced giving no security at all and Obscure, which has a panel over the barcode stopping copying.

Biometric Reader Uses a part of the human body to identify the user fingerprint / retina scanner etc. Most give a Wiegand output and can be integrated with our systems subject to test.

Card Number This is the internal encoded number - as read by the system

Cashless Vending A third party supplied system that allows the employee to use their access control card to purchase lunch, coffee etc. Smart cards are now being promoted for this purpose. Older systems use track 3 of the magstripe - only high output mag-stripe tape is accepted by some suppliers of cashless vending i.e. G2 (formally Girovend).

Clock & Data A card format usually associated with magstripe. This reader output can however be used by proximity and other reader types.

Coercivity This is the term for the resilience of a magstripe. Standard access control cards are Hi Co whilst Bankcards are usually Lo Co.

Dongle Provided with SGA software to stop the software from being duplicated for use on other sites.

Door Forced this is an alarm generated by the access system when the door is opened by unauthorised means break glass box, door override switch or forced entry. Door must be fitted with a monitor contact.

Door Held Open Alarm generated when an access controlled door is wedged in the open position after being opened by authorised means. Door must be fitted with a door contact. Some systems offer local alarm feature prior to a full alarm at a central location.

Door Loop (reader) This is a cable placed around the doorframe, within the floor or ceiling to create a larger aerial for a proximity reader. Used for Hands free access and/or asset tagging.

Door Loop (for lock) Flexible conduit either surface or concealed at the doors hinged side to transfer power and monitoring to a lock or electric release.

Duress Code/PIN By changing the PIN code used by the authorised person to enter the site. An alarm may be generated at a central location identifying that the user has gained access whilst under duress. Access at the door is gained without any local alarm being generated.

Ethernet The most popular standard for networking information technology equipment. Devices are addressed using TCP/IP protocol.

ELH Ethernet Line Header Used by SGA to connect a network of controllers to the central PC via either a dedicated security LAN or customers own LAN/WAN. The ELH provides the RS485 protocol required for the SGA comms line.

Fail-Safe or Fail Unlocked Term for a lock that requires power to lock - power fail releases the door. Not suitable for perimeter doors. Ideal for fire exit routes as a fire alarm input and breakglass box can release the door to meet fire officers requirements. All face to face mag locks are fail safe. Not suitable for very secure areas.

Fail-Secure Term for a lock that requires power to operate and allow the door to be opened. Motor locks and solenoid bolts are typical examples. Mechanical override is required for means of escape to meet the fire officer's requirements.

Graphics Available on SGA. Customers site drawing are either produced or taken from CAD file. SGA uses bitmap files for Graphic maps - which can be site photos etc. Icons can then be added for monitored/controlled points, which are animated to show their status.

Grosvenor Format Grosvenor Format is a wiegand output suitable for direct connection to an IAC. A non Grosvenor Format reader will miss some card reads and cause cards to be presented multiple times before it will be read by the reader. When non Grosvenor Format wiegand readers are being used an in-line pulse stretcher will convert standard wiegand output into Grosvenor Format wiegand.

Hall Effect Monitoring built in to some magnetic locks to ensure that the holding force is up to the specified levels. Provides monitoring to overcome the typical methods of reducing holding force - grease, film etc - making forced entry much easier.

Hands Free The use of long range readers/Door loops with active tags to monitor the movement of personnel and assets.

Hi Co Type of magnetic stripe tape - see Coercivity

IAC Intelligent Access Controller for SGA. Supports two card readers (with or without keypads) and all necessary inputs/outputs for monitoring etc. Auxiliary inputs and outputs for local devices are also provided. The controller is boxed with power supply and tamper feature as standard. Controller will support 12,000 or 65,000 cardholders.

IOC Input-Output Controller for SGA. Provides supervised input monitoring and clean contact outputs for local alarm management of non-access control devices.

ISO Cards A card, which meets the dimension requirements for credit cards. Used for Photo ID printing etc. Available for proximity technologies.

Keyfob Proximity tag supplied in a form that can be put on to a key ring.

LAN Local Area Network. An IT data communications network for a local geographical area. This may be within one building or a cluster of buildings on a site/campus.

Line Header A device to change SGA Comms into a format suitable for RS485 transmission e.g. USB Line Header and Ethernet Line Header. These are sometimes called converters.

MiFare Smart card chip which can be used for access control. Each chip has a unique number, which can be read by an access control system - or a sector of memory within the chip can be programmed with an access control number for use by the system

Glossary of Terms for Access Control (cont'd)

Monitored Access control door or similar that has a contact fitted to it to show its position/status. Contact can be either magnetic or built in to the lock/release - separate magnetic contact is preferred.

Magstripe Contact form of access control - the magstripe is run past read heads within the reader. Low to medium security as the cards can be duplicated.

MDUI2 Multi-Drop Universal Interface. Used with SGA to convert/split or boost RS485 Comms lines.

Modem A device used to convert data (usually RS232) into an analogue format for transmission over telephone lines - and then converts back again. One Modem required at each end of line.

Parallel port Required for a printer to be connected to a PC.

Passive Card A proximity device, which is powered once the card/tag enters the proximity reader field. There is no on-board battery - therefore read ranges are reduced BUT there is no battery to replace.

Photo ID Adding a photograph and printing other details onto an ISO card. This can include customer's company logo etc.

PIN Personal Identification Number. Used with keypads - should be considered for use in addition to any reader technology at the perimeter of a site to reduce the risk of lost cards being found and used by unauthorised person(s).

PIR Passive Infra Red. A technology, which uses the bodies, heat to detect presence and then generate a signal. Can be used for hands free egress control - t.REX. Note any heat sources can be detected by a PIR.

Protocol Converter A device used to change data formats - from a PC's serial or USB port to that required by the controller communications port.

Proximity Card/reader technology which is contactless.

Pulse Stretcher Grosvenor Format is a wiegand output suitable for direct connection to an IAC. A non Grosvenor Format reader will miss some card reads and cause cards to be presented multiple times before it will be read by the reader. When non Grosvenor Format wiegand readers are being used an in-line pulse stretcher will convert standard wiegand output into Grosvenor Format wiegand.

Release Electrically operated keep for either a mortice or latch lock.

Rim Release Surface mounted door release used with rim locks (like the Yale 88).

RS232 Industry's most standard form of serial interface. All PC serial ports transmit RS232. When using fibre drivers - transmit RS232 and then convert at the remote location. Without drivers, RS232 has a very short transmission distance - approx. 15m.

RS422 Standard comms protocol for SGA. Requires two pairs to transmit and receive. This format extends the communications line up to approx. 1,200m.

RS485 Standard comms protocol for SGA. Requires one pair to transmit and receive. This format extends the communications line up to approx. 1,200m.

RTE Request to Exit. Push button or PIR device that releases the door.

SGA Siteguard Access. Tyco manufactured PC based access control system, which supports up to 250,000 card holders and 5,000+ readers. The system can support multiple reader technologies on one system via hard wired networks, LAN/WAN. Systems can have multiple PC connections for system management.

Serial port RS232 port usually found on a PC - required to interface with some other products e.g. Galaxy Dimension.

Shear lock A magnetic lock that is fitted into the transom of the door enabling the door to swing through. Therefore door alignment on closing is critical. When locked the lock has shear pins, which fit into that armature to increase the holding force.

Site Code Part of a card number that can be specific to a site or customer. Used by older systems to save on memory restrictions or limitations of the system. Not used by SGA.

Smart Card ISO style card, which contains a microprocessor and memory. Card can be used to store data for access control and third party applications - cashless vending etc.

Suppression Required for mains, telephone lines and data runs that are between buildings.

T&A Time & Attendance. Record employees' on/off site time and can link to payroll systems. Should be kept separate from the access control system - card compatibility only is the best solution.

TCP/IP Transmission Control Protocol/Internet Protocol. A layered set of protocols that allows sharing of applications among PC, workstations and network controllers (Ethernet Line Header).

Tag A proximity access control device - usually of the "clamshell" type - not a card or keyfob.

Tailgating Entering the secure area by following an authorised user through a door.

Timezone A period of time which can be given to a cardholder to grant access of assigned to other functions on the access control system

Track 2 Standard magstripe cards have three tracks - 1,2, & 3. Track 2 is the most commonly track used for access control. Track 3 is the approved track for "read/write" - used for cashless vending etc.

T.REX Egress PIR specifically designed for access control. The PIR can be directed to release the door only when a specific area (door handle or push plate) is touched.

USB Line Header Used by SGA to connect a network of controllers to the central PC via a USB port. The USB Line Header provides the RS485 protocol required for the SGA comms line.

Watermark Special mag stripe tape produced by Thorn Secure Science. Used by the MoD & BT. Two versions are generally used, 10 character and 9 character LRC.

Wiegand A high security card and reader technology using alloy wires twisted and set into a card insert. These produce a binary number. Wiegand is also a format generally used by proximity readers - 26 bit being the industry standard. Suppliers generally have their own secure formats available.

European Distribution Centre - Echt, Holland:
(Warehousing/Distribution/
Purchasing/Customer Service/
Call Centre Helpdesk)
Voltaweg 20
6101 XK
Echt
Holland
Tel: +31 475 371 666
Fax: +31 475 371 660
tfseu.service@tycoint.com

European TSP Technical Support Call Centre
Toll Free: 00800 CALL TYCO or
(00800 22 55 89 26)
9:00 to 19:00 CET
8:00 to 18:00 GMT
7:00 to 17:00 EET

UK Distribution Centre
(Warehousing/Distribution/Purchasing)
Dunhams Lane
Letchworth
Hertfordshire
SG6 1BE
United Kingdom
Tel: +44 (0) 1462 667 700
Fax: +44 (0) 1462 667 777
tfsuk.service@tycoint.com

tyco

*Fire &
Security*

The right is reserved to modify or withdraw any product or service without notice

a vital part of your world

© 2011 Tyco International
PMCO21B Iss 4 02.11

www.tycoemea.com