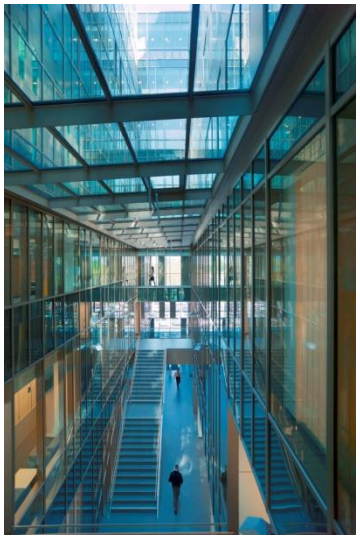
SIEMENS



Integrated Access Control, Security and Video Surveillance System

A&E Specifications

MP 2.76 SP1

Smart Infrastructure

07.2019

Copyright

Technical specifications and availability subject to change without notice.

Edition: 07.2019

Contents

1 System Description

The Integrated Access Control System's (ACS) primary function shall be to regulate access through specific doors, gates or barriers to secured areas of the facility. It shall also have the provision of capturing cardholder images and producing access cards used to provide this access.

The system shall use a single seamlessly integrated database for both its access control and badging functionality. This integration shall be provided under one operating environment.

The system shall provide a multi-tasking environment that allows the user to run several applications simultaneously. The ACS shall be able to run in conjunction with other Windows applications such as MS Word and Excel while concurrently annunciating on-line access and security alarms and monitoring information.

All system application modules, features, and functions shall be generated from a single source code set. In addition, the source code must be designed using object-oriented software development techniques and compiled into native 32-bit and managed code applications. There shall not be separate source code bases for access control and ID badging. All system features and functionality listed in the proceeding pages shall ship with each system. Features and functionality available to the "Owner" shall be determined through licensing and shall be controlled by a software license key. The "Security Contractor" shall work with the Owner to develop and configure the system.

The access control software must offer a high-security solution, based on digital certification. The authentication between the client and server shall be done through certificates using the x.509 standard with authorization through user logon credentials. A Certification Authority (CA) signs the certificates for the server and remote clients, and allows authentication during installation and all operations to ensure there is no manipulation of the data during transmission. It is also possible to use Self-signed Certificate for easier installation, or a Machine Certificate for more advanced and robust installation.

2 Glossary of Terms & Abbreviations

ACS	Access Control System The ACS incorporates the entire access control and security network, including the Server, Workstations and Intelligent field or system controllers.
ISC	Intelligent System Controller The hardware components of the system to which the physical components (input devices, entry devices, and output devices) of the access control system connect. The ISC communicates with the ASC Server.
MMI	Man Machine Interface Also known as the Graphical User Interface (GUI)
NIC	Network Interface Card
DRIM	Dual Reader Interface Module
SRIM	Single Reader Interface Module
GEM	Graphics Editing Module

3 Compliance & Standards

3.1 The “Tenderer” shall be regularly engaged in the manufacturing, installation and maintenance of ACS systems and shall have a minimum of ten (10) years of demonstrated technical expertise and experience in the manufacture, installation and maintenance of ACS systems similar in size and complexity to this project. The tenderer shall also be a maintained service organisation consisting of at least ten (10) competent service people for a period of not less than ten years and be able provide a list of five projects, similar in size and scope to this project, completed within the last five years.

3.2 The Intelligent System Controllers (ISC's) shall comply with at least two standards from the following compliance regulations:

- CE
- C-Tick
- UL

The purpose of these regulations is to maximise the operational useability of the product and to ensure minimum standards within the access control system development have been maintained. These standards will also ensure electromagnetic interference between electronic products are minimized as these may diminish the performance of electrical products or disrupt essential communications.

4 Installation

The ACS shall be designed, installed, commissioned and serviced by manufacturer employed, factory trained personnel.

All materials supplied by the Security Contractor shall be new and shall comply with the latest published specifications and recommendations of the manufacturer in all respects unless otherwise indicated. The Security Contractor shall supply the latest model available for all equipment items. Unless otherwise indicated in the specification, all electronic equipment shall be a standard, unmodified production model.

Equivalent products may not be substituted for previously approved products unless the Architect has approved a written request from the Security Contractor. All requests for substitute equipment must reflect a complete description of the proposed substitute equipment, including manufacturer's technical descriptions, drawings and technical performance.

The Security Contractor shall be responsible for providing complete and operational subsystems, including but not limited to all hardware, software, wire, cable, conduit and boxes, power circuit connections, terminal blocks, labour, management, engineering, training, testing, relocation adjusting and connection to NIC work and devices.

5 System Requirements

5.1 System Architecture

The system shall be of a Server / Client architecture with the option to configure the Server and client ACS software on different PCs residing on the same computer network. Full network functionality shall be available over remote links between the Server and any workstation, using the following protocols:

- NetBEUI
- IPX/SPX
- TCP/IP

Dial-in capability from remote workstation to the Server using a remote access service shall also be available.

Encryption between the Server and each Client is configurable and safeguarded using IPSec, to ensure the integrity and security of the data transferred.

5.2 Server

The ACS Server shall be capable of operating on an IBM compatible computer with the following minimum system requirements:

Operating System	
	Windows 10 (Professional, Enterprise)
	Windows 8.1
	Windows Server 2019*
	Windows Server 2016
	Windows Server 2012 R2
	Windows Server 2008 R2
	Windows 7 (Professional, Enterprise) SP1
ODBC	
	SQL 2017
	SQL 2017 Express
	SQL 2016
	SQL 2016 Express
	SQL 2014 SP2
	SQL 2014 SP2 Express
	SQL 2012 SP2
	SQL 2012 SP2 Express
RAM	8 GB
Hard Drive	1 TB or more
Monitor	1920 x 1080
Network	Ethernet 100/1000 Mbit
Processor	Intel Core i5 or higher (Recommended: 5th Generation or above)

Standard mouse, keyboard, and colour monitor

5.3 Workstation

Workstations shall be capable of operating on an IBM compatible computer with the following minimum system requirements:

Operating System	Windows 10 (Professional, Enterprise)
	Windows 8.1
	Windows Server 2016
	Windows Server 2012 R2 (64-bit)
	Windows Server 2008 R2 (SP1)(64-bit)
	Windows 7 (Professional, Enterprise) SP1 (32-bit & 64-bit)
RAM	8 GB (Recommended)
Hard Drive	160 GB
Monitor	1920 x 1080
Network	Ethernet 100/1000 Mbit
Processor	Intel Core i5 or higher (Recommended: 5th Generation or above)

Standard mouse, keyboard, video card and colour monitor

6 IT Security

6.1 Latest Security Standards

The ACS shall be capable of meeting current market standards of IT security to pre-emptively counter threats in order to provide customers with a highly secured solution having Intellectual Property (IP) and Cyber Security threat protection, data protection and encrypted data transmission throughout the network.

The system shall include the following

- Card Reader (128 bit AES encryption with DESFire)
- Reader Controller (AES up to 256 Bit)
- Server Controller (AES 128 Bit)
- OSDP encryption between controller-reader
- DesFire EV1 encryption for access cards
- RESTful Servers
- HTML 5
- Mutual Authentication between Server and Clients
- Verifies the message has not been changed during transmission
- Clients with no direct database connection
- Permission checks when a client establishes a connection to server

The ACS manufacturer must make updates to the ACS to mitigate potential vulnerabilities that should be identified through continual threat and risk analysis process including penetration testing.

6.2 Mutual Authentication through Digital Certificates

The ACS shall be able to authenticate Server and Clients by using digital certificates. These digital certificates must allow the server to authenticate the connecting clients and verify that any subsequent messages from client to server can be verified to ensure there was no manipulation of the data during transmission.

The ACS shall offer easy to use certificate management process that allows for either customer based certificates to be used or for creation of self-signed certificates. The certification management utility must be able to update certificates or block specific clients, if required.

7 Intelligent System Controllers

The system shall be configured with the ACS software connected via an Ethernet link to any configurable number of Intelligent System Controllers.

7.1 IP Connected Door Controller

The ACS shall support IP connected door controller to help in reduction of overall cost for installation and maintenance; and enable strong autonomous operations of field equipment through peer to peer communications.

The controller shall be capable of controlling up to two doors, supporting FLN devices and hosting of units such as the 8IO, OPM and IPM, while enabling standard features like distributed intelligence, IP addressing of doors, state-of-the art technology and modern design.

7.2 Distributed intelligence

The system shall employ a distributed architecture so that all access decisions are made locally at the Intelligent System Controller (ISC). All decisions to grant access shall be made by the local ISC.

An Intelligent System Controller (ISC) shall link the ACS software to all other field hardware. It shall provide full distributed processing for access control and alarm monitoring operations. Access levels, hardware configurations and programmed alarm outputs assigned at the administrative workstation shall be downloaded immediately to the ACS software. All access granted/denied decisions shall be made at the ISC to provide fast responses to card reader transactions.

The ISC shall be required to operate in a stand-alone and peer-to-peer mode in the event it loses communication with system software. It shall continue to make access granted/denied decisions and maintain a log of events. Events shall be stored in local memory, and then uploaded automatically to the system when communications are restored.

Furthermore, an individual ISC shall be able to communicate with another ISC to distribute cardholder locations and to perform scheduled and alarm events.

7.3 Ethernet Communications

The ISC shall communicate with the ACS via any standard WAN / LAN communications link. The ISC shall provide integrated onboard port for direct Ethernet connection. This connection shall not be an RS-485 communications channel that has simply been converted into an Ethernet connection using a “Terminal Server” or similar conversion device.

The ISC shall be IP addressable and support standard TCP/IP transmission.

7.4 Dial-up capabilities

The system shall be capable of communicating with remotely located ISCs using dial-up modem connectivity. The system shall provide the capability to download database changes to such a controller incrementally.

The ISCs shall also provide the additional functionality of dialling into the ACS Server to communicate alarm events, and other events deemed severe enough for this activity. All other transactions that occur at the remote ISC shall be stored in its internal buffer until that buffer reaches 80% capacity or the server requests the buffer contents, at which point the ISC will upload the entire contents of its transaction buffer.

7.5 Redundant Communications

In the case of main communications line failure with the host system, the ISC shall be able to activate an alternative communications method. This alternative method will be activated automatically and ensure that all critical events and alarm messages are forwarded to the host.

7.6 Internal Memory

The ISCs will be supplied complete with internal non-volatile memory. This memory will allow all program, access permissions, time schedules and the current date and time data stored in the ISC memory to be retained during periods of power failure. The purpose is to ensure the ISC returns to full operation after the event of absolute power failure. In addition, the ISC memory will not require the connection of a battery to permanently store system information.

7.7 Expandable Memory

The ISCs will support the installation of an expandable memory card. This memory card will be used to increase the overall capacity of the ISC and allow the backup of programmed and transaction data locally for recovery immediately following a power failure.

7.8 Local Alarm Input and Output

The ISC shall support the onboard direct connection of a tamper input. This input connection shall be reserved for connecting a tamper switch of the equipment cabinet in which the ISC has been installed.

Upon the Tamper input being triggered the ISC shall also provide a local output that is capable of connecting an output device that can be triggered as a result of cabinet tempering.

7.9 LED diagnostics

As a minimum the ISC shall provide at LEDs that can be easily viewed for diagnostic purposes. These LEDs shall indicate the state of power and communications at any given time.

7.10 Dual Reader Interface Module

A Dual Reader Interface Module (DRIM) shall be available for each controlled door and provide the ability to connect up to two card readers or entry devices. This DRIM shall:

- Monitor the door position (door contact)
- Allow the connection of a Request-to-Exit (REX) switch for exit
- Control an electric door lock or strike
- Provide the facility for up to 3 auxiliary input devices to be connected
- Allow the connection of an alarm buzzer that can be triggered in the case of an alarm event, or more specifically locally trigger a buzzer for a door held event before this alarm is registered at the host.

All events that occur at the door must be reported from the DRIM to the ISC.

To allow for situations where an entry and exit reader may be required at the one door a DRIM will allow two readers to be connected. However, in circumstances where a door shall only require one reader the DRIM can be configured to operate in a two door mode, whereby a reader, door lock and door monitoring device can be connected for each door.

In addition, the DRIM shall also provide connection for single advanced reader that connects via an RS-485 or Wiegand / Clock/Data connections.

Finally, the DRIM shall also provide the ability to work offline in cases where communications with ISC has have been lost and still continue to accept a set of specified cards as being valid to the door(s) which it controls.

7.11 Single Reader Interface Module

A Single Reader Interface Module (SRIM) shall be available for each controlled door and provide the ability to connect a single card reader or entry device. This SRIM shall:

- Monitor the door position (door contact)
- Allow the connection of a Request-to-Exit (REX) switch for exit
- Control an electric door lock or strike
- Provide the facility for up to 3 auxiliary input devices to be connected
- Allow the connection of an alarm buzzer that can be triggered in the case of an alarm event, or more specifically locally trigger a buzzer for a door held event before this alarm is registered at the host.

All events that occur at the door must be reported from the RIM to the ISC. In addition, the SRIM shall also provide the ability to work offline in cases where communications with ISC has have been lost and still continue to accept a set of specified cards as being valid to the door(s) which it controls.

7.12 Eight Reader Interface Module

An Eight Reader Interface Module (ERIM) shall be available for each controlled door and provide the ability to connect up to eight separate card readers or entry devices. This ERIM shall:

- Monitor the door position (door contact) for each door
- Allow the connection of a Request-to-Exit (REX) switch for each exit
- Control an electric door lock or strike for each door
- Provide the facility for up to 16 auxiliary input devices to be connected
- Allow the connection of an alarm buzzer that can be triggered in the case of an alarm event, or more specifically locally trigger a buzzer for a door held event before this alarm is registered at the host.

All events that occur at any door must be reported from the ERIM to the ISC.

To allow for situations where an entry and exit readers may be required at a door the ERIM will allow two readers to be used for single door control and provide the possibility to uses the following combinations of door control:

- Eight single reader doors
- Six single reader doors and one dual reader door
- Four single reader doors and two dual reader doors
- Two single reader doors and three dual reader doors
- Four dual reader doors

The ERIM shall also provide connection for up to eight advanced readers that connect via an RS-485 or Wiegand / clock/data connection.

The ERIM shall also provide emergency override that supports wire supervision, to ensure that false fire override conditions are not triggered.

7.13 Input Control Module

A hardware module shall be available to independently monitor up to 32 alarm input devices and report line fault conditions, alarm conditions, power failure and wire supervision. When an alarm input is activated, the condition shall be reported to the ISC and subsequently to the ACS host. The same module shall also provide the ability to connect up to four control devices and support emergency override capabilities.

The emergency override shall additionally support wire supervision, to ensure that false fire override conditions are not triggered.

7.14 Elevator control module

A hardware module shall be available to monitor up to 16 independent input devices and reports line fault conditions, alarm conditions, and power failure. When an alarm input is activated, the condition shall be reported to the ISC and subsequently to the ACS workstation. The same module shall also allow the control of up to 16 output devices that can be controlled via the change in state of an input (monitor point) or a command received from the ACS Server. These outputs shall support fire override operation.

The emergency override shall additionally support wire supervision, to ensure that false fire override conditions are not triggered.

7.15 Input / Output control module

A hardware module shall be available to monitor up to 8 independent input devices and reports line fault conditions, alarm conditions, power failure, and wire supervision. When an alarm input is activated, the condition shall be reported to the ISC and subsequently to the ACS workstation. The same module shall also allow the control of up to 8 output devices that can be controlled via the change in state of an input (monitor point) or a command received from the ACS Server. These outputs shall support fire override operation.

7.16 Diagnostics

Each ISC and hardware module shall provide a series of visible Light Emitting Diodes (LEDs) that display the status of the controller or module, and can be used as visual diagnostic indicators. As a minimum, the following diagnostic LEDs should be available:

- Communications
- Monitor point (input) status
- Control point (output) status
- Power

7.17 Housings & equipment tamper switches

All access control hardware components shall be housed in a lockable metal cabinet that is fitted with equipment tamper switches and meets the appropriate environmental requirements. The ISC shall allow the connection of equipment tamper switches to detect access to security equipment and shall consist of a spring loaded switch assembly. Any movement of the cabinet door shall cause the switch contacts to transfer. Tamper switches shall incorporate SPDT contacts and be mounted within each cabinet containing security equipment such that the switch cannot be disconnected or disabled from the cabinet exterior.

7.18 Firmware Download

All access control hardware components shall be supported by a built in firmware download and configuration utility from the ACS. This utility shall be included within the MMI and not via an external dedicated tool only.

8 Communications

The system shall use TCP/IP communications techniques over Ethernet, whilst employing proprietary communications protocols. The encryption between the ACS host and each ISC shall use implementation of the Advanced Encryption Standard (AES) to encrypt all messages and ensure data security.

8.1 ACS communications

The connection between the ACS Server and each MMI workstation shall use standard Ethernet communications.

The communications protocol to transfer messages to or from the ACS Server to any MMI workstation in the system shall be of a proprietary nature to the manufacturer providing the highest level of security.

In addition, the communications protocol shall allow an encryption mechanism to be configured, that ensures the transfer of data cannot be interpreted.

8.2 ACS / ISC communications

The connection between the ACS Host and the ISCs shall use standard Ethernet communications. All communications between the ISCs and sub-devices shall be based upon the standard RS485 transmission techniques using a proprietary protocol.

The communications protocol to transfer messages to or from the ACS Host to any ISC in the system shall be of a proprietary nature to the manufacturer providing the highest level of security.

In addition, the communications protocol shall incorporate an error checking routine that checks the integrity of the messages that are transferred on this line.

8.3 ISC communications

The connection between an ISC and a series of entry devices using Reader Interface Modules (RIMs), or system extension boards shall use standard RS485 communications techniques. The communications protocol to transfer messages to or from the ISC to any connected device shall be of a proprietary nature to the manufacturer providing the highest level of security possible.

In addition, the communications protocol shall incorporate an error checking routine that checks the integrity of the messages that are transferred on this line.

Each ISC shall be capable of communicating with at least 96 of these devices at any one time, using four separate channels to co-ordinate the communications process and share the load across different channels.

9 Man Machine Interface (MMI)

As a minimum the ACS shall provide the ability to connect up to 140 workstations to the server. Each workstation shall have the capability of displaying an easy to use MMI, from which all system operation, including programming, control and operation can be accomplished. The MMI shall employ a standard Windows look and feel and provide both an intuitive menu and button driven navigation system.

9.1 On-line help

The MMI shall provide a comprehensive on-line help system, which shall be available at anytime and from any screen. The help system shall describe the use of all system functions and provide a comprehensive glossary of terms. In addition, the help system shall provide the standard windows help contents listing, index listing and key word or phrase search functionality.

9.2 Navigation

The MMI shall use standard Windows controls, including:

- Mouse control
- Menu functionality
- Button navigation
- Keyboard equivalent mouse shortcuts

9.3 Toolbar Customization

The MMI shall use allow for the customisation of an operator specific toolbar. This shall provide the ability to create a custom toolbar that only includes those buttons (links to parts of the ACS) that are most commonly used or required for the operation of the system.

In addition, the operator shall be able to display the look and feel of the toolbar buttons that allow them to perform tasks quickly and efficiently including the text size and placement and size and position of icons displayed.

9.4 Windows look and feel

The MMI shall support a user friendly, Windows Graphical User Interface (GUI) that shall be intuitive. All messages and interface text shall be in English prose unless another language has been specified and installed. All functions shall be either keyboard or mouse driven to allow the System Operators to choose the method of navigating through the screens. In the alarm-monitoring module of the system software, all major functions (opening a door, acknowledging alarms, etc.) shall be accomplished using a minimum number of mouse clicks.

The operator workstation interface software shall minimise operator training through the use of language prompting, on-line help, and industry standard PC application software.

9.5 Languages

The system shall support the installation of multiple language versions.

In addition, the manufacturer shall be able to provide the tools to translate the ACS into other languages as may be required.

9.6 Installation

The MMI and ACS shall use standard Windows installation processes and employ a software installation that is similar in look and feel to other Windows applications.

The installation licensing shall allow for the selection of software installations that cater for the size and functionality of the facility at which the system is being installed. As a minimum the following package types should be available as default:

- Basic
- Intermediate
- Advanced

10 System Operators

The system will only permit authorised operators, who have been given permissions to log on to the ACS at a workstation, to administer aspects of the system. The functionality available to these operators shall be fully configurable via the comprehensive partitioning architecture.

10.1 Authentication

The system shall request an operator's user name and password before entry to the MMI is granted. The password must be fully encrypted on-screen to prevent it from being easily copied. The MMI will not be displayed until the identification of the operator has been verified and access to the ACS is granted. Authentication may be based on a pre-defined time schedule for certain groups of operators.

10.1.1 Authentication Rules

It shall be possible for the following configurable logon rules to apply to each account:

- Password age
- Password Length
- Logon retries
- Complexity

Finally, it may be possible for the operator to change their own password or for authentication to be performed using the standard Windows logon identification. Therefore the currently logged in Windows User's details can be used to verify their permission to log into the ACS.

10.2 Partitioning

Operator specific password access protection shall be provided to allow the user/manager to limit workstation control, display and database manipulation capabilities as deemed appropriate for each user, based upon an assigned password. Operator privileges shall "follow" the operator to any workstation logged onto (an unlimited number of operator accounts shall be supported).

The System shall employ an application partitioning design so that applications are broken into separate distinct programs capable of running independently to other System applications. Applications shall include, but not be limited to, alarm monitoring, system administration & configuration, cardholder management, graphics, ID card printing, and cardholder forms designing modules. Each client workstation shall have the ability to be installed with any combination of the above listed modular applications.

The system shall allow partitioning to be assigned on the basis of the following conditions:

- Cardholders
- System Functions (minimum of 70 feature levels)
- Holidays
- ISCs
- Field Devices
- Custom Pages
- Time Schedules
- Site Plans
- Reports

The system shall prevent the currently logged in operator from viewing the details, regarding any alarms triggered by a system component to which they have not been assigned privileges, including:

- Audit trail alarm entries
- Audit trail reports, which include alarm details
- Audible and visual alarm annunciation

The alarm information associated with any system component to which an operator has been assigned privileges will be displayed.

The system shall allow partitioning to be assigned on the basis of audit trail reports. The currently logged on operator shall only be able to create or run those reports to which they have been assigned privileges.

The system shall also prevent the currently logged in operator from printing reports that include those system components to which they have not been provided privileges.

10.3 Privilege levels

When assigning a function to an operator, the system shall allow the level of assignment to be specified. These levels include:

- **Read only** This type of privilege level does not allow the operator to create or modify components in the specified area of the system. However, they are allowed to view those records.
- **Modify** This type of privilege level does not allow the operator to create components in the specified area of the system. However, they are allowed to view and make modifications to existing records.
- **Full** This type of privilege level allows the operator to create, modify and view components in the specified area of the system.

10.4 Operator profiles

The ACS shall support multiple operator profiles such that preferences are retained for individual operators, irrespective of the workstation that they log onto. The display colours and data layout shall be configurable (and be saved) per operator.

10.5 Operator journal

A system operator journal shall be available to log important daily events. The operator is required to select a journal subject from a pre-defined list. The ACS shall allow an administrator to set the names to comprise this list of subjects. The system shall also allow all journal entries relating to a particular subject to be recalled and viewed on-screen, printed or both.

10.6 Workstation auto-lock

All ACS workstations shall automatically lock if left idle for a configurable period of time - requiring the operator to identify him or herself by re-entering their password. The operator shall also have the capability of manually locking a workstation at any time. Any system initiated or manual workstation locks shall be logged in the ACS audit trail.

10.7 Default Accounts

At installation the ISC shall be automatically configured with default operator accounts. These accounts shall be defined in such a way that they reflect the standard duties of different operators that can be expected to use the system.

11 Cardholders

The system shall include a cardholder management component that is integrated with the access control system. The system must support at least 500,000 cards – all of which are downloaded and retained in the memory of each ISC. This cardholder management functionality must allow the enrolment of cardholders into the database, capturing of images and import/export of employee data. This functionality shall also allow a system operator to assign or modify the access rights of any cardholder.

11.1 Cardholder data

As a minimum, the ACS shall allow configurable fields to be customised by the system administrator to suit the needs of the facility owner. The system shall provide a Graphics Editing Module (GEM) that gives operators the ability to modify any standard field to customise the cardholder screens as desired. Once these fields have been defined, the ACS shall not permit these (database) fields to be changed.

In addition it shall be possible to add cardholders to the database without assigning a card to that cardholder.

11.2 Searching

The system shall allow the search of all programmed cardholders, based on the criteria supplied by an operator. Operators shall only be able to search and retrieve cardholder records to which they have assigned privileges.

As a minimum, the search criteria shall include:

- Card number
- Name (first and / or last)
- Work Group
- Title
- Address
- Contact Numbers (phone, mobile, and pager)
- Payroll Number
- Vehicle Details (registration, colour, model)

Searching shall not only be limited to entire word matches. An operator may also search for cardholders by entering data that appears in the beginning of a word or string.

If more than one cardholder in the system meets the specified criteria, the operator shall be displayed a list of all matching records, from which they can select a particular record.

When search results are returned, the operator shall be able to dynamically re-sort the information displayed so that appears in a useful order (for example, by last name). When selecting an individual record to expand, it shall be possible to keep the search dialog active so that other cardholder records can be opened at a later time if required.

11.3 Cardholder images

The ACS shall support the capturing of a high quality image of a cardholder from any workstation. The system operator shall have the option of capturing images in real-time or alternatively by importing an existing image.

If capturing images in real-time, the operator shall be able to use an appropriate capture card or use a USB digital video camera. If cardholder images already exist, the operator shall be able to import images of all standard formats including jpg, bmp, gif, and tif.

Once an image has been captured or imported, the operator shall be able to preview in full colour, the cardholder image complete with the card, as it will appear when printed. The Operator shall have the ability to crop and resize the image and adjust the brightness and contrast.

The cardholder image shall be able to be recalled at any time from any workstation to verify the identity of any cardholder on the facility.

11.4 Cardholder Fingerprints

The ACS shall support the capturing of high quality finger prints and encoding the finger print into the card during enrolment process that is native of ACS.

Also the ACS shall allow operators to capture and store the fingerprint to the ACS database. The fingerprints shall be captured using a biometric reader and an enrolment reader shall be used for fingerprint encoding.

11.5 Cardholder Signatures

The ACS shall support the capturing of cardholder signatures from any workstation. The system operator shall have the option of capturing signatures in real-time or alternatively by importing an existing signature.

If capturing signature in real-time, the operator shall be able to use a USB signature capture pad. If cardholder signature already exists, the operator shall be able to import images of all standard formats including jpg, bmp, gif, and tif.

11.6 Card Trace

The ACS shall record the last visited access point (with date and time) for every cardholder. A special trace function shall be available for operators to track activity of specific cardholders. When the trace has been applied, all card activity relating to that cardholder will be highlighted in the audit trail. A report may also be generated that details the locations visited by the traced cardholder.

11.7 Grouping cardholders

The ACS shall allow the grouping of cardholders into specific configurable entities. This shall facilitate voiding of a large number of cards with a single action and also assist with operator partitioning.

11.8 Cardholder violations

The system shall monitor every card presented at each reader in the system and prevent access at the reader (door) if any of the following access violation conditions exist:

- The card has not been assigned access permission at the current time.
- The card has not been assigned permission at the reader.
- The cardholder has been voided in the system.
- The cardholder belongs to a group of cardholders that has been voided.
- Entry to or exit from an area governed by anti-pass back control has been violated.
- A card belongs to a group of cards that has been disabled.
- A card was presented at a reader that has been disabled or taken out of service.
- The card has been presented before its allocated start date, or after the card's designated end date.
- The card presented does not belong to the site, which includes an invalid card number, an invalid site number or a card containing an invalid facility code.

In addition, a message will be logged in the audit trail indicating the card use violation, and if configured, a visual and audible alarm will also be displayed.

11.9 Cardholder Data Import / Export

The system shall provide an external software tool that can be used to import or export cardholder data from another application via text file.

This manipulation of data shall be governed by the same login rules applied to a standard operator of the system and shall also be capable of synchronising data over a period of time.

The system shall also provide an automatic synchronization tool that allows changes to be automatically bought in the ACS. .

11.10 Cardholder Changes

It shall be possible to display all changes made to a cardholder record within a specified date range so that record can be reversed to a previous status from any point in time.

11.11 Multiple Cards per Cardholder

It shall be possible to define up to 5 cards for each cardholder in the system and have an independent void or active status for each card and the overall cardholder.

In addition, it shall be possible for each card assigned to the same cardholder to be of a different card technology and for each card to have separate access permissions.

11.12 Inactive Cardholders

It shall be possible to effectively park cardholders by removing a card from their current identity profile. Whilst this data will still remain in the ACS the cardholder will still be considered inactive and not count toward any overall licensing structure or otherwise.

11.13 Custom Cardholder Information

The ACS shall provide an integrated tool for creating custom cardholder information. This shall provide the ability to add the following information types to a cardholder custom page:

- Textbox
- Dropdown List Box
- Date Calendar
- Group Box
- Dialog Labels
- Custom Button
- Attachments Box

In addition, design of custom pages shall be simple drag and drop functionality with automatic page guides for aligning already placed components and the ability to individually change the parameters of each component selected.

Finally, it shall be possible to import or export custom pages using an xml format.

11.14 Cardholder Watchlists

The ACS shall provide the ability to import information regarding any cardholder on a watchlist from a government agency or otherwise

When an operator attempts to enrol a cardholder into the ACS that matches the information already contained in a watchlist, the ACS shall generate an alarm that alerts the operator that a match has been recognised and further action may be required.

This match shall include general cardholder information or may even include custom cardholder information

12 Assignment of access

The system shall allow an infinite number of combinations of access permissions to be assigned to any cardholder programmed in the system. The system shall allow access permissions to be assigned to access points, areas, elevator floors, groups and venues.

In addition, the system shall provide the ability to schedule the times during which cardholder access to each separately allocated resource is permitted.

Access shall also be extended to output points, whereby a cardholder presenting their access badge not only unlocks a door, but can also easily change the state of any output in the system.

Upon changing or assigning access to any cardholder, the details shall be immediately propagated to all on-line ISCs.

Access privileges shall be assignable on the following basis:

- Access based upon access group privileges
- Access based upon personalized privileges
- Access based upon a venue booking privileges
- Access based upon offline doors
- Any combination of the above

13 Time Schedules & Holidays

The ACS shall allow up to 65,000 configurable time schedules to be defined. Each time schedule can consist of up to 20 independent time periods including up to 8 holidays. For ease of configuration, the operator shall be able to select from week days, weekends, or specify a particular day or time. The ACS shall have the intelligence to check whether the time periods are valid and not conflicting with existing credentials.

A time schedule can be configured to include or exclude holidays. Upon changing a time schedule record, the ACS shall immediately propagate the appropriate changes to all affected ISCs.

14 Card Readers and Cards

Card Readers shall read encoded data from the access card and transmit that data back to the ISC. The card reader or entry device should give an audible and visual indication of each read.

14.1 Supported cards and technologies

The system shall be compatible with all major card and access entry technologies, including (but not limited to):

- Proximity cards and readers
- Biometric readers
- Bar code cards and readers
- Magstripe cards and readers
- Wiegand cards and readers
- Smart cards and readers
- Optical cards and readers
- Transmitter and infra-red cards and readers
- Keypads and PIN pads

In addition, the ACS manufacturer shall be able to provide a number of different encoded card technologies, which use sophisticated algorithms. These algorithms shall be proprietary in nature to the manufacturer, and should be sophisticated enough that they increase the security of the installation. The support for these formats will be in addition to any format perceived to be an industry standard. These shall include at least one proprietary format in each of the following:

- Bar code
- Magstripe
- Wiegand (output protocol)
- Smart Card
- RS-485
- Clock & Data

14.2 Ability to produce cards with bar codes, magnetic stripes, smart cards

The system shall be able to create and print either magstripe, bar code, or smart cards using an integrated printing function.

When creating bar code cards the user must have the option to choose the type of barcode that suits their facility. The user should be able to specify the bar code ratios, character length and position on the card.

14.3 Ability to support multiple cards

As a minimum, the ACS system shall support the use of at different card technologies. As such, each tenant within an allotted environment may bring their own card technologies with them.

14.4 Ability to support MIFARE smart cards

The ACS system shall support the use of MIFARE smart card technology. As such the system shall provide the ability to encode smart cards including the ability to program the following:

- Specify a custom format including length, facility, company, card number and parity.
- Program each sector / block on a MIFARE (1K and 4K byte) smart card for access control and non-access control applications
- Specify sector keys and the way in which these keys interact with the sector for the reading and writing of information
- Specify the output type and data type of the information stored on the card
- Program database information for each block / sector

The ACS system shall also support the ability to read an entire smart (1Kb and 4Kb) card based upon a pre-configured profile. This card reading shall provide a dedicated viewing screen from which the currents contents of all blocks and sectors can be viewed on-screen.

14.5 Ability to support DESFire and DESFire EV1 smart cards

The ACS system shall support the use of DESFire smart card encoding technology. This option shall support a wide range of smart cards. The ACS shall provide the ability to encode DESFire smart cards including the ability to program the following:

- Specify a custom format including length, facility, company, card number and parity.
- Program each Application / File on a DESFire (2K, 4K and 8K) smart card for access control and non-access control applications
- Encryption Key for the smart card
- Length of data written on the card, Output format, Access Control, and the Data Type to be encoded on to the smart card.

14.6 Ability to support Custom Wiegand cards

The ACS system shall support the use of proximity card technology with a custom wiegand format including the ability to program the following:

- Specify a custom format including;
  - Length
  - Facility Code
  - Company Code
  - Card number
  - Revision
  - Parity
- Provide a graphical means of specifying the format details

14.7 Enrollment

It shall be possible to connect standard card readers to the ISC workstation directly using a free USB port for the purpose of automatically capturing the card details during the cardholder enrollment process.

14.8 Ability to support iClass cards and readers

The ACS system shall support the use of iClass technology natively (e.g.; not just via a wiegand connection) including the ability to perform the following:

- Support for HADP iCLass readers
- Support for access control via CSN or iClass ID
- Ability to display appropriate status messages on those readers with an LCD screen

15 Host Event Processing

The ACS shall be capable of processing events in the system as they occur, and distributing this information throughout the entire access control and security network.

15.1 Immediate propagation

Changes made using the ACS software shall be automatically recorded to the ODBC compliant database and downloaded to the correct ISC(s) using the appropriate communications channel. In addition, the ACS software shall also provide the tools to manually download all appropriate database information, allowing the full initialisation of each ISC.

All database changes shall be performed while the workstation is on-line without disrupting other system operations.

Changes made at the ISC equipment shall be automatically uploaded to the ACS server, to ensure system continuity. Each ISC shall be capable of reporting all changes in status, system events, and actions performed, to the ACS in real-time. These messages shall be displayed immediately in the ACS audit trail. The affect of each message must be reflected throughout the system as they occur, such as, the immediate changing of the colour of a symbol located on a site plan to indicate a change in point status.

15.2 Local event buffer

The ISCs shall maintain a buffer of all events that occur locally. This buffer shall store all messages until they are uploaded to the ACS server. If the communications between the ISC and the ACS server are lost, the buffer will be retained until communications is restored, at which point all logged events shall be uploaded to the ACS server.

15.3 Database accessibility

All System data must reside on a single database on the network and must be accessible in real-time to every / any system workstation. This shall allow for automatic change propagation to all workstations on the system as well as a common database to consolidate all information and allow for better disaster recovery.

16 Real time Audit Trail

The system shall log all events that occur to both an on-screen audit trail window and a retrievable database record. These events must be logged on-screen as they occur (in real-time). All system changes, alarm events, entry / exit conditions, point state changes, exception messages, miscellaneous system messages, or any information relating to the access control system in general shall be logged to this audit trail.

16.1 Partitioned display data

The system shall be capable of filtering all displayed audit trail messages based upon the currently ‘logged in’ operator’s assigned privileges. Only those events to which the operator has been assigned privileges will appear on-screen or any audit trail report printed whilst that operator is logged on.

16.2 Operator audit trail profile

The system shall allow the operator to select which information columns are displayed and which information columns are not displayed on-screen in the audit trail window. The system shall also allow the operator to change the width of any displayed audit trail column by simply using the mouse to drag the column wider.

The system shall allow the operator to select the colours in which certain events are displayed in the on-screen audit trail window. The operator shall also be able to select the background colours displayed behind these entries. As a minimum, the system shall allow the following audit trail component colours to be configured:

- Alarm message text color
- Normal message text colora
- Alarm message background colour
- Normal message background colour

In addition, it shall be possible to display each alarm with an individual alarm color, this will allow alarms of a similar to type to be instantly recognised.

16.3 History View

The system shall provide the ability to switch to an audit trail history mode that allows history events to be easily searched. This view shall allow events to be searched based upon any text contained in the audit trail messages that have been recorded.

16.4 Event short-cuts

The system shall facilitate a quick link (short-cut) from any event appearing in the audit trail. As a minimum, there shall be a link to the cardholders and the point location relating to the audit trail event. This will enable easy access to the respective record, allowing the operator to change the details of that record, if necessary.

16.5 Dual window

The ACS shall allow any operator to scroll through past events without losing the ability to monitor new events. This shall be easily achieved via a split-pane audit trail window. Both viewers shall display all events as they occur. The upper viewer shall allow the operator to scroll-back and view previous events that have occurred at the facility, but have scrolled off screen as other events are logged. The lower viewer shall display the latest logged events at all times.

The two viewers shall be separated by a movable partition that allows the operator to change the viewable area by simply using the PC mouse. In addition, the system shall allow the operator to select the number of entries that are retained in each on-screen viewer at any time.

Any older events that cause the viewer to exceed the configured entry limit, will be removed and must be logged to a permanently stored log-file that can be recovered by creating an audit trail report.

The currently logged in operator shall also be allowed to determine the order in which events are displayed (i.e.: latest event appearing at the top or the bottom of the audit trail).

16.6 Real-time audit trail printing

The ACS shall allow the system administrator to configure the type of events to print to a dedicated printer in real-time. The administrator shall have the option of selecting to print all events or only alarm events. This can be in addition to displaying the events on-screen.

16.7 Filtering and Search

The MMI workstation shall allow the audit trail messages displayed on-screen (in history mode) to be searched using a full text search field. In addition, should be possible to filter the displayed records.. The filter options will include, but will not be limited to:

- Date and Time
- Type and Category of event
- Point Information
- Group
- Name
- Employee ID

16.8 Change Tracking

The Audit Trail shall detail each database change made within the system, including the data that was changed and a record of the operator who made that change.

16.9 Custom Audit Trails Views

The ACS shall provide the ability for an operator to create a custom Audit Trail view that includes the following features:

- The customised view should update in real time as transactions occur in the system
- Multiple custom views shall be permitted at any point in time
- Ability to filter information displayed (for example may only display messages from a select group of doors)
- An operator shall be permitted to share views (configuration of) with other ACS operators
- Ability to configure a view with special trace conditions such that any important event in the system is displayed with identifying colors. For example, whenever a specific door is unlocked a message should appear in green
- Any view shall support the configuration of multiple trace conditions at any time
- It shall be possible to print the custom view at any system printer

17 Advanced Alarm Management

The ACS shall provide an advanced alarm management system. This system shall allow the visual and audible annunciation of alarm events as they occur, in real-time. The annunciation of an alarm shall take priority over all other system functionality to ensure the alarm is registered immediately upon occurring.

17.1 Alarm annunciation

The system shall provide an audible and visual annunciation of all appropriate alarm situations as they occur. Each alarm annunciation shall be configurable, so that it requires positive action to be taken by the System Operator when acknowledging it, and always appears in the foreground of the MMI.

Immediately following the visual and audible annunciation of an alarm, a field shall become available where the system operator can enter comments regarding the alarm situation, and shall prevent the alarm from being cleared until an entry in this field has been made. Once entered the System Operator shall be allowed to acknowledge the alarm.

In addition, pre-defined alarm responses shall be available. These responses are specific to the facility and can be selected from a drop-down list to ensure quick and efficient acknowledgement of an alarm situation, in lieu of typing a message.

After an alarm has been announced, the system shall allow the operator to silence the alarm for a selected period of time. After this time period has elapsed the alarm annunciation will be regenerated.

Upon an alarm being announced, the System Operator shall be provided with the facility to view an alarm queue before taking further action. Alarms with the highest priority shall be placed at the head of the queue. As a minimum the alarm queue will display the following alarm attributes:

- Priority of the alarm
- Date and Time at which the alarm occurred
- Name of the system component that caused or initiated the alarm
- Current status of the system component that caused or initiated the alarm

The system shall provide the ability to outline unique emergency instructions to be specified for each type of alarm. These instructions should be displayed on request before the alarm is actioned, in order to help the Operator understand the requirements and necessary routines for clearing the alarm. These alarm instructions should be able to contain any combination text or graphics and if appropriate contain a windows video (*.avi) that can be played on request of the system operator.

In addition, these instructions should appear in a dialog that allows the system operator to enter a log in relation to the alarm and acknowledge the alarm, whilst simultaneously viewing the instructions.

17.2 Visual alarm graphics

The system shall be configured so that the activation of any alarm provides text and audio instructions outlining the procedures to follow in responding to the alarm, at the Alarm Monitoring Workstation and automatically calls up associated maps upon grabbing the alarm.

The alarm-handling portion of the system shall provide dynamic colour alarm graphic maps. These maps shall allow the operator to respond to and clear alarms from the alarms graphics screen.

The system shall allow the creation of colour graphic floor plan displays and system schematics for each piece of equipment, including card readers, inputs (monitor points), and outputs (control points) to optimise system performance, analysis and speed alarm recognition.

The MMI shall allow users to access the various system schematics and floor plans via a graphical penetration scheme, menu selection or text-based commands.

The system shall allow the equipment state to be changed by clicking on the point block or graphic symbol and selecting the new state. In addition symbol colours shall be used to indicate status and change as the status of the equipment changes.

Real-time, dynamic graphical maps will mean that the map screen will not have to re-paint or refresh each time a new alarm or event condition occurs.

17.3 Multimedia alarming

The system shall extensively integrate and use multimedia throughout the ACS. The system shall provide owner customisable voice alarm annunciation and a flashing coloured system icon for each alarm in the System. In addition, the System shall provide customisable voice instructions so that each alarm or event in the System can have both sets of text instructions and/or pre-recorded audio voice instructions.

17.4 Alarm re-activation

The ACS shall allow each alarm to be configured with an internal timer that re-activates the alarm annunciation if the change in status that initially caused the alarm to be announced has not been rectified. This timer shall only accompany those alarms where the status of the system component can be restored to a normal state.

17.5 Alarm Queue

The ACS shall place each outstanding alarm in a queue with the highest priority alarm at the top of the queue. The alarm queue shall be able display different alarms with unique colours to allow for easy and quick identification of any outstanding alarm.

In addition, each entry in the queue as a minimum, will display the alarm location, its current status, and the date and time at which the alarm first occurred. The alarm queue will also provide the ability to clear alarms when necessary.

17.6 Alarm configuration

The ACS shall allow each alarm to be fully configurable. As a minimum the System Operator shall be able to configure alarms in response to changes in state or messages received from the following system components:

- Access Points
- Areas or zones
- Communications
- Elevator floors
- Input points
- Output points
- Intelligent System Controller (ISC)
- Interlocked Door Groups
- External System Points

As a minimum, each alarm created shall allow the operator to define the following attributes:

- Whether or not the alarm is required to be acknowledged when announced
- Alarm priority, with up to 7 priority alarm levels
- The colour of each alarm priority level
- Instructions to be associated with the alarm
- Sound to be played when the alarm is visually announced
- Alarm re-activation time
- State change or event that will trigger the alarm or return the system component to normal
- Description of each status
- Symbols to represent the alarm and normal status of the component on a graphical map

The system shall also allow alarms to be forwarded to an alternative alarm handling solution. The methods in which alarms can be forwarded include:

- To a mobile phone using SMS
- To a pager
- Via email
- From one ACS server to another (in the same security network and communications structure)
- To an OPC (Alarm and Events) compliant system

18 Printers

All printers can reside on the same network as the access control and security system.

18.1 Dedicate printers by function

The system shall be capable of configuring dedicated printers for each specific task that requires the use of printed results. As a minimum the system shall allow the following printer types to be specified:

- Audit Trail printing
- Card printing
- Plan printing
- Report printing

18.2 Reports

The system shall be capable of configuring a dedicated printer specifically for the task of printing audit trail, database, or operator journal reports. This facility shall provide the selection of a default printer for this task and the ability to change the printer characteristics to suit the printing requirements.

18.3 Real time printing

The system shall be capable of printing all audit trail entries as they occur, using a dedicated printer specifically for this task. This facility shall allow the filtering of audit trail messages that are printed, including alarm messages only or all messages. In addition, the system shall allow the printer type used to be selected, be it 132 column, 80 column, or other printer types.

18.4 ID card printing

The system shall support any card printer with industry standard Windows drivers. It shall support double-sided full colour printing, edge to edge printing with the additional ability to encode magnetic stripes or bar codes on cards.

18.5 Plan printing

The system shall be capable of configuring a dedicated printer specifically for the task of printing graphical site plans. This facility shall provide the selection of a default printer for this task including the ability to select the following type of printers:

- pen plotters
- inkjet printers
- bubblejet printers
- laser printers
- electrostatic printers

The ability to change the printer characteristics to suit the operator’s requirements shall also be available.

19 Archiving System

The system shall be capable of archiving the programmed database information, the logged audit trail data, operator journal entries, graphics, alarm sound files, alarm instructions and custom designed reports. Once archived, the system shall provide the tools required to restore this data at a later time if necessary.

19.1 Archiving medium

The system shall provide the ability to select the location of the archived data, be it using a local hard drive, another hard drive located on a machine in the same computer network, a floppy drive or any other mass storage device as deemed acceptable.

19.2 User-definable archiving parameters

The archiving facility shall allow the operator to select what information is to be stored. When archiving database information, the operator should be able to independently or collectively select the following information for storage:

- All programmed database records
- All system graphics, including site plans, symbols, alarm instructions and drawings
- System parameters
- Operator profiles
- Cardholder images
- Reports

Upon restoring the archived data, the system operator shall have the same flexibility in choosing which components are to be restored if more than one component was part of the archived file.

When archiving audit trail information, the operator should be able to independently or collectively select specific dates for storage. Upon restoring the archived data, the system operator shall have the same flexibility in choosing the dates for which audit trail entries are to be restored.

In addition, the operator shall be able to choose whether to encrypt the backed audit trail data.

19.3 Automatic Archive

The system shall provide the mechanisms to create an automated backup. This will allow a backup schedule to be implemented for the ACS data and will include scheduling for one off date and time, day of the week, or monthly. In addition it shall be possible to specify the type of data to be automatically archived

20 Reporting

The system shall be capable of providing detailed reports through a specialized application within the main GUI. This application provides reports regarding the information contained in the database, audit trail, or operator journals, without the need for programming skills.

The system shall provide the capability for the configuration and set-up of a specific system printer for printing reports, and allow the use of network printers. The system shall also exclude those records from any report to which the currently logged in System Operator has not been assigned privileges to view.

20.1 Available Reports

The list of reports shall be available in a tree view sorted by functional area of the system, whereby individual report views can be easily selected and displayed within the MMI. As a minimum the system shall supply at least 50 pre-defined reports in the following functional areas:

- Alarm Information
- Hardware Components
- Time Schedules
- Groups (hardware / cardholders)
- Access Definitions
- Site Plans
- Cardholders
- Audit Trail Messages
- Event Routines
- External Devices (eg: CCTV)
- Holidays
- Elevators
- Operators
- Mustering
- General

The report view MMI shall be displayed within an independent window to the ACS main operation window so that the reporting function never takes away focus from the audit trail view or other important access control information being displayed on screen,

In addition, it shall be possible to hide the tree view navigation pane to maximise the area on screen in which to view the data associated with the report selected.

20.2 Report sort and filtering

Once displayed, each report can be filtered and information ordered as required. The main functions that shall be available to customise the current view of a displayed report shall include as a minimum:

- Customised column view (order columns, add new columns, remove columns)
- Column order (alphabetical sort order – ascending / descending)
- Information Grouping (Group information based upon data in a column, including hierarchical grouping)
- Key word filter (filter any information in a column based on a key word including wild card characters etc.)
- Automatically size columns for the information displayed

20.3 Design custom report views

The system shall provide the tools necessary for the operator to create custom reports regarding information in either the audit trail or database. This customization shall allow the following selection criteria as a minimum:

- Customised report creation wizard
- Custom report name
- Report type selection (for example: cardholders)
- Selection of column information to be displayed (for example: first name, last name)
- Filtered criteria (for example: first name = John) with more than 15 different filter types (equal to, greater than, etc)
- Ability to add additional filtered criteria including logical operators (and / or / and not / or not)
- Addition of the new custom report to the tree view for easy and permanent selection

20.4 Print to reports printer

The system shall provide the functionality to configure and setup individual printers for each different system task that may require printed results. This includes the ability to configure a printer specifically for the purpose of creating printed reports. In addition, the printer configuration shall allow for the setup of local or network printers for these tasks.

20.5 Print reports automatically

The system shall provide the tools to automatically generate reports, based upon a defined schedule without operator intervention. These automatically generated reports shall be saved to disk and can be viewed at any later time while still saved.

20.6 Print Preview

It shall be possible to provide a print preview on screen with the option to change the printer settings so that the view can be customised by the operator before printing.

20.7 Report Export

It shall be possible to export the data contained within a report to the following data formats:

- Microsoft Excel (.xls)
- Tab delimited (.txt)
- XML (.xml)
- Comma delimited (.csv)

20.8 Report Layout

Finally, where applicable it shall be possible to dynamically change the report layout on screen by selecting an appropriate current view. For example, when creating a report based upon cardholders it shall be possible to view layouts based upon a list, by card status, alphabetical order, grouping, or with photograph. Once selected, the screen will reflect the layout chosen.

20.9 Interactive Reporting

The ACS shall provide a report with an interactive functionality. As a minimum, interactive reports shall permit the following:

- Ability to create a complex report based on any information contained within the ACS
- Alternatively, it will be possible to import reports from an external source
- Each interactive report will provide the facility for a set of conditions to configured for the report information (e.g.: date > mm/dd/yyyy)
- Perform functions on any information that meets the criteria selected. These functions shall include voiding a cardholder.
- Functions shall be activated manually by right clicking or automatically upon report analysis by the ACS.

20.10 Unused Cards

The ACS shall provide a mechanism to remove unused cards from an active state in the system.

The length of time which defines an unused card shall be configurable.

The ACS shall allow a report to be generated that lists all cards that at the time the report was generated the cards listed were considered unused.

It shall be possible to directly from right clicking on entries in the report to void any or all unused cards as seen applicable by the operator who produced the report.

The ACS shall also provide the ability for unused cards to be automatically voided in the system at a regular interval (for example, on a weekly basis), without the need for operator intervention.

21 Scheduling

The system must provide the capability for an operator to define specific times, during which certain events and system control will occur. The system must be capable of handling at least 65,000 distinct time schedules. These schedules must be operator customisable, so that, they can schedule events across an entire week, with up to twenty distinct time periods during that week. Primarily, the time schedules must be able to handle holidays, provide access at certain times, and schedule or permit events during the specified times.

21.1 Holidays

The system must be capable of defining over 100 holidays in advance of them occurring. A defined holiday will override the normal timed schedules where configured and allow other system functions to behave as normal.

21.2 Public floor access

The system must be capable of scheduling specific times when access to floors in an elevator system are taken ‘off’ security and are accessible to the general public. At all other times the system shall secure those floors and provide access only to valid cardholders.

21.3 Access per door

The system must be capable of scheduling specific times when a cardholder is permitted to access a specified door, barrier or gate. At all other times the cardholder will be prevented from gaining access at that door.

21.4 By specific date & time

The system shall be capable of scheduling certain programmable events to occur on specific dates or during specific times of the day.

21.5 By certain event

The system shall be capable of scheduling certain programmable events to occur in response to the activation of another event or system status change. The event or status changes that trigger this response shall be fully configurable.

22 Anti-passback

The system shall be capable of providing anti-passback control, whereby, a cardholder that uses their card at an entry reader must not be able to re-enter until they have first exited using the specified exit reader. The system must also be capable of operating in either a soft or hard anti-passback mode

The anti-passback control should also be flexible so that cardholder's that have violated anti-passback rules or have lost their access card can be forgiven by a system operator.

22.1 Soft Anti-passback

The system shall provide the selection of a soft anti-passback mode, which permits entry at a door or barrier (to a valid cardholder) when the anti-passback rules have breached. However, the system will still generate an alarm in response to this anti-passback violation.

22.2 Hard Anti-passback

The system shall provide the selection of a hard anti-passback mode, which does not permit entry at a door or barrier (to a valid cardholder) when anti-passback rules have been breached. In addition this type of breach will also generate an alarm.

22.3 Peer-to-Peer Anti-passback

The system shall provide full anti-passback capabilities across multiple ISCs without the need to consult the ACS host. This will allows full anti-passback capability even when communications with the host has been lost.

In addition, peer-to-peer anti-passback operation shall provide a fail-safe mode, whereby entry or exit to a secure area will be permitted when communications between controllers has been lost.

22.4 Mustering Area

The system shall provide the facility via the anti-passback functionality to designate specific mustering areas. These areas shall allow reports to be generated that display all those cardholders currently logged into that area.

22.5 Area Limits

The system shall allow each area to be defined with a maximum cardholder count. Once this limit has been reached the area will be considered as being "Full". Once the full capacity has been reached, the system shall allow:

- The prevention of further cardholders from entering the area
- The triggering of an output device, for example a "Parking Lot Full" sign

22.6 Cascading Anti-passback

The system shall allow single reader doors to be created within an area. These doors will not fall under normal anti-passback control, however, entry will not permitted unless the anti-passback conditions assigned to the surrounding area have been previously observed.

22.7 Four Eyes Access

The system shall allow an area to be nominated as a “Four Eyes” location. An alarm in a four eyes location shall be raised when a single cardholder has entered that location and resided within the location for a specified amount of time without a second or subsequent cardholder entering. A four eyes area will also allow an alarm to be raised when no cardholders reside within the location.

22.8 Timed Re-entry

The system shall allow an entry point(s) to be nominated as a timed re-entry point. Once a cardholder has used their card at a timed re-entry access point, that cardholder will not be permitted to re-use their card again to gain access to that location within a specified time period.

22.9 Door Interlocking

The system shall allow the configuration of a set of interlocked doors, such that opening any single door within the defined set prevents any other door from being opened at the same time, even if a valid cardholder attempts to gain entry at that door.

In addition, it shall be possible define a time period once the first door has been closed, before another door in the set can be opened.

22.10 Dual Custody

The system shall allow the configuration of a door such that it can only be opened if two valid cardholders present their access badge at the door within a defined time period. This mode shall also allow for supervisory access (eg: visitor escort) and an override function based upon cardholder so that cardholders of an authorised level do not require a subsequent cardholder before entry is permitted.

22.11 Clustering

Finally, the system shall allow the configuration of a set of controllers in a single group for the purpose of anti-passback configuration. Whilst both local anti-passback and global anti-passback operation shall be available, this subset allows a group of controllers to monitor anti-passback within their own cluster.

This type of clustering shall also allow cardholders to maintain a current count in separate anti-passback locations. For example, when a cardholder leaves their car in the carpark the increased count because of that card remains raised, even if the cardholder enters another anti-passback area that is managed across multiple controllers.

23 Parking Lot Management

The system shall allow a parking lot or similar location to be configured, whereby; entry to that location is governed by access privileges set in the system.

The system shall count the number of entries and exits from that location and when the specified limit has been reached, will raise a visual and audible alarm and prevent any further cardholders from accessing the parking lot. The system should also be capable of triggering an event when the car park limit has been reached, allowing a sign or other visual indicator to be turned on.

The system will allow entry into the carpark based upon groups of cardholders. Each group of cardholders can be configured with a capacity that applies only to that group. In addition, the system shall be capable of raising alarms when the group has violated the anti-passback limit assigned to them.

A dynamic screen shall be available that lists all cardholders who have entered the carpark and the date and time during which they entered. In addition, this screen will also show count for each group of cardholders that have been set a limit for the area.

The system must also be capable of producing a report that provides the details of all cardholders with a vehicle currently parked within the parking lot.

24 Intrusion Detection

The system shall have the ability to provide intrusion detection. When the system has been armed, any detection point that is breached will automatically raise a visual and audible alarm.

24.1 Intrusion Capabilities

The intrusion detection system shall provide as a minimum the following capabilities:

- Automatic zonal arming and disarming based on a pre-defined schedule.
- Independent arming and disarming of discrete zones within the facility.
- The last cardholder to leave the facility shall be able to automatically arm the entire facility when they arm their specific zone.
- The system shall allow zones to be graphically depicted on a site plan that indicates their current status in real-time.
- Configurable entry and exit timers, that allow passage prior to alarm activation.
- Cardholder specific override privileges on alarm points (sectors) that cannot be secured because that point is in an alarm state at the time of activation.
- The system shall intelligently handle zones, so that any locations within that zone, which are also common to other system zones, are not armed till all the associated zones have already been armed. This intelligence shall allow the securing of the entire facility and intruder alarm detection system.

24.2 Sectors

The intrusion detection shall be capable of including many sectors (detection devices) in multiple zones. Each of these zones should be able to be independently or collectively controlled by the assigned cardholders.

24.3 Grace Period

The system shall be capable of sounding an audible alarm during the entry or exit period, to alert the user that they can now enter or exit the detection zone without generating a nuisance alarm. This entry or exit time shall be customisable.

24.4 Arming

The system shall provide entry and exit devices that allow users to arm or disarm a zone (group of detection devices) as they exit or leave a facility. This entry / exit device, shall display provide the necessary tools for the cardholder to make the appropriate selections and carry out the task of arming or disarming.

24.5 Part Arming

The system shall provide the ability to arm part of an intrusion area, such that the perimeter points become armed, but the internal intrusion points to that area remain unarmed.

25 Duress

The system shall allow cardholders to indicate whether they are requesting access under a forced or duress situation and thus communicate a potential emergency to the ACS. When such a duress action has been registered, the cardholder will be permitted access and a duress alarm will be announced on the system, without arousing suspicion.

In addition, the system shall allow the configuration of a duress button, which, when triggered shall raise a visual and audible alarm at each ACS workstation.

26 Security Programming

The ISC or the system controller shall have a Programmable logic engine allowing security programming and control.

The security control shall be presented to the operator through a user-friendly graphical designer. The programmable security control shall operate like a programming logic engine running in a controller. This feature shall give the ACS operators an ability to construct logical activities using the graphical designer. The logical activities shall then be executed by the controller

The programmable security control shall allow the operator to visually design activity programs in the system and download them to the controller. The operators shall be able to customize activities for multiple triggers, and resulting effects via the graphical designers.

As a minimum, the ACS's security programming shall make the following features available:

- Enabling users to create and design customized, site-specific activity programs for their site, without having to contact vendors for related firmware modifications
- A Single ISC or controller shall execute multiple programmable activities simultaneously. A single programmed activity shall be executed from multiple ISC's.
- The programmable activities shall be controlled and executed by Time Schedules
- A variety of entities like Access, Input and Output point, Access Events, Intrusion Areas, Anti-Passback areas, Workgroups, and Floors shall be supported.
- Virtual Components like flags, timers, counters shall be incorporated as triggers and effects.

27 Time and Attendance Recording

The system shall be capable of recording the entry and exit of cardholders at designated card readers or groups of card readers.

Once recorded the system shall allow for the export of the time and attendance information to a third party T&A or HR application. This export shall be available in a “.CSV” or “tab delimited” format to a pre-defined file location and file name.

In addition, the exact information contained within the export file shall be selectable and extend to at least the following required information:

- First Name
- Last Name
- Date of record
- Time of record
- Location that the record was logged

28 Elevator Management

The system shall be capable of providing access control and security for both high-level and low-level elevator systems.

28.1 Low-Level

The low-level elevator management shall provide floor access control, with the ability to provide security during nominated times (after hours) and general access during busier times of the day.

The system shall also provide the mechanism, whereby, a fire emergency or override system can be turned on either automatically via a trigger from another system or manually using the MMI.

In addition, the system shall provide the option of configuring remote access buttons that allow visitors to be granted entry to both the facility and selected floor from a remote location.

The system shall also provide the option of configuring fail-safe or fail-secure operation after power-loss or system reset has occurred.

The system shall only allow one valid floor selection (to a secured floor) each time a card reader is presented at the elevator.

The system shall provide a “Wizard” like configuration for elevator components. This will ensure the quickest possible method for adding elevator floors to the ACS.

28.2 High-Level Interface

The High-Level elevator management shall provide the ability to connect the access control and security system to an Elevator Management System (EMS) using a high-level interface.

This interface shall provide the ability to allow security during nominated times (after hours) and general access during busier times of the day. The system shall also provide the mechanism whereby a fire emergency or override message can be sent to the EMS.

Connection to the Elevator EMS shall be via an RS-485, RS-232, or RS-422 wired connection.

The system shall be flexible enough to allow communication to any Elevator EMS, with a small amount of interface programming required. This programming will be independent to the ISC firmware and its operation. This shall also allow the ISC to communicate and control access to an elevator system, even in those situations where a custom elevator implantation has been commissioned.

28.3 High-Level interface to thyssenkrupp Destination Control System

The ACS shall be able to interface to a IP based elevator control system and not require any customisation by the customer. This support shall be such that the user Interface (UI) is adaptable, as much as is possible, to multiple lift systems (not concurrent in a single Central Controller instance). It shall also be capable of running on Linux based Operating System and for this initial release, the hardware nominated is the Central Controller.

The UI shall be able to show the configuration options within the elevator system and allow upload, download and editing if the lift system allows it.

Assignment of floor access privileges should be consistent with the existing elevator programming. Customisation for further lift protocols shall be implemented in the ACS software and firmware.

29 Graphics

The system shall support a graphics module that allows the design, import and construction of site plans, drawings, dynamic symbols, alarm instructions and card templates. This graphics module shall support the standard ACS partitioning, to prevent those System Operators without the appropriately assigned privileges from accessing graphical objects.

29.1 Graphical Maps

The system shall allow the design, import, and construction of site plans, which can be used to visually handle alarms, control access, and generally monitor the facility. Each site plan shall be updated dynamically as the status of system components change. The symbol representing each component will automatically update in colour, alerting the operator of its change in status.

The system shall provide a pre-defined library of symbols that represent the most common access control and security components. In addition, the system shall allow the operator to create their own library of symbols that represent the devices installed at the facility.

The system shall provide a built-in suite of graphics tools that can be used to create or modify a site plan. As a minimum, these tools shall include:

- Import of existing site plans, including AutoCAD, bmp, jpg, wmf, tif, and most other raster type images.
- Common Windows text tools, such as alignment, font, and style.
- Colour tools to change the fill and border colour of components in a plan.
- Drawing tools, so that lines, boxes, circles, arcs, and free-hand lines can be drawn.
- Alignment tools, to align separate components in a site plan.
- Shortcuts that add a button to a site plan that, when clicked automatically open a new site plan or trigger a system action, such as opening a door.
- Grid or crosshairs that aid in the alignment and scale when creating a site plan.

Each site plan shall have the ability to unlock a door to allow entry, control points at the click of a button, retrieve point information at the click of a button, and create shortcut buttons to other plans in the system or frequently used system commands.

In addition, the ACS shall allow partitioning for each graphical map. This partitioning shall allow only those System Operators that have been assigned the appropriate privileges to the graphical map, to view it and control points located on that map.

29.2 Symbols and Drawings

The system shall provide a clipart library of access control components and symbols including doors, car park boom gates, and PIRs. The user shall have the ability to add custom symbols or design new symbols for this library. Once created, these symbols shall be able to dynamically change colour in response to a change in status of the component which they represent.

The system shall also allow the importing or creation of drawings that can be used in other parts of the system. The graphical editor will provide the tools necessary to import and add features to these drawings.

30 Control and Monitor Points

The system shall provide a mechanism to define both control and monitor points. These points will allow the system to link input devices with output devices, trigger event generated tasks, and be used to override general system operation through the use of the MMI.

30.1 Monitor Point Parameters

As a minimum, when programming a monitor point in the ACS, the System Operator shall be able to:

- Enter a unique name for each point. This name will be used in Audit Trail messages regarding the status of the monitor point.
- Select the mode of operation for each point from the MMI, based on the desired reporting and general alarm activation for that point.
- Define the specific conditions that cause the point to go into alarm and the type of annunciation parameters associated with that alarm.
- Select the specific delay times for each monitor point programmed in the system.
- Select the time schedule that will be applied to the monitor point.

30.2 Control Point Parameters

As a minimum, when programming a control point in the ACS, the System Operator shall be able to:

- Enter a unique name for each point. This name will be used in Audit Trail messages regarding the status of the control point.
- Select the time schedule that will be applied to the control point.
- Define the specific conditions that cause the point to go into alarm and the type of annunciation parameters associated with that alarm.
- Select the specific delay time for each control point programmed in the system.

31 Event Routines

The system shall allow an Operator to create their own event driven routines based on any required system operation. These event routines shall run automatically without the need for human intervention or the workstation MMI being operational.

The ACS shall be able to trigger event routines from the ACS host or from an individual ISC. Routines initiated by an ICS shall be able to trigger outcomes affecting other ISCs without the need for ACS host intervention. This scenario will allow peer-to-peer routines to run even when communications with the host are lost.

31.1 Event Triggers

As a minimum, the Operator shall be able to configure event routines that can include any of the following individual event triggers:

- System Components, including access points, input devices, and output devices
- Specific time
- Communications channels (lost / resumed)
- Date

31.2 Event Actions

As a minimum, the Operator shall be able to configure event routines that can include any of the following system actions in response to an individual trigger:

- Change the state of any of the following system components; access points, input devices, output devices, and areas.
- Send commands to the CCTV equipment that manipulate the movement of cameras or images displayed on a monitor.
- Start DVR recording processes.
- Send specific commands to a system ISC.
- Automatic program execution. Which includes any executable program on the host PC or that is accessible on the network on which the host PC resides. This should also allow for the inclusion of additional parameters to start that program, if required.
- The control of external third party systems, such as lighting control etc.
- Send messages to mobile phones, pagers or via an email system.

31.3 Host Events

The ACS shall be capable of imitating host based event routines. These routines shall be able to target physical devices, but also extend to communication with third party products such as Windows Applications, CCTV systems, DVR systems etc. The triggering of the majority of these events will rely upon communications of the ACS with the field hardware devices for status information.

31.4 ISC Events

Each ISC shall be capable of imitating event routines. These routines shall be able to target physical devices in the access system. In addition, these event routines shall be able to operate in a peer-to-peer mode. This means that a single ISC can control the operation of a device on another ISC as a direct result of the routine.

The system shall allow an Operator to define a message that will appear in the audit trail when the event is initiated. This message will indicate that the event task has been activated.

31.5 Events via GSM

The ACS shall support the ability to send messages as a result of events triggered in the system via SMS using a GSM modem connected to the system.

32 (Point) Grouping

The system shall be able to collectively group components of the same type for the purposes of controlling those components as a single entity. As a minimum, the components that can be grouped shall include:

- Access points - card readers and other entry devices
- Input devices (monitor points) – detection and monitoring devices
- Output devices (control points)
- ISCs – field controllers
- CCTV monitors
- CCTV cameras
- DVRs
- Elevator floors
- External third party system points

The system shall allow the visual and audible annunciation of a group alarm. This alarm shall be triggered when a pre-defined number of group members have individually initiated alarms within a configurable time period.

33 System Status

The system shall provide a status bar that indicates the current status of system components. As a minimum the system shall be capable of displaying the status of the following components in that status bar:

System messages	All text messages that indicate relevant information to the process currently being performed.
Alarm count	Indicates the number of outstanding system alarms that are waiting to be either acknowledged by an Operator or returned to a normal state.
ISC communications	Indicates the number of ISCs that are currently on-line and communicating with the ACS server.
Workstation status	Indicates the status of communications between the workstation being used by the logged in Operator and the ACS server.
Locked workstation	Indicates when the workstation has been locked, indicating that an authenticity check is required before the workstation can be used again.
Zoom	Indicates the zoom ratio of any graphic that is opened and displayed on-screen.
Date and time	Indicates the current date and time.

In addition, the status bar shall provide short tool tips when the mouse pointer is placed directly over the icons contained in this bar.

A full system status screen shall also be available that provides a summary of points defined in the system. This screen shall be able to provide a summary at a glance providing full system counts. It shall also be able to provide the status of both physical and logical points currently in alarm, including:

- Complete system summary
- Physical points in alarm
- Logical points in alarm
- Door status

34 System Overview

The system shall be able to display a full architecture of the access control and security network in a Windows™ Explorer type view. By simply clicking on any component in the system, the operator shall be able to display the full details regarding that component.

Furthermore, by right clicking on a component the operator shall be able to open its property dialog, from which, its basic properties can be changed.

35 Video Imaging / Badging & Card Printing

The ACS shall include a state-of the-art, 32-bit, ID badge creation and production system that is integrated with the cardholder management system. This shall allow for the creation of different badge types based on a database field and the linking of that field to a badge type to automate the process of credential production.

In addition, the use of security colours, graphic images, photos or signatures shall be supported to allow security officers to quickly identify personnel access authority by the badge design.

The ACS shall incorporate into a single, seamless integrated system, imaging technology and personnel management, which is written from the same source code as the access control and alarm-monitoring functionality. The system shall generate and store personnel records as well as monitor badge use throughout the facility.

The system shall allow badges to be fabricated at any system Workstation, based on data and images that are input and captured at the time of enrolment.

Images are to be digitised using industry standard JPEG image compression, and printed using a direct card printing process. A record for each cardholder shall be created in the badging module of the system by entering the required data. Once all fields have been entered, the system shall store the cardholder's record in the system database.

35.1 Card Design

The System shall provide a badge layout creation and editing facility to allow for the creation of custom badge designs. The System shall support credit card, government, and custom ID card sizes in either a landscape or portrait format.

The ACS shall also allow for the incorporation of bar codes or magnetic stripes onto the card template. This shall be visible at run-time from the respective cardholder record.

35.2 Image capture from Live Video Source

The system shall allow live image capture using a Windows compatible video source including support for USB type image capture devices (using either live video or still digital picture). If required, the image capture shall be able to be performed on any Windows Workstation connected to the ACS.

These captured images shall then be saved to the cardholder’s record in the ACS database with the ability to be recalled at any later time. The system shall also provide the necessary tools to import existing images into each cardholder’s record.

Once an image has been captured or imported to the ACS, the Operator shall be able to crop the image or select the appropriate image aspect to be printed on a card using a simple click and drag graphical mask.

The System Operator shall be able to preview in full colour, the badge, as it will appear when printed. As a minimum, the System Operator shall have the ability to:

- crop images
- adjust the image intensity
- adjust the image contrast
- adjust the image saturation
- adjust the image sharpness

35.3 Cardholder Verification

The system shall allow a cardholder’s record to be recalled from the audit trail window. The System Operator must be able to display a cardholder record with the stored cardholder's image. This feature shall be provided at the MMI, to assist the System Operator in determining access rights of an employee who may have lost their badge.

36 Digital Video Recorder (DVR) Management

The ACS shall be able to provide an interface to multiple DVR units via an Ethernet link. This management of DVRs will allow for the remote surveillance of the facility using the ACS to monitor and control the operation of DVR components.

The DVR functionality shall be available only to those operators who have been granted the appropriate permissions to either configure DVR functions or operate the DVR equipment. The DVR interface shall be an integrated component of the ACS and shall not be a separate application.

36.1 High Level Interface

The DVR system shall be facilitated via a high level Ethernet interface to a range of DVR unit types. As a minimum, the DVR HLI shall support DVRs from the following corporations:

- Siemens SISTORE
- Nexus
- DVTel
- Bosch
- Genetec Security Centre
- Siveillance VMS
- Seetec

36.2 Cameras

The Security Operator shall have full control of all camera functions directly from any ACS workstation. As a minimum, the operator shall have pan/tilt/zoom control, iris control, focus, pan/tilt speed, heater and wiper controls. Camera control shall be via mouse, keyboard or a combination of both and be integrated into the ACS MMI.

36.3 Live video

The system shall allow the operator to view live video input from within the ACS and be able to manually control the appropriate cameras from this view. This shall be achievable via either mouse or keyboard control.

36.4 Multiple Video Matrix Display

It shall be possible for live video to be displayed inside a window that can handle and display multiple live video streams simultaneously in a matrix view. The layout of this matrix shall be configurable so that the operator can select the optimum display setup for streaming live images.

In addition the live video matrix display shall support the drag and drop of cameras images. This means that from a list of available cameras, the operator shall be able to drag the camera name from that list to a video display square in the matrix and the live video from that camera shall appear.

36.5 DVR Configurations

As a minimum, the ACS shall allow the configuration of the following DVR functions directly from the MMI:

Presets A defined, recallable position for a camera. A preset allows a PTZ camera to be automatically moved to a pre-defined co-ordinate position.

Patterns A defined, moveable camera routine. A pattern allows a PTZ camera to continuously move in a pre-defined manner using pan, tilt and zoom functions.

In the case of communications being lost, the ACS shall be able to restore all DVR functions to normal activity when communications are restored.

36.6 Switching in response to certain events

The ACS shall be able to do any of the following DVR actions in response to a specific event:

- switch a camera to a specific monitor
- run a pattern
- run a sequence
- begin recording

36.7 DVR MMI

The ACS shall provide an intuitive easy-to-use operator MMI. This MMI shall be an integrated component of the ACS interface and allow the configuration and operation of the DVR system directly.

When controlling the DVR equipment the System Operator shall be able view live images on-screen in real time. This on-screen display shall allow the System Operator to easily control both PTZ and fixed cameras using the PC mouse. As a minimum, the following DVR control functions should be available using the mouse pointer or left click of the mouse button:

- image display (including specific monitor and camera selection)
- camera movement
- zoom-in and zoom-out
- open-iris and close-iris
- focus-near and focus-far
- pan / tilt speed
- heater control
- wiper control

36.8 DVR Playback

The ACS operator shall be able to playback any recorded event stored on any connected DVR unit by simply selecting the appropriate unit and camera and then entering the date and time at which the event occurred. Once these options have been specified it shall be possible to playback the recorded image within the MMI.

36.9 DVR Playback from Event Log and Reports

The ACS operator shall be able to playback any ACS triggered recording event by simply selecting the appropriate message in either the ACS live event log or any historical report that includes such events. Once selected the ACS shall playback the recorded image within the MMI.

36.10 Video Verification

In conjunction with the DVR unit the ACS shall be able to display a live video signal together with the stored cardholder photograph upon a valid card badge. Using these two images the system operator shall be permitted to allow or deny access to the cardholder attempting to gain entry at the door.

36.11 DVR Alarms

The ACS shall also be able to receive and display within the MMI DVR specific alarms. As a minimum Motion Detection alarms and Video Loss alarms shall be communicated and displayed within the MMI.

36.12 IP Camera Support

The ACS shall support the connection of IP based cameras. It shall support the connection of these cameras via two methods:

- Directly to the ACS without the need for a DVR for video display purposes
- Via a DVR for recording and control purposes

36.13 Support for Input / Output Points

The ACS shall also support the physical output and inputs connected to the DVR system, as a minimum allowing input state changes to be notified, alarms to be registered and the ability to send commands directly to output devices.

The ACS shall support the ability to upload the following configuration from the connected DVR

- Cameras
- IP Camera
- Input Points
- Output Points
- Monitors
- Sensor Points (like motion detection in EDS)

37 DVR System Interface

37.1 DVR System Interface

The system shall support the ability to manage any generic DVR system via the use of an Application Programming Interface (API). This API must be DCOM compatible and execute the same logon routine as if logging on from a standard ACS workstation.

The integration of DVR units using this interface shall still be governed by the standard authentication used by the ACS, and prevent those System Operators from accessing information to which they have not been assigned appropriate privileges.

As a minimum, the DVR API shall provide the following management of DVR units:

- Viewing of live camera images
- Ability to configure multiple DVR units and cameras
- Full PTZ functional control of cameras
- Configuration of alarms that trigger DVR recording events
- Configuration of routines that manage DVR functions
- Audit trail log playback of recorded images
- Display of messages in the audit trail log

37.1.1 The API shall provide the flexibility to communicate with multiple DVR units of different manufacturers.

37.2 Interface integration

The system shall display video images and provide controls within the ACS MMI itself. Whilst it shall be possible to use the image player software provided with the DVR unit, the ACS shall, via the API, provide all the tools necessary to integrate live video, and DVR unit control from its own MMI.

37.3 Tools and Documentation

The system shall come with a complete API guide to assist in creating the required components to manage a DVR unit from the ACS. Sample code shall also be provided with examples of how to most efficiently integrate the ACS with a DVR unit.

38 Guard Tour

The system shall be able to provide guard tour functionality. The guard tour functionality shall be an integrated component of the ACS. It shall take advantage of existing card readers or inputs, to allow a guard to conduct specific tours around the facility using these devices to register their attendance at pre-defined stops and monitor their progress as they conduct their tour.

The system shall be capable of registering alarms to indicate breaches in a tour or notify the System Operator of potential safety conflicts. The guard tour functionality shall allow the user total flexibility over the configuration and programming of guard tours using any combination of access points or input devices that have already been programmed in the system.

As a minimum the guard tour operation shall include the following:

- The Operator must also be able to start tours independently and if required abort a tour already in operation.
- Once a tour is operational, the system must be able to initiate alarms when a guard arrives early, arrives late or fails to arrive at a designated checkpoint.
- An Operator shall be able to print a report that details all the checkpoints to be visited by the guard and the order in which these checkpoints should be visited
- The system shall provide a window from which the movements of guards and the tour, which they are currently conducting, is displayed.
- The system shall allow tour recovery after power failure has occurred.

In addition, the guard tour specifications must meet or exceed the following:

- Allow a minimum of 100 tours to be defined in the system.
- Allow each tour to contain up to 30 independent stop points.
- Allow up to 20 tours to run simultaneously.
- Allow at least 500 guards to be programmed in the system.

39 Visitor Management

The system shall include a visitor management component that is integrated with the access control system. The system must support at least 100,000 visitor cards. This visitor management functionality must allow the enrolment of visitors into the database, capturing of images and import/export of visitor data.

39.1 Visitor data

As a minimum, the ACS shall allow up to 196 configurable visitor fields to be customised by the system administrator to suit the needs of the facility owner. The system shall provide a Graphics Editing Module (GEM) that gives operators the ability to modify any standard field to customise the cardholder screens as desired. Once these fields have been defined, the ACS shall not permit these (database) fields to be changed.

The visitor module shall also enable additional fields not used with other system cardholders including:

- Visited Cardholder – selected from a list of existing cardholders in the system.
- Card Status – card issued to or returned by visitor
- Card issue time and date
- Card return time and date
- Visitor profile
- Visitor's Company
- Reason for visit
- Visitor's driver's license
- Visitor's email address

39.2 Searching

The system shall allow the search of all programmed cardholders, based on the criteria supplied by an operator. Operators shall only be able to search and retrieve visitor records to which they have assigned privileges.

As a minimum, the search criteria shall include:

- Card number
- Name (first and / or last)
- Profile
- Reason for visit
- Driver's Licence
- Email Address

Searching shall not only be limited to entire word matches. An operator may also search for cardholders by entering data that appears in the beginning of a word or string.

If more than one visitor in the system meets the specified criteria, the operator shall be displayed a list of all matching records, from which they can select a particular record.

39.3 Visitor images

The ACS shall support the capturing of a high quality image of a visitor from any workstation. The system operator shall have the option of capturing images in real-time or alternatively by importing an existing image.

If capturing images in real-time, the operator shall be able to use an appropriate capture card or use a USB digital video camera. If visitor images already exist, the operator shall be able to import images of all standard formats including jpg, bmp, gif, and tif.

Once an image has been captured or imported, the operator shall be able to preview in full colour, the visitor image complete with the card, as it will appear when printed. The Operator shall have the ability to crop and resize the image and adjust the brightness and contrast.

The visitor image shall be able to be recalled at any time from any workstation to verify the identity of any visitor on the facility.

39.4 Visitor violations

The system shall monitor every card presented at each reader in the system and prevent access at the reader (door) if any of the following access violation conditions exist:

- The card has not been assigned access permission at the current time.
- The card has not been assigned permission at the reader.
- The visitor has been voided in the system.
- The visitor's card has not been issued.
- The visitor belongs to a group of visitors that has been voided.
- Entry to or exit from an area governed by anti-passback control has been violated.
- A card belongs to a group of cards that has been disabled.
- A card was presented at a reader that has been disabled or taken out of service.
- The card has been presented before its allocated start date, or after the card's designated end date.
- The card presented does not belong to the site, which includes an invalid card number, an invalid site number or a card containing an invalid facility code.

In addition, a message will be logged in the audit trail indicating the card use violation, and if configured, a visual and audible alarm will also be displayed.

39.5 Restricted Visitors

The system shall provide the ability to restrict specified visitors and visitors that belong to a specified company from being issued a visitor card. When an operator attempts to add a visitor from a restricted company a warning will be displayed.

39.6 Visitor Card Issue and Return

The system shall provide the ability to log the issue and return of visitor cards. This functionality will include:

- Enabling of the card once it has been issued in the ACS.
- Automatic voiding of the card once it has been returned in the ACS.
- Full date and time recording of card issue and return.

39.7 Expected Visitors List

The system shall provide the ability to maintain a list of expected visitors that displays the name of the visitor, their company and their expected time of arrival and departure. This list shall also be able to display visitors that are currently on site with the same information as expected visitors.

40 Intrusion System Integration

The ACS shall allow the integration of an intrusion system. After integration the ACS shall be used to view the status of areas in the intrusion system and also send a variety of manual commands to the intrusion system. In addition it shall be possible to configure cardholder rights to arm/disarm intrusion system areas.

The ACS shall also support the input points connected to the intrusion system and shall integrate them into alarms, graphic maps, manual commands and event tasks.

Arming and Disarming of intrusion areas can be performed by:

- Manual control of intrusion areas
- Creating graphic maps
- Intrusion Terminal Control

The Manual Commands available for the intrusion system shall be as a minimum:

- Arm
- Disarm
- Part Arm
- Clear Intrusion Alarms
- Clear All Bells

41 Offline Door Integration

The ACS shall support the integration of offline doors, so that remote doors and doors without wiring can be managed through a single MMI. As a minimum the system shall support the following offline door features:

- Assignment of Doors and Lockers in the ACS.
- Offline door messages appear in the event log (e.g.: low battery)
- Management of card access to online and offline doors in a single system
- Ability to void cards at offline doors
- Support for SPACE Protocol
- Support for Cerpass Protocol
- PIN Function
- ADA - Disability assistance (latch time extension)

41.1 Access Assignment

It shall be possible to assign offline doors in the standard manner via the ACS for any cardholder in the system. The ACS shall provide support for simultaneously adding access to both offline doors and online doors at exactly the same time.

41.2 Offline Door Alarms

It shall be possible to display alarms received from the offline doors in the same MMI as all online doors without the need for the operator to change applications.

41.3 Offline Behavior

As a minimum the offline doors shall exhibit the following characteristics

- Access cards shall carry all events (logs) over a period of time with a minimum of 50 events in history
- The same card shall be used for both online and offline doors
- It shall be possible to “activate” the card everyday for offline doors only

41.4 Wireless Lock Capability

The ACS shall support the Wireless Lock capability through the IP Connected Door Controller for bringing down the cost, effort and time required for installation. The Wireless Hub shall be connected to the ACS ACC through FLN port (RS485 communication channel), and will support up to 8 wireless Lock devices to be paired with one hub.

42 Multiple Facility Linking

The system shall be capable of connecting multiple independent facilities to build a complex access control and security network and provide a complete enterprise solution. This network should allow a single cardholder to be programmed at any facility within that network. This link should distribute cardholder information including images.

The system should be capable of reconciling all cardholder information, so that each facility is updated with the most current data. The system should provide a mechanism by which the reconciliation process can be performed using either a manual or automatic routine, but should also be able to perform this task in real-time.

The communications between facilities should be compliant with a wide variety of networking protocols, and as a minimum include:

- Remote Access Server (RAS)
- Local Area Network (LAN)
- Wide Area Network (WAN)

As a minimum, the ACS shall be capable of linking independent sites across:

- campus
- large single facility
- cities
- states
- nationally
- internationally

43 Siemens APOGEE Building Management System Integration

The system shall integrate with the Siemens APOGEE Building Management System (BMS), using the ACS workstation to send security data to the system. The two systems should provide hardware connectivity so that points programmed in one system, can be used to trigger actions and change the state of points contained in the other system.

As a minimum the system shall be capable of allowing the BMS operator to:

- Query the status of the ACS Input and Output Points
- Secure/Unlock individual doors
- Schedule through the BMS system
- Bi-directional alarm acknowledgement
- Control HVAC and lighting zones (Notification Zones) based on cardholder entry
- BMS should know cardholder identity

The interface shall support the Siemens APOGEE system without the need for custom software:

43.1 Auto Discovery Mode

There shall be an auto discovery feature to provide efficient start-up and commissioning. When communication is established between the BMS and the ACS, the BMS must auto discover the devices and points from the ACS database and automatically build security points in the BMS system.

44 Intrusion Panel Interface

The system shall integrate with a dedicated intrusion panel, using an ISC to communicate directly with that panel.

As a minimum the system shall support the following intrusion panel integration features:

- Automatic zonal arming and disarming based on a pre-defined schedule.
- Manual (via card badge within the access system) arming and disarming of discrete zones within the facility.
- The system shall allow zones to be graphically depicted on a site plan that indicates their current status in real-time.
- Permit operators to send manual commands to the intrusion panel
- Display audit trail messages from the intrusion panel
- Ability to arm an entire zone or just part of the zone (perimeter) based upon the chosen arming option.

44.1 Auto Discovery Mode

There shall be an auto discovery feature to provide efficient location and programming of intrusion zones and inputs that have already been programmed within the intrusion panel.

45 Third party integration

45.1 Cardholder Application Programming Interface

The system shall support information sharing both to and from third party applications via the use of an Application Programming Interface (API). This API must be DCOM compatible and execute the same logon routine as if logging on from a standard ACS workstation.

This sharing of information shall still be governed by the standard authentication used by the ACS, and prevent those System Operators logging into the third party package from accessing information to which they have not been assigned appropriate privileges.

As a minimum, the system shall allow the transfer of the following cardholder data to and from the third party application:

- Card number
- Name (first and last)
- Employee ID
- Start and End Dates
- Vehicle Details (registration, colour, model)

In addition to sharing cardholder data, the API shall also allow the ability to set cardholder access control privileges from a third party application, again governed by standard ACS authentication techniques.

All activity carried out via the API shall be logged to the ACS audit trail in real-time. Reports may also be generated at a later stage detailing all the events that occurred from the third party application.

In addition, the API shall not simply be a disguised SQL interface that may allow invalid changes to database information. Rather, it must be a full application programming interface that enforces all the standard business rules of the ACS.

45.2 Building Management System (BMS)

The system shall support the integration of the ACS with a Building Management System (BMS), using the same workstation to control both systems from the MMI. The two systems should provide hardware connectivity so that points programmed in one system, can be used to trigger actions and change the state of points contained in the other system.

45.3 Alarm Monitoring Systems (AMS)

The system shall be capable of sending alarm messages to an alarm monitoring company, via the use of a dedicated alarm monitoring protocol. The alarms shall be configurable and the scheduling of these alarm messages should also abide by the standard system scheduling rules.

45.4 Danger Management Station (DMS)

The system shall be capable of integrating with a danger management station. This integrating shall allow the ACS alarms to be handled from the same interface used to respond to critical nature alarms such as fire etc. In addition, the ACS shall be able to connect with multiple MDS simultaneously, and enforce the same authentication rules that apply to the ACS natively.

46 Management station integration

46.1 Management Application Programming Interface

The ACS shall provide a management interface that allows data to be accessed and maintained using a RESTful API Web Service.

As a minimum, the system shall allow the transfer of the following data to the third party management application:

- Audit trail logging (all transactions)
- Ability to send commands from the management station to the ACS
- Point monitoring
- View alarms
- Acknowledge alarms

The API shall provide the flexibility to customise the logged audit trail messages, so that only those messages that are required are sent to the management station by the ACS.

46.2 Tools and Documentation

The system shall come with a complete API guide to assist in creating the required components within the management station application. Sample code shall also be provided with examples of how to most efficiently integrate the ACS with the management station.

47 Open Communications

47.1 OPC

The system shall support message sharing both to and from third party applications via the use of an OPC interface. This OPC implementation must be compatible with the “Alarms & Events” section of the OPC protocol.

This sharing of information shall still be governed by the standard authentication used by the ACS.

As a minimum, the system shall allow the following communications with other OPC compliant applications:

- Receive events from third party applications
- Send events to third party applications
- Receive alarms from third party applications
- Send alarms to third party applications
- Group points into logical collections
- Alarm acknowledgement

In addition all activity carried out through the OPC interface shall be logged to the ACS audit trail in real-time. Reports may also be generated at a later stage detailing all the events that occurred from the third party application.

47.2 OPC Based Routines

The system shall support the triggering of event routines based upon messages received from third party OPC compliant applications.

48 Server Redundancy

The system shall be capable of duplicating all database information on a backup Server. When the primary server fails, the system shall be capable of continuing operation using the backup server without loss of data. In instances when the backup server is required, the system should fail-over automatically.

During fail-over, workstations shall automatically be locked out from the database preventing further database changes from taking place. Once the secondary server is on-line workstations should only allow manual logon to gain entry back into the system to ensure correct authentication has taken place.

Data mirroring shall be provided across a dedicated link between the primary and secondary servers. This will prevent an increased traffic load on the WAN/LAN due to data mirroring.

The system shall be configured so that it is possible to remove the primary or backup server for maintenance or repair without interrupting the operation of the access control and security network. As a minimum, the system will fail-over in the event of:

- Hard disk drive failure
- Power supply failure
- Mother board failure

As a minimum, the Server Redundancy solution shall incorporate the following functionality:

- Bi-directional failover
- Hardware independence
- Operates at the device driver level
- Use of TCP / IP protocols and industry standard network cards for mirroring traffic
- RAID compatible

49 Pharmaceutical Site Ready

The system shall be capable of fulfilling the FDA's 21 CFR Part 11 code. This ensures that electronic records and signatures must be proven to be as trustworthy and reliable as handwritten ones.

49.1 Security

The system shall restrict system access to only those users who have the appropriate access rights. A report shall be available detailing each operator account. The system shall also record all successful and unsuccessful attempts at logging on including complete date and time stamping for these actions.

49.2 User Identity

The system shall provide multiple operator access levels and can identify each user via a unique electronic user name and password. The ACS shall provide basic default operator accounts at the time of installation.

49.3 Electronic records

The system shall be able to provide accurate and complete copies of electronic records in human readable form. It shall be possible to provide a printed report of any data or activity in the system based upon reproducible and known criteria.

49.4 Data Retention

The system shall permanently store historical data and this data can be accessed if the ACS completely fails.

49.5 Data Protection

The ACS or systems employed by the ACS shall protect records from accidental or intentional modification, moving or deletion while on the system. It shall be possible to determine if records have been organically modified.

50 Full Web Availability

The ACS shall be compatible with a complete web interface allowing the MMI to be made available via the internet.

It shall be possible to run more than one such web client instance simultaneously as if it were simply a native application client connecting to the ACS.

50.1 Web Available features

In addition to applying to full logon rules administered by the ACS, the following features shall be able to be used over an internet connection, as a minimum:

- Cardholder configuration and access assignment
- Visitor configuration and access assignment
- Access level configuration
- Access group configuration
- Venue and booking

simply a native application client connecting to the ACS.

50.2 Web Client User Interface

The web based client shall have a user-centric design with simple and self-explanatory menu structures and buttons. It shall be built on the latest Web technology and use high security communication for data transfer. The user shall able to create a customizable dashboard with widget capabilities, linking and pinning. The web client shall also be based on responsive design model so that it can support multiple resolutions on multiple monitors. Browser support shall include Chrome, Firefox and IE.

51 Documentation

A comprehensive documentation portfolio shall support the system.

51.1 Software Documentation

The ACS manufacturer shall be able to supply a full range of software documentation, including:

- An Installation Guide
- User's Guides for the core software module and any additional optional modules
- Product Sheets that outline the system requirements and specifications

The software shall include a comprehensive help system that provides information regarding all aspects of the ACS. This help system shall include written procedures that guide the System Operator through the use of the ACS.

51.2 Hardware Documentation

The ACS manufacturer shall be able to supply a full range of ISC documentation, including:

- User's Guides
- Installation Sheets
- Product Sheets that outline the system requirements and specifications.

51.3 Other Documentation

The ACS manufacturer shall also be able to supply a guide that outlines the Third Party Application Protocol Interface (API) and instructions regarding the programming of third party software to communicate with the ACS system.

Software installed on the system such as operating system, database application and others shall be supported by the documentation provided by the manufacturers of those applications.

52 Upgradeability / Expandability

The system shall be fully upgradeable, with the possibility of upgrading software and hardware components at minimum cost.

The system should also be fully expandable to easily permit the increase in control points, monitor points, access points and cardholders.

Each ISC shall be designed so that they can be easily added to an expanding facility and communicate with the ACS using the same communications channels as any existing ISC. In addition, the operation of any new ISC shall not affect or cause the re-programming of any already installed ISC.

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies