



Integrated Security & Building Management System

Architect & Engineer Specifications

October 2007



Table of Contents

PART 1 - GENERAL	5
1. SUMMARY	5
2. SMS DESCRIPTION	5
3. SUBMITTALS	5
4. QUALITY ASSURANCE	8
MANUFACTURER QUALIFICATIONS	8
BIDDER QUALIFICATIONS	8
5. DELIVERY, STORAGE & HANDLING	8
6. PROJECT CONDITIONS	9
7. SEQUENCING	9
8. SCHEDULING	9
9. WARRANTY	9
SMS SOFTWARE AND FIELD HARDWARE WARRANTY	9
CONTRACTOR INSTALLATION WARRANTY	9
10. SMS STARTUP & COMMISSIONING	9
11. MAINTENANCE SERVICES	9
PART 2 - PRODUCTS	12
12. MANUFACTURER	12
13. SMS FUNCTIONAL REQUIREMENTS	12
WORKSTATION MODULE	12
REPORT GENERATOR MODULE	12
AUTHORIZATION MANAGER MODULE	12
STUDIO MODULE	12
SERVER MODULE.....	12
DEPLOYMENT FLEXIBILITY	12
ARCHITECTURE	13
DRAG & DROP TOOLBOX.....	13
ICONS	13
CUSTOMIZABLE LOGIC	13
GRAPHICAL SYSTEM OVERVIEW TREE.....	13
INTERFACING.....	14
ALARM/EVENT LOGGING.....	14
TEXT INSTRUCTIONS.....	14
VOICE ANNUNCIATION	14
ALARM AND EVENT ATTRIBUTES	14
HIGHLIGHTING OF UNACKNOWLEDGED ALARMS:.....	15
PRE-DEFINED "CANNED" ALARM ACKNOWLEDGMENT RESPONSES	15
REAL-TIME, LIVE VIDEO USER VERIFICATION.....	15
AUTO EXIT TO WINDOWS 2000 / 2003/ XP LOGIN WINDOW	16
ALARM MONITORING – COLUMN DISPLAY & CONFIGURATION	16



REAL-TIME, DYNAMIC GRAPHICAL MAPS.....	16
ALARM MASKING.....	16
SORTING CAPABILITIES.....	16
27. SMS SERVER & CLIENT HARDWARE	17
SMS SERVER MINIMUM REQUIREMENTS:.....	17
WORKSTATION MINIMUM REQUIREMENTS:	17
28. NVR AND CCTV INTEGRATION	17
29. ACCESS CONTROL INTEGRATION	18
GENERAL.....	18
DESIGN OF THE INSTALLATION.....	18
MODULARITY	19
INTEGRATION.....	20
OPERATING PRINCIPLES	21
<i>Geographic authorization</i>	21
<i>Time related authorization</i>	21
<i>Access authorization groups</i>	22
<i>Access authorization</i>	22
<i>Additional functions</i>	22
<i>Multi-card support per person</i>	23
ACCESS CONTROL HARDWARE	24
ACCESS CONTROLLER.....	24
INPUT/OUTPUT CONTROLLER.....	27
LIFT CONTROLLER	28
NETWORK COMMUNICATION DESCRIPTION.....	29
<i>Cabling architecture:</i>	29
<i>Communication Dispatcher</i>	29
READER TECHNOLOGIES.....	30
INSERTION READERS.....	30
ACCESS CONTROL SOFTWARE	31
ACCESS CONTROL MODULE	31
<i>Environment</i>	31
<i>Functions of access control software module</i>	31
ADVANCED ACCESS CONTROL FUNCTIONS.....	34
<i>Logical control of position</i>	34
<i>"Confirmation" cards</i>	34
<i>Access to sensitive areas using multiple cards (Multi-card access)</i>	34
<i>Multi-site management</i>	34
<i>Graphic monitoring module</i>	35
<i>Macro-instructions language</i>	35
TECHNICAL MONITORING OF THE SOFTWARE	36
CRISIS MANAGEMENT	36
ADDITIONAL SOFTWARE MODULES	37
FILTERS CRITERIA / REPORT GENERATION.....	37
VISITOR MANAGEMENT MODULE	38
<i>Advanced functionality of the visitor management software:</i>	38
<i>Pre-visit management via Intranet</i>	39
CARD PERSONALIZATION MODULE.....	39



EXTERNAL DATABASE INTERFACES	40
30. INTRUDER ALARM INTEGRATION.....	41
INTEGRATED INTRUSION DETECTION INTERFACE	41
SYSTEM MAIN PANEL.....	41
COMMUNICATION BUS TESTING	41
BUS DETECTORS.....	41
INTERACTIVE VOICE MODULE.....	42
SCHEDULING	42
HYBRID WIRELESS EXPANSION.....	42
KEYPADS.....	43
USER CODES	43
PARTITIONS.....	43
GROUPS.....	43
SUPERVISION	43
FALSE ALARM PREVENTION	43
CENTRAL STATION REPORTING.....	43
PROGRAMMABLE OUTPUTS	44
INTEGRATED ACCESS CONTROL	44
SYSTEM EVENT BUFFER.....	44
SYSTEM PRINTER.....	44
SYSTEM PROGRAMMING.....	44
UPLOAD/DOWNLOAD SOFTWARE	44
PROGRAM TRANSFER MODULE	45
TCP/IP MODULE	45
ADVANCED GSM/GPRS MODULE.....	45
31. FIRE ALARM INTEGRATION	46
32. INTERCOM INTEGRATION	46
33. BUILDING MANAGEMENT INTEGRATION	46
34. OTHER THIRD PARTY DEVICE INTEGRATION.....	46
35. EXECUTION (** TBD BY SPECIFIER).....	46

PART 1 - GENERAL

1. Summary

This document includes a general description, functional requirements, operational characteristics, and criteria for the Security & Building Management System (SMS).

2. SMS Description

The Security Management System outlined in this section and detailed in Part 2 of this document is the key central component for managing physical security and the bridge between physical and logical security and between building management systems for this project. The system shall provide a variety of integral functions including the ability to track and interface alarms; to regulate access and egress; provide identification credentials; monitor, view, record and store digital surveillance video linked to SMS events.

The SMS shall comprise of several software modules that work together seamlessly in a Client/Server architecture.

Upgrades or expansion of the SMS to a larger size system in scale shall not require installation of a different and or new SMS application or require the administrator/operator to learn a different and or new interface from the previous version.

The SMS shall be written using Unicode format. Unicode enables a single software product to be transported across multiple platforms and languages without re-engineering and allows for data to be transported through different systems without corruption.

The SMS software shall be written to ISO Standards on Software Development.

3. Submittals

Drawings:

Provide complete drawings which include the following:

Indicate all system device locations on architectural floor plans. No other system(s) shall be included on these plans.

Include full schematic wiring information on these drawings for all devices. Wiring information shall include cable type, conductor routings, quantities, and connection details at device

Include a complete SMS one-line, block diagram.

Include a statement of the system sequence of operation.

**Product Data :**

Provide complete product data that includes the following:

Manufacturer's technical data for all material and equipment at the system and sub system level to be provided as part of the SMS.

A system description including analysis and calculations used in sizing equipment required by the SMS. The description shall show how the equipment will operate as a system to meet the performance requirements of the SMS. The following information shall be supplied as a minimum:

- Server(s) processor(s), disk space and memory size
- Description of site equipment and its configuration
- Network bandwidth, latency and reliability requirements
- Backup/archive system size and configuration
- Start up operations
- System expansion capability and method of implementation
- System power requirements and UPS sizing
- Device / component environmental requirements (cooling and or heating parameters)
- A description of the operating system and application software.

Contract Close-Out Submittals:

Provide X (**X) sets of hard copy manuals and X (**X) sets electronic format manuals including operating instructions, maintenance recommendations and parts list including wiring and connection diagrams modified to reflect as-built conditions.

Manuals:

Final copies of the manuals shall be delivered within X (**X) days after completing the installation test. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of the contractor responsible for the installation and maintenance of the system and the factory representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The final copies delivered after completion of the installation test shall include all modifications made during installation, checkout, and acceptance testing. The manuals shall consist of the following:

Functional Design Manual: The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included.

Hardware Manual: The manual shall describe all equipment furnished including:



- General description and specifications
- Installation and check out procedures
- Equipment layout and electrical schematics to the component level
- System layout drawings and schematics
- Alignment and calibration procedures
- Manufacturers repair parts list indicating sources of supply

Software Manual: The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

- Definition of terms and functions
- System use and application software
- Initialization, start up, and shut down
- Reports generation
- Details on forms customization and field parameters

Operators Manual: The operators manual shall fully explain all procedures and instructions for the operation of the system including:

- Computers and peripherals
- System start up and shut down procedures
- Use of system, command, and applications software
- Recovery and restart procedures
- Graphic alarm presentation
- Use of report generator and generation of reports
- Data entry
- Operator commands
- Alarm messages and reprinting formats
- System permissions functions and requirements



Maintenance Manual: The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

As-Built Drawings:

During system installation, the Contractor shall maintain a separate hard copy set of drawings, elementary diagrams, and wiring diagrams of the SMS to be used for record drawings. This set shall be accurately kept up to date by the Contractor with all changes and additions to the SMS. Copies of the final as-built drawings shall be provided to the end user in DXF format.

4. Quality Assurance

Manufacturer Qualifications

Manufacturer of the SMS shall be an established organization with referenced and documented experience delivering and maintaining Security Management Systems of equal or higher sophistication and complexity as compared to the system detailed in this specification.

SMS Manufacturer's manufacturing facilities shall be certified ISO-9000:2000 operations, utilize ISO-9000:2000 manufacturing procedures and maintain their ISO certifications.

SMS Manufacturer shall employ at a minimum the following methods for QA of component and assembly devices.

Visual inspection of devices shall be performed to verify assembly according to defined procedures. End of line operational tests shall be performed to ensure product functionality has been correctly configured. A system burn-in period shall be utilized to screen for early life failures of electronic components.

Individual functionality and system level regression testing shall be performed to ensure compliance with product specifications. Single and multiple unit system tests shall be performed to mimic end-user installation configurations. Automated hardware and software testing shall be utilized to evaluate system performance under published operational loads and shall be compared to published system capabilities.

Bidder Qualifications

At the time of the bid, the bidder shall have satisfactorily completed projects similar size, scope and complexity as the system detailed in this specification. The bidder shall furnish written proof of experience from three (3) references and proof of current accreditation/certification by the manufacturer for required training for sales/installation/service of the SMS and associated devices.

The bidder shall also be a factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for the SMS and related systems under this contract. Local shall be defined as an area in a (**X) mile radius of installed location.

5. Delivery, Storage & Handling

(**TBD by Specifier)



6. Project Conditions

(**TBD by Specifier)

7. Sequencing

(**TBD by Specifier)

8. Scheduling

(**TBD by Specifier)

9. Warranty

SMS Software and Field Hardware Warranty

SMS Software shall be warranted for a period of one (1) year from the date of shipment from the manufacturer to be free of defects and will function in substantial accordance to the published specification.

SMS Field Hardware shall be warranted for a period of two (2) years from the date of shipment from the manufacturer, will be free from defects and will function in general accordance with the product specifications.

SMS Third Party Device warranties are transferred from the manufacturer to the contractor, which may then transfer third party warranties to the owner. Specific third party warranty details, terms and conditions, remedies and procedures, are either expressly stated on, or packaged with, or accompany such products. The warranty period may vary from product to product. These products include but are not limited to devices that are directly interconnected to the SMS field hardware or computers and are purchased directly from the SMS manufacturer. Examples may include but not be limited to; Controllers, Reader Heads, Biometric Devices, Computers, etc.

Contractor Installation Warranty

Contractor shall warrant all equipment, not covered under Part 1 Section 1.11.A of this specification and associated installation labor for a period of one (1) year from date of beneficial use.

10. SMS Startup & Commissioning

(**TBD by Specifier)

11. Maintenance Services

General Requirements: The Contractor shall provide all services required and equipment necessary to maintain the entire SMS in an operational state as specified for a period of **X year(s) after formal written acceptance of the system, and shall provide all necessary material required for performing scheduled service or other unscheduled work.



Description of Work: The service and repair of the SMS including all equipment provided under this specification supplied by the successful contractor. The contractor shall provide the manufacturer's required scheduled and unscheduled maintenance and all other work necessary to keep the SMS at its maximum performance.

Personnel: Service personnel shall be factory certified in the maintenance and repair of the equipment installed under this section of the specification. The owner shall be advised in writing of the name of the designated service representative, and of any change in personnel.

Schedule of Work: This work shall be performed during regular working hours, Monday through Friday, excluding federal holidays.

Inspections: The Contractor shall perform two minor inspections at 6 month intervals (or more often if required by the manufacturer), and two major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.

Minor Inspections: These inspections shall include:

Visual checks and operational tests of all console equipment, peripheral equipment, field hardware, sensors, and electrical and mechanical controls.

Mechanical adjustments if required on any mechanical or electromechanical devices

Major Inspections: These inspections shall include all work described under paragraph Minor Inspections and the following work:

Clean all SMS equipment, including interior and exterior surfaces.

Perform diagnostics on all equipment.

Check, walk test, and if required by the manufacturers maintenance procedures, calibrate each sensor.

Run all system software diagnostics and correct all diagnosed problems.

Operation: Performance of scheduled adjustments and repair shall verify operation of the SMS as demonstrated by the applicable tests of the performance verification test.

Emergency Service: The owner will initiate service calls when the SMS is not functioning properly. Qualified personnel shall be available to provide service to the complete SMS. The owner shall be furnished with a telephone number where the service supervisor can be reached at all times. Service personnel shall be at site within X hours after receiving a request for service. The SMS shall be restored to proper operating condition within X hours after service personnel arrive on site.

Records and Logs: The Contractor shall keep records and logs of each task, and shall organize cumulative records for each component, and for the complete system chronologically. A continuous log shall be maintained for all devices. The log shall contain all initial settings. Complete logs shall be kept and shall be available for inspection on site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the SMS.

Work Requests: The Contractor shall separately record each service call request on a service request form. The form shall include the model and serial number identifying the component involved, its location, date and



time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the materials used, the time and date work started, and the time and date of completion. The Contractor shall deliver a record of the work performed within 5 days after work is accomplished.

System Modifications: The Contractor shall make any recommendations for system modification in writing to the Owner. No system modifications, shall be made without prior approval of the Owner. Any modifications made to the system shall be incorporated into the operations and maintenance manuals, and other documentation affected.

Software: The Contractor shall provide all software updates during the period of the warranty and verify operation in the system. These updates shall be accomplished in a timely manner, fully coordinated with SMS operators, shall include training for the new changes / features enabled, and shall be incorporated into the operations and maintenance manuals, and software documentation.

PART 2 - PRODUCTS

12. Manufacturer

The SMS shall be the SynopSYS Integrated Security & Building Management Software manufactured by RISCO Group. (**Delete references to SynopSYS if spec needs to be generic)

The product/s specified shall be manufactured by a firm whose quality system is in compliance with ISO 9001:2000.

13. SMS Functional Requirements

The SMS shall comprise of several software modules that work together seamlessly in a Client/Server architecture. These shall include but not be limited to the following modules:

Workstation Module

This module enables Security Officers and their employees to monitor, manage and control the security and building needs via “drill-down” site, building and floor maps.

Report Generator Module

Enabling set-up (filtering, search, etc.) and generation of one-time or periodic reports of events. Reports shall be exportable in a periodic manner in Excel format or directly to standard printers. The Report Generator shall be a separate module and shall run independently from the Workstation module, to allow flexibility in preparing, setting-up, viewing and exporting reports without interfering with ongoing workstation operation or using a workstation seat license.

Authorization Manager Module

Used by the Site administrator to define user roles and authority to perform actions, view maps or specific devices (cameras, points, etc.), add and modify user groups, add new users, etc. The number of authority levels shall be virtually unlimited, and different authority can be defined independently per user for each specific map, control button, action, input or output point, or camera within the SMS. The Authorization Manager shall be a separate module and shall run independently from the Workstation module, to allow flexibility for modifying or viewing authority levels, without interfering with ongoing workstation operation or using a workstation seat license.

Studio Module

Used by the integrator to design and build the project according to the requirements in a simple manner with a “drag and drop” toolbox.

Server Module

A background Service that handles communication between the hardware devices, the software modules and the database.

Deployment Flexibility



The SMS shall enable Pilot deployment with Pilot hardware, and then deployment with similar hardware on-site without the need to redesign parts of the project. Replacement of hardware controllers or devices (due to hardware malfunctions) with identical controllers shall not require any modifications in the project setup.

The SMS shall be able to seamlessly interface with and monitor Access Control devices, intruder alarm systems, biometric devices, intercom systems, fire alarm panels (secondary monitoring only), digital video recorders, network video recorders and building management systems that are approved for use by the SMS manufacturer.

The SMS shall be able to communicate with devices and controllers via TCP-IP/Ethernet, RS-485 and RS-232.

Architecture

All tasks shall be accessible from any client workstation on the network utilizing one or all of the following:

Traditional client server architecture

N-tier architecture where the SMS shall support the expansion of the system architecture and allow for end-user deployment based upon their system architectural needs. The SMS shall allow but not require the separation of the database, application server, web server and client interface. The system shall require that all connections to the database are performed through a trusted link from the client or internet browser interface.

Drag & Drop Toolbox

The SMS shall include a “drag & drop” Tool Box for simple implementation and on-site modifications of the project. All controller devices and their points (readers, cameras, doors, zones, etc.) shall be displayed in the Tool Box in a tree structure. Any device point can be “dragged and dropped” onto any map. When the device point is “dropped”, the relevant icon (reader, camera, detector, control button, etc.) will appear on the map and it’s default properties will be assigned. The properties can then be modified in a simple manner.

Icons

The icons displayed on the maps in the SMS shall be “point action based” to allow a virtually infinite number of variations to be displayed per icon, without the need to use or generate additional icons per display variant. The integrator shall be able to modify the icon display properties (size, accompanying text, colour, blinking rate, etc.) for each point per point state (alarmed, armed, recording, ready, standby, etc.) in a simple manner according to customer requirements and preferences.

Customizable logic

The SMS shall include “behavior logic” modification screens in which device point behavior and action logic can be modified without any writing of code. Device point Rules and Controls can be freely modified and added. Event behavior logic shall allow addition and modification of event details, event handling, event instructions, event display rules, and event notification rules.

The behavior logic shall allow modification for all point types per controller (modification of default behavior), and shall also allow specific modification for each and any point (Custom behavior modification).

Both the default and the custom behavior logic shall be exportable and importable, to allow use of behavior logic defined for specific controllers in similar situations.

Graphical System Overview Tree



A graphical system overview tree shall display a graphical representation of all field hardware (including ISCs, fire panels, intrusion detection devices, personal safety devices, intercom systems, central station alarm receivers), digital video hardware, access levels, time zones, access groups, holidays, and card formats that have been configured in the SMS. System Administrators shall be able to modify a device that is depicted on the graphical system overview tree or see its properties by double clicking on the icon and the SMS shall bring them to the appropriate form.

Interfacing

The SMS shall be able to connect to and interface bi-directionally with external data sources utilizing all of the following methods:

- ASCII with support for XML formatted text exchange of data activated both manually and automatically.
- ASCII with support for XML formatted text exchange of data using a direct table interface activated both manually and automatically.

Alarm/Event Logging

All alarms and events in the SMS shall by default, always be recorded in the database.

Text Instructions

The SMS shall allow for a set of text instructions to be associated with each alarm that arrives into the SMS. The text instruction function shall allow the System Administrator to enter text for procedures to follow for each alarm that arrives at the Alarm Monitoring client workstations. Each alarm or event in the SMS shall have its own unique set of text instructions should the System Administrator desire.

Voice Annunciation

The SMS shall allow for a customizable voice annunciation to be associated SMS alarms. The customizable voice annunciation shall allow the System Administrator to record a voice annunciation of unlimited length.

Alarm and Event Attributes

System Administrator shall have the ability to configure how the SMS handles the annunciation of alarms on an individual basis. Each alarm and/or event shall have the option(s) to:

1. Display at one or more Alarm Monitoring client workstation.
2. Allow higher priority alarms to be displayed on the Alarm Monitoring client workstation ahead of lower priority alarms.
3. Require the field device, which generated the alarm to be restored to its normal state before the alarm is cleared.
4. Print the alarm to the local event printer.
5. Have a customized voice message annunciate at the client workstation.
6. Have the alarm breakthrough to the Alarm Monitoring window should the System Operator be working in another application
7. Allow System Operators to change the journal entry once the alarm has been acknowledged.



8. Insure that the alarm will not be able to be deleted from the Alarm Monitoring window upon acknowledgment.
9. Display text and audio instructions outlining the procedures to follow when responding to the alarm.
10. Automatically call-up associated maps.
11. Automatically call up the associated cardholder record.
12. Automatically call up the associated cardholder photo using the video verification function.
13. Require a password to view the alarm.
14. Require a password to acknowledge the alarm.
15. Require acknowledgment to clear.
16. Allow mandatory journal entry upon acknowledgment.
17. Use pre-defined journal entries for alarms.
18. Select the option for journal entry based upon the specific alarm.
19. Send CCTV interface commands to the matrix switcher.
20. Automatically send an e-mail message.
21. Automatically send an alphanumeric page.
22. Have the alarm appear on the Alarm Monitoring window with a flashing colored coded bar across the alarm for high priority alarms.
23. Have the alarm, when acknowledged, display an alternative flashing color coded bar across the alarm than for the original alarm color.
24. Trigger a function list(s) when the alarm is acknowledged.
25. Require User Logon for Acknowledgment
26. Have the ability to mark an alarm as "In Progress" where the system shall silence any repeating audio notifications on the Workstation where the alarm was routed and remove the alarm sprite notification on the graphical map. Additional operators monitoring alarms shall be notified that the alarm has been marked "In Progress".

Highlighting of Unacknowledged Alarms:

The SMS shall provide a Unacknowledged Alarm pop-up window that displays alarms that have been unacknowledged after a user defined period of time.

Pre-Defined "Canned" Alarm Acknowledgment Responses

The SMS shall have the capability for pre-defined alarm acknowledgment responses for alarms in the SMS. An unlimited number of pre-defined responses shall be able to be configured for each alarm in the SMS.

Real-Time, Live Video User Verification



The SMS shall have the capability of interfacing to a CCTV system and displaying a live video image next to a stored cardholder image record. This feature shall be system configurable.

Auto Exit to Windows 2000 / 2003/ XP Login Window

The SMS shall be configurable to automatically exit the Alarm Monitoring application and log the System Operator out of the Windows 2000 / 2003 / XP Operating System when a System Operator logs off an Alarm Monitoring client workstation. The SMS shall then bring the System Operator to the Windows / XP Login Window for the next System Operator to log on.

Alarm Monitoring – Column Display & Configuration

The SMS shall allow System Administrators and System Operators to define which columns are displayed in the Alarm Monitoring Window and in which order. System Administrators and System Operators shall also be able to determine the column order.

Real-Time, Dynamic Graphical Maps

The SMS shall support graphical maps that display device status, dynamically in real-time. The maps may be configured to appear on command or when specified alarms are selected for acknowledgment. Map device icons shall have the ability to dynamically change shape and/or color to reflect the current state of the device.

The SMS shall support the map formats listed below:

- JPEG (.jpg)
- TIFF (.tif)
- Windows Bitmap (.bmp, .dib)

The SMS shall support map hierarchies or maps within maps. There shall be no limit to the number of maps that shall be nested hierarchically with each other. Multiple maps may be displayed simultaneously.

The SMS shall support user defined icons for field hardware devices. The graphical maps shall have the ability to be printed to a local printer.

The SMS shall have the capability for filtering out alarm types from the Alarm Monitoring window. Alarms that may be filtered are access granted alarms, access denied alarms, system alarms, duress alarms, and area control alarms. If applicable, fire alarms, asset alarms, intercom alarms, central station receiver alarms, intrusion detection alarms, video event alarms, and transmitter alarms may also be filtered.

Alarm Masking

The SMS shall support the masking of alarms to be controlled on a time zone basis or by manual control.

Sorting Capabilities

The SMS shall allow System Operators to arrange the way that alarms and/or events in the Alarm Monitoring window are listed by sorting the alarms and events.



27. SMS Server & Client Hardware

The SMS Server shall be 100% IBM Personal Computer Standard compatible, approved for use with Microsoft Windows 2003 Server or Microsoft Windows XP Professional:

SMS Server minimum requirements:

- Operating System: Windows XP Professional SP2, Windows 2003 Server SP1 or above
- CPU: Minimum Pentium 4 3GHz or AMD3500
- RAM: Minimum 1GB Dual DDR, 400MHz (2GB recommended)
- Hard Disk: NTFS file system formatting, minimum 40GB free space
- Network: Ethernet port
- USB: Free port for Hardware License Key

Workstation minimum requirements:

- Operating System: Windows XP Professional SP2 or above
- CPU: Minimum Pentium 4 3GHz or AMD3500
- RAM: Minimum 1GB Dual DDR, 400MHz (2GB recommended)
- Hard Disk: NTFS file system formatting, minimum 40GB free space
- Network: Ethernet port
- Display Card: DirectX 9 compatible 128MB
- Display Monitor: Dual-head displays of 19" 1280x1024 resolution or above are recommended

For a PC that is both a Server and Workstation, use Server requirements and add display card and monitor requirements of Workstation.

28. NVR and CCTV INTEGRATION

(**TDB by Specifier)



29. ACCESS CONTROL INTEGRATION

General

The project consists of installing a system for controlling access by use of Readers and Controllers that activate various access, egress and locking systems: electrical locks, ventilation outlets, parking barriers, turnstiles, etc.

In order to be able to offer the best guarantees with regard to reliability, security and simplicity, the installation of the Access Control system shall be designed in accordance with the principle of distributed intelligence.

The principle of distributed intelligence means that under no condition will a Controller have to interrogate any concentrator or central processing unit in order to authorize the opening of the controlled access. Passing an authorized card through the reader results in an immediate command to open the controlled access, regardless of the load on the communication network or on the system's main control unit (computer). A detectable waiting period may only occur when an anti-passback function has been configured, or in a rare case where the administrator of access authorization management has selected this configuration option in the management system for a specific part of the installation.

The Controllers shall be CE Marked.

Design of the Installation

Each monitored access shall be equipped with:

- Electronics Controllers managing up to two entrance/exit doors* or up to four ordinary entrance doors (with distributed intelligence in all cases)
- Entry: a card reader outside the protected area.
- Exit: a pushbutton or request-to exit unit and a reader if exit control is required (option).
- An electrical system for locking and unlocking the door, continuously operating at 12 V and opening when there is a power failure.
- A monitoring switch providing the status of the door.

** NOTE: The Controller shall be able to have a maximum of 4 readers*



Comments:

- All Controllers shall be able to support a reader for exit, in addition to entry (if the Controller manages one or two doors).
- All Controllers shall support a keypad, at the entrance as well as at the exit, in order to enable the use of personal identification numbers (PIN) in addition to the card.
- Should directional obstacles (turnstiles, single-person locks, etc.) be used, the same Controller shall enable a different command relay to be activated, depending upon the direction of passage (one relay for entry and another for exit).
- All the Controllers shall be connected to a main management PC via a reliable communication link (Ethernet, etc.).

This connection shall serve three objectives:

- Enabling the configuration data to be downloaded into the Controller to allow distributed intelligence (cards, codes, schedules, etc.).
- Enabling PC commands to be sent to the Controller (unlocking, etc.).
- Enabling the information to be retrieved by the PC (events, alerts, etc.).

Should this connection be interrupted, the system's operation shall not be affected and the Controller's response time shall remain the same (due to the principle of distributed intelligence).

- The switching power supply of a Controller shall be sufficient to operate a 12V locking system. The power supply shall be backed up by battery.

Modularity

The principle of distributed intelligence and the type of communication used shall enable the broadest possible modularity.

Controllers shall easily be added or removed from the installation at any time.

There shall be no limit to the number of Controllers that the installation can contain. Nevertheless, a management capacity of 15 Controllers per loop is advised to maintain adequate response times; an unlimited number of loops can be used.



Integration

The system shall be comprised of an integrated solution for managing access, timetables, alerts, card personalization and visitor management, all using a common database and enabling use of different cards technologies.

The system shall enable:

- The integration of a card identification management system with photos (**MaxImage – delete references to product names if spec needs to be generic) which makes it possible to capture photographs, store them and print cards. This system uses the same card and the same database, and can use the same management PC.
- The integration of an optimized visitor management system (**MaxVisit – delete product name if spec needs to be generic) thereby making it possible to rapidly enroll and edit the visitor cards. The visitor management system shall be able to generate paper or adhesive cards as well as regular access control tags. These tags will be automatically validated on the company access control system according to the visit needs. Management of visitor's history shall also be possible.
- The integration of a graphic management software (**SynopSYS – Delete product name if spec needs to be generic) for protection and security resources, which shall ensure the synthesis of information from the different asset and people protection systems, displays to the operator the instructions to be applied in case of an alarms and events, and is able to display the sites and action resources available to him.

The graphic management software shall also enable (among other functionality):

- The display of alerts on a map
- The selection of the events and alerts to be displayed
- The programming of an order of precedence of the alerts
- The acknowledgement of the alerts
- The processing of the alerts
- Automatic actions and/or transmissions in the absence of an operator
- The integration of information from other systems by controller contacts and software integration (intrusion alarm systems, fire alarm systems, NVR and DVR systems, Building Managements systems, etc.)
- The display and management of security and safety elements (fire-fighting resources, emergency exits, etc.).

The solution shall be part of a comprehensive and integrated system that enables future development and expansion of the system.



Operating principles

The authorization for card access shall depend upon the following criteria:

- Geographic authorization
- Time-related authorization
- Beginning and end dates and times for the validity of the card for the whole installation
- Beginning and end dates and times for the validity of the card at certain specific doors

Geographic authorization

Accesses shall be sorted by reader groups, which define the authorized access zones for certain categories of people.

There shall be up to 1,500 reader groups.

An access shall be part of several reader groups.

A card shall only be authorized for the access assigned to a specific group and within a specific timeframe.

This principle enables flexible and easy management of access authorizations and does not require individual reprogramming for each card in the event of changes in the organization.

Nonetheless, exception management is anticipated (for one time events, contactors, service people, etc.) and makes it possible to individually program authorized access for each card (reader-by-reader and/or by reader group).

Time related authorization

The access authorizations can be limited to specific times during the day.

Time related constraints shall be based upon the following principle:

- The timetables shall be sorted according to different categories (known as “access types”).
- Each card shall be identified by an Access Authorization Group (AAG) which classifies the reader groups and the types of access.
- 16 types of access shall be available.
- An authorized access schedule shall be assigned to each access type in each Controller, thereby allowing different access authorizations for each door for the defined categories of people.
- There shall be 299 schedules available.
- One schedule shall allow definition of three authorized timeframes per day, for all days of the week including holidays. These timeframes shall be configurable in the software at any time; they shall be definable minute-by-minute.
- 36 holidays shall be programmable.

This principle enables flexible and easy management of access authorizations and does not require individual reprogramming for each card in the event of changes in the organization.



Access authorization groups

Different access authorizations may be grouped into “access authorization groups” to simplify enrollment and management.

An access authorization group may contain an unlimited number of access authorizations.

Each card can be assigned an individual selection of access authorizations or a group of access authorizations.

Access authorization

All of the parameters that make it possible to define the programming of a card will be sorted into “access authorization groups”.

An “access authorization” covers the following parameters:

- A Controller group
- One type of access
- The use of a PIN (personal identification number)
- Triggering automatic commands when the card is presented (for instance, triggering an additional relay on the controller)
- The authority to send commands from the keypad
- The validity starting date and time
- The validity expiration date and time
- A selection of access days

Each card can have an unlimited number of access authorizations.

Thus, it shall be possible to schedule different starting and expiration validity dates and times for the card, for different installation areas.

Similarly, different and very specific authorizations and behaviors for different areas of the installation shall be programmable.

This key function in the software enables, among others, provisional planning of the authorizations and provisional management of the irregularities, as well as changes in the allocation of personnel.

Additional functions

A “highly privileged” (VIP) type of access shall make it possible to associated permanent access (24 hours / 7 day a week) to a card for all doors or areas of authorized geographical access.

A Controller can be deactivated thereby restricting access, even for “highly privileged” cards, and deactivating all logical entries and exits.



Multi-card support per person

Each person may receive up to four cards (with or without PIN [personal identification number]) and one unique PIN code. Each of these cards and codes shall have its own access authorizations.

This broadens the range of card technologies that may be assigned to and used by single person (vehicle tag and card, proximity card and barcode card, etc.). It also allows to easily manage cases where people forgot or temporarily lost their cards.

These cards must be able to be verified simultaneously or individually.

(**Delete screen image if spec needs to be generic)

Persons

Window Edit Search Options

4 Alphabetical

Personal info

Name Mr John Smith Identification 1 10

First name Smith 2

Reference number 46DEA3AE 3

Language English 4

Badge layout RISCO 5

Valid from The / / At : Valid until The / / At :

Cards and code

Card	Code	Access authorization	Status	Level
1 <input type="checkbox"/> 71422331 ? E		<<<< SELECT >>>>	Activated	Only
2 <input type="checkbox"/> ? E		and Select	Activated	Only
3 <input type="checkbox"/> ? E		and Select	Activated	Only
4 <input type="checkbox"/> ? E		and Select	Activated	Only
Code only ?		and Select		Only

Bypass position antipassback

Access authorization for a visitor 0

Reception site

Authorized access time slots

Presence board 0 Last Other The

Zone 0

Options

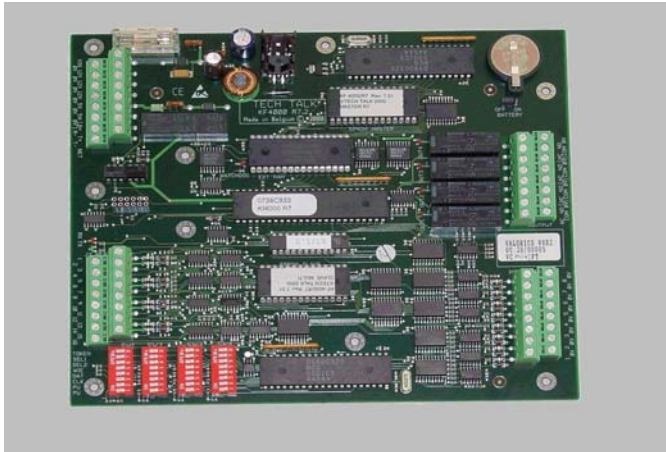
Moreover, it must be possible to refer to recent events linked to a person in the persons screen.



Access Control Hardware

Access Controller

Access Controller (**KF-R7 – delete product name and photo if spec needs to be generic)



Access Controller - Main Capabilities

Management and control

- ✓ 1 to 4 doors
- ✓ 1 to 2 turnstiles
- ✓ 4 relays, 4 readers and 8 inputs
- ✓ Memory: 22,000 people / 2,500 events
- ✓ Performance monitoring and alert

Communication

- ✓ 4800 & 9600 bauds (Keyfree)
- ✓ TCP/IP (option)
- ✓ RS232 (option)
- ✓ WiFi (option)

Security

- ✓ Detecting when switching to backup battery operation
- ✓ Detecting low backup battery power
- ✓ Detecting low lithium battery power

The Access Controller (**KF-R7 – delete product name if spec needs to be generic) shall ensure control over one or two accesses (reader + keypad at entry or at entry/exit) or four entry accesses. The Controller shall be CE marked.

The Controller's main operational features shall be:

- The capacity to handle and process 22,000 cards*
- A buffer memory which can retain the last 2,500 transactions: authorized accesses, denied accesses, alerts, etc.
- Stand-alone logical operation (the Controller does not interrogate any concentrator or PC for access authorization, except in specific cases).
- The possibility to function in a centralized mode (a specific mode in which management software generates an exception to the access authorization, for doubtful situations, etc.)
- The possibility to connect different reader technologies to the same Controller (proximity and barcode, for example).

** NOTE: the number of people retained by the Controller may be reduced when very specific software functions are used. (**Please contact RISCO Group for more information).*



- Scheduling capacity according to the following breakdown:
 - 14 access profiles (access types)
 - One reader schedule
 - One schedule for free access
 - One schedule for free exit
 - One schedule for conditional contact
 - One schedule for the use of PIN (personal identification number)
 - One schedule for the use of the logical position (anti-passback)
 - One schedule for activation per entry
 - Three timeframes per day
 - 36 holidays
- Configurable inputs:
 - For free access, subject to an individual activation schedule
 - For free exit, subject to an individual activation schedule
 - For controlling the status of the door (open, closed, open too long, etc.)
 - For managing locks or barriers (conditional sensors or inputs allowing, for instance, opening of a gate only if a car is present) subject to an individual activation schedule
 - Additional entrances whose use is subject to an individual activation schedule (one schedule per entry)
- Option to display of the status of the entries on an intelligent synoptic chart
- Configurable outputs:
 - Door activation relay
 - Specific alarm relay
 - Ancillary command relay (configured as an exit relay in the case of reader module for a directional barrier)
 - Individual relay configuration
 - LED status display of the relays
- Remote-controlled operation of the relay via software
- Managing a door alarm: door open too long, door not opened following presentation of a valid card, door forced open
- The possibility of connecting a keypad to use PIN codes
 - The use of PIN codes can be imposed individually (on a card-by-card basis)
 - The use of PIN codes can be imposed on a reader by reader basis
 - The use of PIN codes can be subject to an individual usage schedule (on a reader by reader basis)
 - The use of the PIN code can be imposed for single direction monitored access only (entry or exit)
 - The card can be invalidated for after the introduction of three wrong PIN numbers (card + code)



- The possibility of triggering automatic functions by activating the relay with the use of PIN code and card
- The possibility of activating a logical control of geographical position (anti-passback) for 199 area zones, subject to an individual activation schedule (on a reader by reader basis)
- The possibility of activating an anti-timeback functionality (on a reader by reader basis). This prevents a badge to be re-presented within a specified time on the reader.
- The possibility of using a coerced code without changing the number of keypad keystrokes used.
- The possibility of activating the Controller's command relay from an optional keypad to which it is connected
 - An individual authorization for using these commands can be selected (per card and per reader)
- The possibility of disabling an access (halt / resume free access)
- Possibility of selecting the types of events to be stored, per door
- Saving events in case of power failure
- Real-time clock
- LED watchdog for the electronic components
- A network loop bypass relay making it possible to isolate the Controller from the communication loop in the case of power failure, etc.
- TTL inputs configured as NO/NC
- Detecting 220VAC power failure and switching to backup battery operation
- Detecting low backup battery power
- Detecting low lithium battery power (RAM protection)



Input/Output Controller

The Input/Output Controller (**KF-24/24 Input/Output – Delete product name if spec needs to be generic) shall be an electronic remote control and acquisition unit with 24 inputs / 24 relay outputs, operating in accordance with the principle of distributed intelligence. The Controller shall be CE marked.

The Controller's main operational features shall be:

- 24 configured inputs:
 - Protected TTL inputs configured as NO/NC
 - Subject to an individually activated schedule (on an input by input)
 - Able to launch one or several of the Controller's 24 output relays.
 - Alarm point groups can be configured to activate / disconnect automatically or manually
 - The groups may trigger relays on specific Controllers (sounder, transmitter, etc.) even when not communicating with the server
 - The groups may be controlled via key contacts
- 24 configured outputs (relays with 250V 8A power):
 - Individual configuration of the relays
 - LED status display of the relays
 - Buffer memory retaining the last 1,500 events
 - Remote-controlled operation of the relay via software
 - Relays configured as NO/NC

The connection blocks of the Input/Output Controller shall be "unpluggable" in order to simplify maintenance.



Lift Controller

The access control system shall also make it possible to manage lifts (elevators), and shall operate in accordance with the principle of distributed intelligence.

The Lift Controller (**KF-Lift - delete product name if spec needs to be generic) shall be capable of managing a minimum of 12 floors.

A larger number of floors shall be manageable by installing additional Lift Controllers in series.

The Controllers shall be CE marked.

Following are the main operational features:

- Stand-alone operation (the Controller does not interrogate a concentrator or a PC for access authorization, except in specific cases).
- Floor-by-floor control
 - Each floor is considered as a door
 - A name is assigned to each floor in the software
- Ability to adapt to different types of lifts by using four operating modes
- 16 available schedules:
 - One schedule per floor for free access
 - One reader schedule
 - 14 types of access schedules per floor
- The possibility to track floors selected by a person (modes 1, 2 and 3 only)
- Automatic bypass function (mode 1 only)
 - In case a breakdown is detected
 - In case of a power failure
 - In case a specific input is closed
- Each floor appears in the software by name
- Priority mode
- A technical failure output (absence of 12V or current failure)

Note:

In order to be able to install the Controller in the equipment room, and the reader in the lift cubicle, reader distance extension modules shall be used (**KF Far – HD Far - delete product names if spec needs to be generic)



Network communication description

Cabling architecture:

All of the following solutions shall be possible within a single installation.

- Cabled link (bus with RS-232 or USB link)
- Ethernet link addressing TCP/IP 10/100 Mbits
- Optical fiber link
- Specialized lines
- WiFi
- PSTN link

Communication of the Controllers with each other and with the PC shall be accomplished by a double current loop. This method is highly protected against external interference and enables, for example, proper operation of the system in lifts or in zones with strong electrical or electromagnetic interferences.

The cable between the various Controllers shall be a two-pair cable. Should a Controller network be created, it is recommended to use a 9/10th notched cable. The communication network is opto-coupled.

The distance between two Controllers shall be up to 600m on a 9/10th copper cable, where each Controller restores the signal. This distance may be increased to +/- 5 km by adding modem line drivers

Should any Controllers fail or encounter a power failure, an automatic bypass system in each Controller shall remove this Controller from the loop and allows the communication loop to remain operational.

Once such a Controller returns to normal operation, the same system shall automatically enable re-integration of the Controller into the communication loop.

To ensure a high level of security when managing communication with the Controllers connected to an Ethernet TCP/IP network, it shall possible to encrypt this communication (3-DES encryption).

Communication Dispatcher

The solution shall include communication dispatchers for providing the following functionality:

- Enabling Star cabling architecture
- Providing LED display of the communication status with each Controller connected
- Enabling quick identification of any defective Controller in case of failure and allowing to manually isolate (via a simple switch on the dispatcher) one or several Controllers from the network
- Enabling gradual setting up of the installation should this be necessary



Reader technologies

The access control system shall enable use of the following different means for identification:

- Identification by card:
 - Magnetic readers
 - Contact-less readers (Wiegand)
 - Read/write readers (Mifare, i-Class, Legic)
 - Infrared (barcode) readers
 - Hyper frequency readers
 - Remote radio control readers
- Biometric Identification
 - Hand
 - Fingerprint (integration of the Sagem biometric module within the access control software: enrollment in a single software)
 - Eye (iris)

All these identification means may be combined in the same installation.

Insertion readers

Insertion readers may also be integrated into the system.

The following functions shall be configurable with regard to an insertion reader, taking the parking exit as an example:

- After insertion of an “employee” card, returning the card and opening the barrier
- After insertion of a “visitor” card, keeping the card and opening the barrier



Access Control Software

Access control module

Environment

The access control software module (**MaxiTalk – delete name if spec needs to be generic) shall be flexible and user-friendly, written in an advanced language (C and C++).

The database used shall be a standard one, and not exclusively that of the software's creator.

The availability of an ODBC access to the database shall expose it to external databases and tools via ODBC links. These links open up potential opportunities for dynamic compatibility between the integrated Keyfree system software and the client's internal databases and tools, without going through the process of exporting the data.

Several languages shall be available (multilingual software):

- French, English, Dutch, German, Italian (**For additional languages: please contact RISCO Group for further information).

The software shall be available for Windows 2000, 2003 and XP for single-user, multi-user and client/server configurations.

(**Please consult RISCO Group regarding for PC requirements, as they depend on the size and functionality of the installation).

Functions of access control software module

The basic function of the software shall be to offer a user-friendly interface in order to be able to program the system, as well as to manage the events.

The access control software shall enable:

- Loading the data into the Controller intelligent synoptic and presence charts or panels.
- Sending PC commands to the Controller (unlocking, etc.).
- Managing the different types of communication.
- Retrieving data from the Controller using the PC (events, alerts, etc.).
- Optimizing the rate of communication for the start-up phase
- Setting the date and time of the installation and automatic changing of summer and winter time.
- Managing card status:
 - Active
 - Inactive
 - Lost
 - Stolen
 - Returned
 - Out of service
 - Not returned



- Managing access:
 - Per Controller
 - Per reader groups
 - Per person
 - Per groups of people
 - Using cards and/or PIN codes
 - Etc.
- Programming up to 4 access cards and one access code for each person
 - Each of these cards or codes has its own access authorization
 - Each card or code may be verified simultaneously or individually.
 - Each card can be for different identification technologies
- The definition of access authorization consists of the following parameters:
 - One reader group
 - One access type
 - The use of a PIN code
 - Launching automatic commands
 - The authorization to execute commands from the keypads
 - Date and time for the beginning of the validity
 - Date and time for the expiration of the validity
 - A selection of access days
- The definition of access authorization groups to simplify card management
- The definition of zones enabling logical control of geographical position.
- Managing schedules (up to 3 cycles per day) in which the following are selected:
 - The schedules used for the configuration
 - The schedules used for the deferred and the automatic processes (for instance, printing the list of people on-site every Monday morning at 9:00 AM)
 - Each reader's individual schedule:
 - Access schedules for the access types
 - Free access schedule
 - Free exit schedule
 - Schedule for using the PIN codes
 - Schedule for activating anti-passback
 - Schedules for activating the sensors
 - Etc.
- Up to 36 holidays
- Event management and monitoring:
 - Intrusion alarms
 - Open door alarms
 - Technical alarms
 - Etc.



- Selecting events to be stored
- Relay commands
- Defining the connection between card presentation and commands
- The authorization to activate/deactivate other systems (authorization on a card-by-card basis) by using the auxiliary command relay
- Direct enrollment by card reader (option)
- Storing and retrieving encoded data
- Generating lists :
 - Lists of events (by type, by timeframe, by person, etc.)
 - In alphabetic order
 - In chronological order
 - For a period freely determined by the user
 - Lists of people
 - In alphabetic order
 - By card number
 - By reader group
 - By access type
 - Etc.
- All the printed reports can use filters that make it possible to select the components to be printed, based upon a variety of selection criteria
- The possibility to export reports in Microsoft Word and Microsoft Excel format as well as in HTML format.
- Managing user and passwords
 - Accessing the session by user name + case sensitive password
 - Five password levels
 - An unlimited number of passwords
 - Display the previous use of the software (user log file)
 - Display the list of users currently using the software
 - LDAP (Lightweight Directory Access Protocol) authentication
- Administrative breakdown of the database
 - Five personalized levels (departments, services, etc.)
 - An unlimited number of categories for each level
- The configuration of a description of the personnel in 50 customized fields

The principle of distributed intelligence makes it possible to use this software on a non-dedicated PC (A PC that is used for other tasks and not always on site).



Advanced access control functions

Logical control of position

The system shall enable an anti-passback (logical control of position) function to be initiated:

- For certain accesses
- For a section of the user population (for example, the option to deactivate anti-passback for security personnel or the General Manager).

The anti-passback function shall verify the logical position of a card for all those zones in which it is activated, and shall prevent use of a card to enter or exit a zone where logically it should not be, or use of the same card by two people to enter or exit.

The anti-passback function shall be programmable by the access control software which defines the different zones (up to 199 configurable zones per user) as well as the Controllers which are not taken into account for this function. It shall be possible to define a usage schedule to determine, Controller by Controller, the periods during which the anti-passback function will be active.

A timed anti-passback function (enabled on each reader independently) shall also be available (enabling to deny access to a card presented twice within a configurable period of time).

“Confirmation” cards

This function shall enable verifying and authorizing the passage of a person "requiring confirmation" by presenting a "confirmation" card.

For example, this function is used to authorize visitor access to sensitive areas in the building, ensuring that someone accompanies them.

Access to sensitive areas using multiple cards (Multi-card access)

Multi-card access shall consist of defining that the passage through an access requires presentation of up to 10 cards, and by defining the maximum time between presentation of each card.

This function is used, for example, to ensure the presence of two people when accessing a sensitive room.

Multi-site management

The system shall include an advanced Multi-site management function regarding the user passwords, that enables multi-site management of access control systems, alarms and visitor management and includes:

- User rights based upon a password
- A multi-criteria filter can be attributed to each user
- Filtering criteria using any combination of:
 - The password levels
 - The people
 - The readers
 - The reader and access authorization groups.
 - Geographical zones



Graphic monitoring module

A Graphic monitoring module (**MaxiMon – delete name if spec is generic) shall enable display of all or selected events with customized graphic monitoring:

- By color (Windows Palette)
- The possibility to affix a photo to an event card
- The possibility to configure the maximum number of events to avoid displaying too much detail, and to place the monitoring option in “pause” mode.

Access to the software shall be by customized password, with the option of defining multiple environments (filtering events, selecting colors, the origin of the alarm points, monitoring a selected population, etc.)

Macro-instructions language

The system shall include a macro-instructions language, intended for advanced users to enable creating a macro-instructions library to program actions and reactions in different components of the integrated system.

Macro-instructions shall enable to adapt the system to installation specifications and to adapt and simplify the user interface of the operators, without software engineering intervention.

It shall be possible to trigger the macro-instructions automatically upon receipt of an event, or manually from a management PC.



Technical monitoring of the software

When the installation consists of several management PC's, the system administrator must be kept informed of any technical problems throughout the installation.

It shall be possible to monitor the proper operation of each software program and generate error messages in case of failures (hardware and software monitoring).

The error messages shall be displayed on the management PC's, if required.

It shall also be possible to program the automatic sending of an email message when an internal technical problem is detected in the system.

An application that makes it possible to monitor all communications from a remote station shall also be available with the possibility, for example, to monitor and manage the communications between the controllers and the server remotely from a PC located in the IT department.

Managing event logs in the database

The software shall include the possibility to manage event logs; to decide which events will be logged and where they will be located in a "syslog" database.

The types of logs shall be: urgent, alarm, critical, error, warning, notification, information and debug. The first seven log types are standard and used by the syslog protocol on all the larger servers (AIX, UNIX, Linux, Windows). The latter type, bug, shall be used internally by the access control manufacturer.

Crisis Management

In order to be able to rapidly modify the access authorizations in the event of a crisis (strike, demonstration, terror attack, etc.) crisis level management will be integrated into the access control software, thereby allowing the authorized person on site to change personnel access parameters.

The five-level crisis management shall meet requirements of DEFCON, ISPS, Vigipirate standards.



Additional software modules

The following additional software modules shall be integrated to simplify project implementation:

- ASCII import/export module
- Management of people present in areas (people count)
- Deferred processing module (automation of reports, purges, backups, etc.)
 - Possibility to define a number of alerts and a number of events online
 - Possibility to define the number of days online
- Interactive access control module used when video verification for doubtful situations is required. It can be directly interfaced with the PC or using the output of a Video matrix. The operator may view a live video of a person presenting his card, together with a database image and the personal information linked to the card presented.
- Internet/Intranet server module. This module enables Web access for visit planning and macro-trigger (using Maxiweb) and card and person management using Maxi.Net

Filters criteria / Report generation

The software shall enable creating filters and generating reports according to the following specific criteria:

- Name
- Card
- Controller
- Controller group
- Access type
- Type of events
- Date or period
- Five additional criteria that are opened in a multi-criteria selection process

These different criteria may be combined, or processing libraries created and carried out automatically (using the deferred processing module) or manually by the operator.

Printing may be performed continuously, with or without sorting criteria, on any printer (networked on local) as long as a Windows printer driver is available.



Visitor management module

Visitor management software (**MaxVisit – delete name if spec needs to be generic) that uses same database as the access control module shall be available.

This visitor management software shall make it possible to assign access authorizations (using predefined profiles) to visitors. It also enables to assign authorization based on a predefined access profile associated to the host being visited.

Each visitor can be assigned a card with access authorizations based upon:

- A reader or group of readers
- An access type
- A start and/or expiration date and time

(**delete screen if spec needs to be generic)

**Advanced functionality
the visitor
management software:**

- Multi-site management of visitors (visitors are received at the reception center at X or Y location)
- Unwanted visitors: the screen shall become red if the designated visitor appears on the list of excluded persons (unwanted visitors).
- Printing cards sequentially and automatically in alphabetical order (for printing cards for a meeting, a conference, etc.)
- The visitor management module shall be able to list all scheduled visits in chronological order, in which visitor names are in random order or in chronological order to select a visitor.
- Possibility to detect who added or modified a scheduled visit and when was this done
- Possibility to automatically or manually send an email with the visit details to the host person alerting him/her of the visit.

of



Pre-visit management via Intranet

A pre-visit management module, available via Intranet at all the office PC terminals, shall make it possible to introduce a future visit into the visitor management database. It shall also allow to query the database for ongoing and future visits.

The module shall enable inserting scheduled visits via an HTML page that can be accessed from a browser.

The inserted data are, on the one hand, shall be the host's name and password which has to be verified on the Intranet, and on the other hand, the information regarding the visitor (name, surname, company, scheduled arrival and departure dates and times).

This will enable the receptionist to permanently access the list of expected visitors and prepare their cards, if needed.

The data will be verified and automatically transferred to the Access Control visitor database by the Access Control HTTP server.

Standard HTML pages shall be included in the module. It shall also be possible to customize the pages to include, for instance, company logo or other customer specific data if needed.

Card personalization module

The solution shall include a card-personalization module (**MaxImage – delete name if spec needs to be generic) that enables:

- Video camera capture
- Digital storage of photos
- Printing of cards

The database shall be shared with the Access Control module (**MaxiTalk – delete name if spec needs to be generic) ; the data shall be entered only once.

The package shall enable to use existing photo files in BMP or JPG format and re-using the current photo material if compatible. (This shall be confirmed after analysis of the technical documentation, drivers, etc.)

A 160*200 pixel format shall be used for the personnel file (conversion to this format is not included, in case current photos need to be used).

The system can also acquire a signature (in addition to a photo) to be printed on the card.



External database interfaces

The system shall provide an integrated solution for managing access, timetables, alerts, card personalization and visitors, by using a single central database and allowing use of many different card technologies.

Several standard interfaces in the application shall make it possible to add, change and delete records in the system's database, using external applications:

1- *ASCII files interface*

This interface shall enable the access control applications to import and export data in ASCII format (one line per record), one file shall contain all records to import.

This interface allows importing personal information (name, title, department, etc.) but does not enable real-time validation of cards on the Controllers.

2- *ACC interface: ASCII files interface*

ACC is an ASCII file, one file per person, describing the identity of the person and his/her access authorizations. The ACC interface specification is available upon request.

This interface shall function in real time.

Once the file(s) have been placed in the specified directory (the directory location can be configured), the information will be dealt with in real-time, import will be performed and card validation on the Controllers will also be done automatically.

This interface shall enable to verify information by using the access control parameters (i.e., start and expiration dates for the verification, Controller groups, time periods, etc.)

Note: It shall be possible to generate the ACC files directly in the specified directory, or to generate them elsewhere and transfer them to the specified directory using FTP.

3- *General interface*

A general interface shall enable communication with the software application using TCP/IP or RS232 interface. It shall enable to output Access Control events to external customer applications in real-time using a predefined protocol. The General Interface protocol definition is available upon request.

4 - *ODBC link*

The software application shall be accessible via an ODBC link, which shall enable, for example, to display the table content in Excel or adding a record from an external application



30. INTRUDER ALARM INTEGRATION

Integrated Intrusion Detection Interface

The SMS shall provide seamless integration with intrusion detection panels. This shall allow for the ability to monitor intrusion detection alarms in real time inside the SMS Alarm Monitoring module and allow for command and control of supported intrusion detection. Once alarms are brought into SMS, they shall have the ability to be linked to digital video and/or global I/O, and they shall be stored in the SMS database.

Communication with the intrusion detection panel shall be direct wired RS-485 or a LAN connection.

Intrusion detection panel devices (zones, relays) shall be definable and added to the SMS database.

The SMS shall allow for the configuration of Intrusion Detection Zones, Areas, Relays and Doors. Operators shall have the ability to mark intrusion detection Zones, Areas, Relays and Doors as 'enabled' or 'disabled'.

The SMS shall be able to report status information for the Intrusion Detection Devices. All Status Information for Intrusion Detection Systems shall be able to be displayed.

The Intruder Detection System shall be an electronically supervised, battery backed-up intruder alarm system with multiple expansion capabilities.

System Main Panel

All zones shall be fully supervised and programmable. Panel shall be complete with integral power supply and supervised battery charger, auxiliary power for powering security detection devices, programmable switched auxiliary power supply for smoke detectors, integral supervised digital communicator, and 6 programmable outputs: one 3A relay, one 500mA, and four 70mA outputs. The main panel shall include automatic fuses except for the battery fuse.

Communication Bus Testing

The system shall be complete with a standard non-shielded, 4 conductor wire RS485 bus which can run up to 300 meters (1000 ft), for powering and communicating with hardwired system expansion modules and devices.

A bus test feature shall be available to check the communication quality on the bus, enabling quick location of intermittent wiring or communication problems. The communication quality shall be displayed on the keypad in percentages ranging from 0% to 100% for each of the expansion modules on the bus.

The system shall have an auto-install feature capable of recognizing the connected modules upon power-up, in order to enable rapid and error free configuration and installation.

Bus detectors

The Intruder Alarm system shall have the capability to install detectors on the Bus of the system, using the 4 wire RS485 Bus. This enables shorter cabling length saving costs of wiring, Installation in either star or serial or any combination.



The Bus detectors shall be remotely controllable and diagnosable from the systems keypad or from the Upload/download software. Remotely Controllable parameters shall include, LED ON/OFF, MW range setting, Detection sensitivity and other parameters according to the detector model. Diagnostics shall include measurement and display of the voltage input to the detectors, the signal and noise level on each PIR and microwave sensor, and the firmware version of the detector.

The Bus detector models shall include an Grade 3 industrial ceiling mount dual technology detector with installation height up to 8.6m (28'), a Grade 3 Wall mount dual technology industrial detector with two microwave channels and 2 PIR channels and IP65 environmental rating for harsh environments, and Outdoor Detector with two microwave channels and 2 PIR channels and IP65 environmental rating.

Interactive Voice Module

An optional interactive voice module shall provide remote system control and voice status via any touch-tone or mobile telephone. The voice module shall include a full voice menu guide enabling the user to listen to and select the required. The system shall include a prerecorded word library and allow customized messages for zones, partitions, outputs and common system message. System shall be capable of listen-in and speak-in capability to the premises.

Scheduling

The Intruder Alarm system shall provide for up to 32 weekly time schedules with two intervals per day. All schedules shall be programmable via the LCD keypads and via downloading either locally or remotely.

Hybrid Wireless Expansion

The panel shall be expandable to a maximum of 120 supervised and programmable wireless zones, by adding 8 and/or 16 zone receiver expansion modules. The system shall be capable of hardwired and wireless expansion in any mix that suits the application, up to the maximum expansion capability of the control panel.

Wireless receiver modules shall have an internal antenna for higher security. Frequency generation shall be PLL based for high stability and precision in either 433MHz or 868MHz bands. The system shall include signal jamming indication and transmitter low battery indication. Supervision time of the wireless transmitters shall be programmable.

Noise level, threshold level and transmitter signal level shall all be displayable on the system's keypads, enabling installation and calibration without using a separate signal strength meter. The jamming threshold level shall be automatically calibrated per receiver according to the measured environmental noise level, and shall be adjustable, in order to reduce jamming from high incidental environment noise.

The wireless transmitters shall be dipswitch free and have a preprogrammed address (1 out of 16 million codes) that is learned by the system during installation. Wireless transmitters shall be supplied with a long-life lithium battery. The following wireless transmitters shall be available: Universal, magnetic contact and special purpose transmitters, Outdoor Wireless Detectors with integral Active IR Anti-Masking capability, Indoor Wireless PIR detectors with look down creep zones, smoke detectors, 4 button rolling-code keyfobs, 2 button panic keyfobs, Shock Flood and Glassbreak detectors.



Keypads

The Intruder alarm system shall accommodate up to 16 keypads. LCD keypads shall have a display capacity of 32 alphanumeric characters with adjustable contrast. Keys shall be backlit for low light level ease of use. Keypads shall have 4 one-touch buttons that may be programmed for one-touch operation of predefined macro sequence. Keypads shall have a removable door closure that opens down.

The system shall support optional “disabling” of the keypads during arming periods for higher security. In this mode the keypad will be disabled according to a schedule and immediately upon arming, and will be enabled at a scheduled time.

User Codes

The system shall provide for up to 99 user codes selectable as either 4 or 6 digits. Each code can be assigned to one of several authority levels and to multiple partitions. A double code option shall be available that requires 2 users to enter their code in order to disarm the system. For access control an additional 900 access user codes shall be provided.

Partitions

The system shall be programmable for up to 8 fully independent partitions. Each partition shall have its own account code. Keypads shall be assignable to any partition, combination of partitions, or the whole system. Each zone in the system shall be assignable to one or more partitions.

Groups

In each partition the zones shall be assignable to 4 groups enabling 4 levels of quick partial arming in each partition. The keypads shall support 4 level one-touch partial arming.

Supervision

Each zone in the system shall be fully supervised. The system shall be supervised for AC loss. Batteries shall be supervised for low power and be short circuit protected. Additional power supplies shall be supervised for AC loss, low battery, tamper, auxiliary output failure, and loss of sounder loop integrity. Wireless detection devices shall be supervised for presence and low battery. The RS485 bus shall be supervised for low voltage and presence of each defined expansion module and keypad. Digital alarm communicators shall be supervised for phone line trouble and failure to communicate.

False Alarm Prevention

The system shall include the following false alarm prevention features: audible exit delay, arm/disarm bell squawk, audible exit fault, swinger shutdown programmable by zone, transmission delay, pulse count by zone, double knock, soak test by zone, cross zoning, and arming/disarming from outside the protected space using access control. The system shall conform to UK DD243:2000 false alarm prevention requirements.

Central Station Reporting

The system shall support Contact ID and SIA reporting formats and shall be capable of being programmed to call up to 3 telephone numbers. Separate account numbers shall be available for each partition with additional backup accounts. The system shall be programmable for multiple or split reporting, and shall have call saving features.



Programmable Outputs

The system shall be expandable to a maximum of 70 programmable outputs to operate external devices in response to activities related to alarms, zones, partitions, system events, user actions, and scheduled events.

Integrated Access Control

The system shall support up to 8 dual reader access control modules for a total of 16 readers. Each access control module shall provide standalone operation if communication with the main panel is lost. Access control modules shall contain non-volatile memory to retain all schedules and programming even if AC and battery power is lost. Each module shall be able to store the most recent 1000 events. The access control module shall be able to support magnetic, proximity, bar code, touch or Wiegand technology readers. Up to 999 users may be accommodated.

Each access control module shall have a "request-to-exit" input, a "door" contact input, a reader input, and a door strike output.

Access control shall allow users to arm/disarm the security system while locking/unlocking the doors from outside the protected space. Access control software shall be an integral part of the main panel software and shall provide the following functions: capacity for 999 cards, up to 16 user groups with different access levels, and up to 25 weekly schedules with 2 intervals per day, and holiday schedules. Access control functions shall be fully programmable through any system keypad and either locally or remotely using the upload/download software.

System Event Buffer

The system shall have the capability to store up to 999 events, including arming, disarming, bypassing, alarms, troubles, restores, and resets. The events may be read from the system's LCD keypad or uploaded via the upload/download software and printed for further analysis.

System Printer

The Intruder system shall be capable of supporting parallel printers installed anywhere on the bus. All significant events shall be printed as they occur, including access control events. Each event shall include the date, time, and if applicable, the affected partition and user involved.

System Programming

The system shall be fully programmable via the LCD keypads or the upload/download software. LCD keypad programming shall be "Menu Driven" and not "Address & Data" based in order to allow simple programming of the system without continuous reference to the installation manual. Quick shortcuts shall be available to each option of the menu in order to facilitate quicker service phone calls and faster programming and fault diagnosis.

All system programming shall be maintained in a non-volatile memory such that program information is maintained even if all AC and battery power is removed.

Upload/Download Software

The Upload/Download software shall be Windows based with a friendly graphical user interface. The software shall work both locally via a local adaptor to a USB or RS232 port of a PC, or remotely via a telephone line. The software shall enable remote monitoring of system status and shall have several security level and password controlled access. The software shall support shared database capability enabling multiple users to work on the same database via the network.



Program Transfer Module

The system shall support a program transfer module which is capable of downloading, uploading and storing the system's programming without power, without the need for a phone line, a PC or any other peripheral device. The program transfer module shall be connected to the main panel via quick plug in connector.

TCP/IP Module

The system shall have a TCP/IP (Internet Protocol) module enabling secure, economic and constant communication over the Intranet (LAN and WAN) infrastructure.

The advanced communication module shall be a fully supervised accessory of the main panel, enabling detection and reporting of network failure or other trouble. The module shall physically reside in the same box as the main panel and shall be remotely upgradeable via the network for version upgrades.

The module shall be programmable via the system keypads or remotely via the network using the upload/download software. Network communication security shall be of the highest level including a full SSL/TLS secure communication layer. The encryption shall be 256 bit and the cipher key shall be changed frequently for added security. The frequency of cipher key change shall be programmable by the administrator.

The module shall enable automatic sending of selected system event messages to two email addresses. The module shall support the Modbus TCP/IP industry standard protocol for facility control. The module shall be capable of multiple channels of Ethernet and Fast Modem interface.

The system shall include an IP/GSM receiver software application for transferring the encrypted events received via the network at the Monitoring Station to existing Monitoring Software applications.

Advanced GSM/GPRS Module

The system shall have an optional Advanced GSM/GPRS module for primary or backup communication.

The GSM/GPRS module shall enable upload/download via the GSM Data channel

The GSM/GPRS module shall allow SMS reporting of events and remote control.

The GSM/GPRS shall enable emailing of events to predefined email addresses

The GSM/GPRS module shall enable Encrypted SMS reporting of events to an IP/GSM Receiver in the Alarm Receiving Center.



31. FIRE ALARM INTEGRATION

(** TBD by Specifier)

32. INTERCOM INTEGRATION

(** TBD by Specifier)

33. BUILDING MANAGEMENT INTEGRATION

(** TBD by Specifier)

34. OTHER THIRD PARTY DEVICE INTEGRATION

(** TBD by Specifier)

35. EXECUTION (TBD by Specifier)**