



S2 NetBox™
Specifier's Guide &
Generic
Technical & Functional
Specifications

Software version 2.0
Specifier's Guide Release 2.0 - November 2005

For use by Specifiers and Application Engineers.

Specifiers and Applications Engineers:

Enclosed please find the following major resources:

Section I: System Architecture and Functional Capabilities at a Glance.

If you do not require in-depth specification data, or you just need an overview, start here.

Section II: Architects & Engineers Generic Functional and Technical Specification.

Required descriptions can be cut and pasted as required.

Feel free to contact S2 Security Corporation for additional assistance: sales@s2sys.com,
+1.781.237.0800

S2 Security Corporation makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, S2 Security Corporation reserves the right to revise this publication from time to time in the content hereof without prior notification or the obligation to notify any person of any such revision or changes or substitution.

Table of Contents

I.	EXECUTIVE SUMMARY: SYSTEM ARCHITECTURE & CAPABILITIES.....	6
A.	OPERATIONAL ARCHITECTURE	6
1.	<i>Network</i>	<i>6</i>
2.	<i>Hardware</i>	<i>6</i>
3.	<i>Software</i>	<i>7</i>
B.	FUNCTIONAL CAPABILITIES	7
1.	<i>Access Control Features</i>	<i>7</i>
2.	<i>Alarm Monitoring Features</i>	<i>7</i>
3.	<i>Camera and Video Monitoring Features</i>	<i>8</i>
4.	<i>Security Database Features</i>	<i>8</i>
II.	GENERIC FUNCTIONAL AND TECHNICAL SPECIFICATION	9
A.	PART 1: SYSTEM ARCHITECTURE	9
1.	<i>Software Architecture</i>	<i>9</i>
2.	<i>Hardware Hierarchy.....</i>	<i>9</i>
3.	<i>Network Architecture</i>	<i>9</i>
B.	PART 2: FIELD HARDWARE	10
1.	<i>Modular 3-Tiered Hardware Technology.....</i>	<i>10</i>
2.	<i>Hardware List, Drawings, and Descriptions</i>	<i>11</i>
a)	<i>Network Controller Blade</i>	<i>11</i>
b)	<i>Network Node</i>	<i>12</i>
c)	<i>Access Control Blade.....</i>	<i>12</i>
d)	<i>Alarm Input Blade</i>	<i>13</i>
e)	<i>Relay Output Blade.....</i>	<i>14</i>
f)	<i>Temperature Monitoring Blade</i>	<i>14</i>
g)	<i>System Enclosures</i>	<i>14</i>
C.	PART 3: TECHNICAL & FUNCTIONAL SPECIFICATIONS.....	17
1.	<i>System Overview.....</i>	<i>17</i>
a)	<i>Design Elements.....</i>	<i>17</i>
(1)	<i>Scalability</i>	<i>17</i>
(2)	<i>Integration of Subsystems.....</i>	<i>17</i>
(3)	<i>Browser-based User Experience.....</i>	<i>17</i>
(4)	<i>User Licensing</i>	<i>17</i>
b)	<i>System Capacities</i>	<i>17</i>
c)	<i>Internationalization/Localization.....</i>	<i>18</i>
(1)	<i>Supported Languages</i>	<i>18</i>
(2)	<i>Date formats</i>	<i>18</i>
(3)	<i>Character Set Support.....</i>	<i>19</i>
d)	<i>Online Documentation</i>	<i>19</i>
e)	<i>Access Control.....</i>	<i>19</i>
f)	<i>Threat Levels</i>	<i>19</i>
g)	<i>Alarm and Event Monitoring.....</i>	<i>19</i>
h)	<i>IP Camera Surveillance</i>	<i>19</i>
i)	<i>Video Management System (VMS) Integration</i>	<i>20</i>
j)	<i>Graphical Map Management of Sites and Devices</i>	<i>20</i>
k)	<i>System Administration</i>	<i>20</i>
l)	<i>Person Management.....</i>	<i>20</i>
m)	<i>Open Database Connectivity Compliance</i>	<i>20</i>
n)	<i>Data Import</i>	<i>20</i>

o)	Warranty.....	20
2.	<i>Operating System.....</i>	21
3.	<i>Hardware Capacities and Operation</i>	21
a)	Network Controller	21
(1)	Network Communication	21
(2)	Data Security	21
(3)	Database and Event Storage Capacities	21
b)	Network Node	22
(1)	Network Communication	22
(2)	Data Security	22
(3)	Application Blade Capacities.....	22
(4)	Database and Event Storage Capacities	22
c)	Access Control Application Blade	22
(1)	Communication Format	22
(2)	Supported Readers, Input and Output Devices	22
(3)	Capacities.....	23
d)	Alarm Input Application Blade.....	23
(1)	Communication Format	23
(2)	Capacities.....	23
e)	Control Point Relay Output Application Blade	23
(1)	Communication Format	23
(2)	Supported Output Devices	23
(3)	Capacities.....	23
f)	Temperature Monitoring Application Blade.....	24
(1)	Communication Format	24
(2)	Supported Devices	24
(3)	Capacities.....	24
4.	<i>Software Features and Requirements.....</i>	24
a)	Person Enrollment and Administration	24
(1)	Creating Person Database	24
(2)	Using the API to Automate Enrollment.....	24
(3)	Person Data.....	24
(4)	Database Fields.....	25
(5)	Person Query	25
(6)	Import Person Image.....	25
(7)	User-defined Field Labels	25
(8)	Required Fields	26
(9)	Activation/Expiration Date & Time.....	26
(10)	Revoke Card Command.....	26
(11)	Assigning Credentials.....	26
(12)	Enrollment Reader.....	26
(13)	Multiple Credentials	26
(14)	System Administrator Logon ID and Password.....	26
(15)	User Roles	27
(16)	Recent Person Activity	27
b)	Alarm, Event and Alarm Panel Functions	27
(1)	Alarm Panel	28
(2)	Events.....	28
(3)	Inputs	30
(4)	Input Supervision.....	31
(5)	Input Groups.....	31
(6)	Virtual Inputs.....	31
(7)	Outputs	32
(8)	Output Groups	32
c)	Event and Activity Monitoring	32

(1)	Activity Log	33
(2)	Cameras	33
(3)	Camera Views	34
(4)	Floor plans	34
(5)	Monitoring Desktop	34
d)	Access Control	36
(1)	Time Specifications	36
(2)	Card Formats	36
(3)	Access Levels	36
(4)	Holidays	37
(5)	Portals	37
(6)	Floorplans	39
(7)	Elevator Control	40
e)	Threat Levels	40
f)	Reports	40
(1)	Configuration Reports	41
(2)	History Reports	41
(3)	People Reports	41
g)	Network TCP/IP based Video Surveillance	42
(1)	Definitions	42
(2)	Menu Order	42
(3)	Presets	42
(4)	Types	42
(5)	Views	43
(6)	Video Management System	43
h)	System Administration	44
(1)	Network Architecture	44
(2)	Database Backups	44
(3)	Database Restore	44
(4)	Badge Design and Printing	44
(5)	Card Format Decoding	45
(6)	Upgrades and Patches	45
(7)	File and Image Uploads	45
(8)	File Cleanup	45
(9)	System Shutdown	45
(10)	System Reboot	46
(11)	Network Node Refresh	46
(12)	Test Network Connection	46
(13)	Get Node Messages File	46
(14)	Reset AlarmTables	46
(15)	Repair Database Tables	46
(16)	Backup System Files	46
(17)	FTP Backup	46
(18)	Designating Domain Name Servers	47
(19)	Email Settings	47
(20)	Defining Network Storage Locations	47
(21)	Setting Time Zone, Time Servers, and System Time	47
(22)	Changing Operator Passwords	47
(23)	Session Limits and Restrictions	47

I. Executive Summary: System Architecture & Capabilities

A. Operational Architecture

The System shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tiered software architecture.

1. Network

The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network connected PC with a browser. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

IP video cameras, video storage subsystems, VoIP intercoms, and other network connected storage systems shall be usable by the system via TCP/IP communications over the network.

Security of the data communicated over the network to and from the browser, network controller, and nodes is protected by encryption (SSL 128-bit) and authentication (SHA-1).

No separate networking shall be required.

2. Hardware

At the top of the hardware tiers is the Network Controller. Embedded on the network controller are an operating system, a web server, security application software, and the database of personnel and system activity.

The middle hardware tier is the Network Node. The network node shall make and manage access control decisions with data provided by the network controller, and it shall manage the communication between the network controller and application blades connected to the system's inputs, outputs, and readers.

The bottom hardware tier is the Application Blades. Four unique application blades shall be available. An Access Blade shall support two readers, four inputs, and four outputs. An Alarm Input Blade shall support eight input devices. A Relay Output Blade shall support eight output devices. A Temperature Monitoring Blade shall support eight analog temperature sensor inputs.

This modular design makes it possible, even during network downtime, for the system to continue to manage access control, and store system activity logs. When network connectivity is reestablished the system activity logs are automatically reintegrated.

No separate client or server hardware shall be required.

3. Software

The database tier uses MySQL. MySQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database without requiring the use of a separate server.

The web server tier shall be based on GoAhead's embedded web server. This shall provide a graphically rich security management application through a standard web browser.

The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.

This three tiered embedded software design runs within an embedded Linux operating system and shall require no client side software other than a web browser.

No additional client-side software, except a browser, shall be required.

B. Functional Capabilities

The System shall integrate in the browser interface the access control, alarm monitoring, camera and video monitoring, intercom, and temperature monitoring applications. The system shall also maintain a database of system activity, personnel access control information, and system administrator passwords and user role permissions.

1. Access Control Features

Access control features shall include:

- Multiple access levels and cards per person.
- Multiple card formats for mixed card populations.
- Activation/expiration date/time by person with one minute resolution.
- Access level disable for immediate lockdown.
- Use of Threat Levels to alter security system behavior.
- Multiple holiday schedules.
- Timed unlock schedules.
- Card enrollment reader support.
- Photo ID creation support.
- Counted-use access control.
- Dual reader portal support
- Keypad PIN support
- Integration with supported alarm panels.
- Up to 60,000 access cards.

2. Alarm Monitoring Features

Alarm monitoring features shall include:

- User interface securely access under encrypted password control.
- Integrated real time IP and DVR cameras.
- A monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications.
- Integrated alarm monitoring and event management with alarm panels.
- Integrated alarm inputs from the Video Management System.
- Alerts delivered to browsers, email, and cell phones.
- Graphic floor plans with active icons of security system resources.

3. Camera and Video Monitoring Features

Camera and video monitoring features shall include:

- Real time video monitoring displays, including multiple cameras simultaneously.
- Video switching based on access activity.
- Video Management System integration including digital recording of events.
- Multiple supported cameras.
- Recall of photo ID and real time image for comparison.
- Full monitoring through a web browser interface.

4. Security Database Features

Security database features shall include:

- Record recall by vehicle tag, name, or card.
- SQL capability and ODBC compliance.
- Optional storage and recall of ID photos and personal/emergency data.
- Storage of system administrator passwords and permissions.
- Pre-defined reports on system configuration, system activity history, and people.
- English-based query language for instant custom reports.
- Periodic backup to onboard flash ROM and optional network attached storage, including FTP servers.

II. Generic Functional and Technical Specification

A. Part 1: System Architecture

1. Software Architecture

The System shall consist of a network device with a three tiered embedded software architecture.

The database tier uses MySQL. MySQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database without requiring the use of a separate server.

The web server tier shall be based on GoAhead's embedded web server. This shall provide a graphically rich security management application through a standard web browser.

The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.

This three tiered embedded software design runs within an embedded Linux operating system and shall require no client side software other than a web browser.

2. Hardware Hierarchy

The System shall be built with a three-tiered hardware hierarchy.

At the top tier is the network controller, which shall contain the database, web server, and application software. It is at this level that System Administrators, through a browser interface, shall interact with the System, set configurations, monitor activities, run reports, and manage alarms.

At the second tier is the network node, which shall make and manage access control decisions.

At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras, or temperature monitoring points.

The network device shall run on existing building networks and shall be configurable for access from separate subnets, through gateways and routers, and from the internet.

3. Network Architecture

The major components of the System shall be a Network Controller and Network Nodes. Both are solid-state and connect to a common LAN or WAN and use TCP/IP communications. VoIP intercoms, IP video cameras, digital video storage subsystems, and storage systems from other manufacturers shall also be network connectable and the System shall communicate with them using TCP/IP over the network.

The system shall have resident on the network controller a Linux-based database (MySQL) and a web server. The database shall be ODBC compliant, and the web server shall provide a graphically rich user application through a standard web browser.

The system shall be configurable to function and be administered on one subnet, across subnets and gateways, or from any remote site via the internet.

B. Part 2: Field Hardware

1. Modular 3-Tiered Hardware Technology

The system is implemented in a 3-tiered network appliance architecture designed to easily scale up or down to fit any facility's security system needs. At the heart of this native IP device architecture is an embedded Network Controller based upon Intel's IXP425 Network Processor.

Each Network Controller shall support up to 32 Network Nodes. All system functions operate on the nodes and, therefore, reliability is independent of network connectivity.

Each Network Node can support up to seven Application Extension Blades. Application blades provide supervised inputs, relay outputs, reader connections and temperature monitoring points.

Additional Nodes and additional Application blades may be added to a system at any time making it easily scalable.

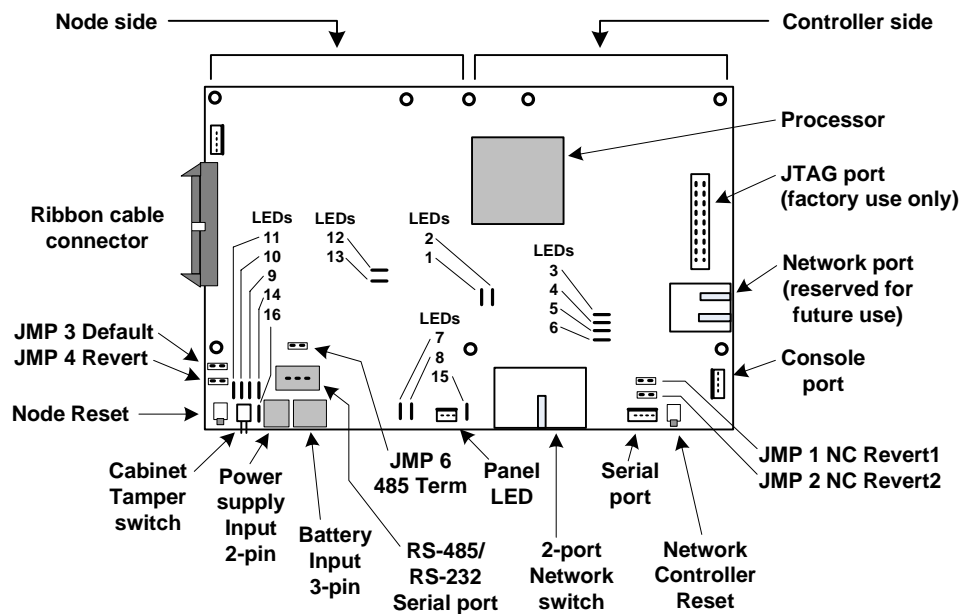
All blades shall be solid state for reliability and long life.

2. Hardware List, Drawings, and Descriptions

a) *Network Controller Blade*

Each Network Controller shall support up to thirty-two network nodes each composed of a Node and up to seven application blades (Access, Input, Output, Temperature).

Each Controller may include an on-board Node or not. Pictured below is a combination Controller/Node Blade.



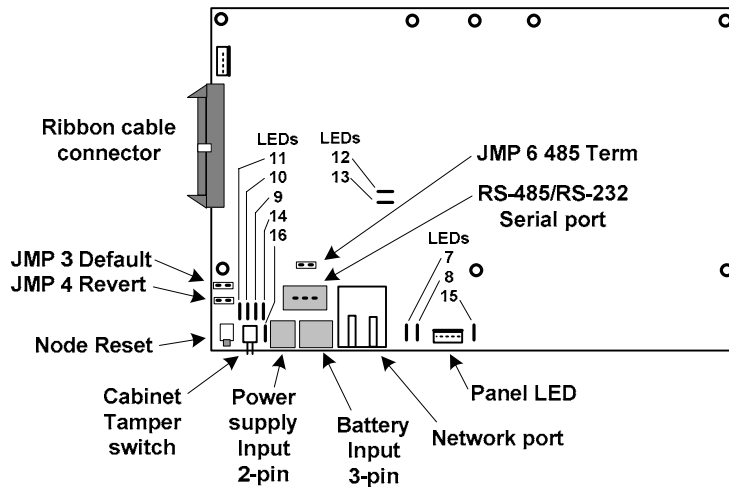
The network controller shall be supplied with 12V DC at a minimum of 3 amps. Internal battery backup shall supply sufficient power to provide for an orderly shutdown of the system in case of loss of external power.

Communications between the node and network controller shall be encrypted (SSL 128-bit) and authenticated (SHA-1).

b) Network Node

Each Node shall support up to seven application blades (Access, Input, Output, Temperature).

A Node may be included on a Controller/Node Blade or it may be a Node-only blade as pictured below.



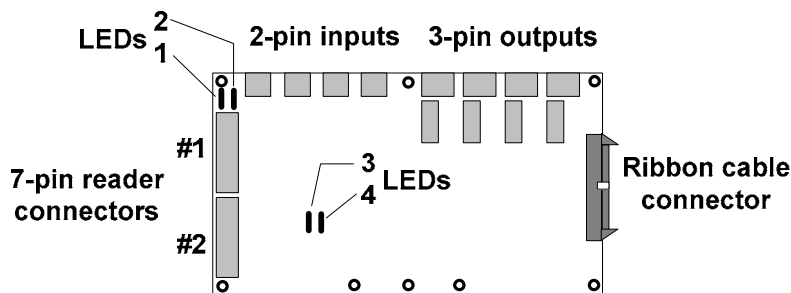
The Node shall be supplied with 12V DC at a minimum of 3 amps. The Node blade shall supply all application blades in the node with power.

The Node shall support onboard data storage of up to 20,000 credentials for access control decisions and up to 27,000 records of logged system events.

Communications between the node and network controller shall be encrypted (SSL 128-bit) and authenticated (SHA-1).

c) Access Control Blade

Each Access Control Blade shall support up to two readers, four alarm inputs, and four relay outputs.



Reader connectors are 7-pin. Reader LED color control and reader beeper control are supported.

Readers require twisted, shielded 22 AWG Belden #9536 (6 conductor) or equivalent wiring and may be no more than 500 feet (152 meters) from the Access blade.

Alarm input connectors are 2-pin. The system shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

Inputs require twisted, shielded 22 AWG Belden #9462 or equivalent wiring and may be no more than 2000 feet (610 meters) from the blade.

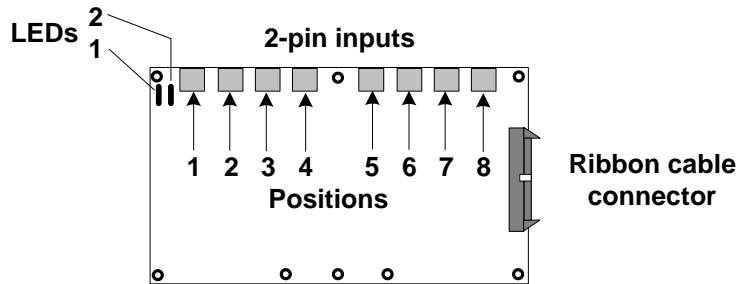
Relay output connectors are 3-pin. Both normally-open circuit and normally-closed circuit output devices are supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

Outputs require twisted, shielded 22 AWG Belden #9462 or equivalent wiring and may be no more than 2000 feet (610 meters) from the blade.

The access control blade shall receive power via the ribbon cable bus directly from the Node Blade. The access blade shall supply up to 400 milliamps of power to one reader or 200 milliamps of power to each of two readers. Readers requiring more power than this shall be equipped with separate external power supplies.

d) Alarm Input Blade

Each Alarm Input Blade shall support up to eight alarm inputs.



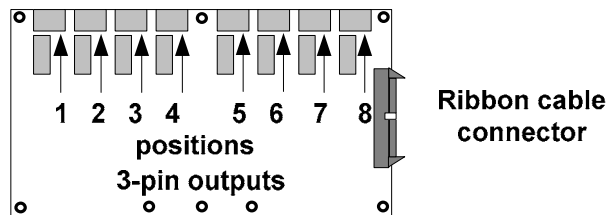
Alarm input connectors are 2-pin. The system shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

Inputs require twisted, shielded 22 AWG Belden #9462 or equivalent wiring and may be no more than 2000 feet (610 meters) from the blade.

The alarm input blade shall receive power via the ribbon cable bus directly from the Node.

e) Relay Output Blade

Each Relay Output Blade shall support up to eight relay outputs.



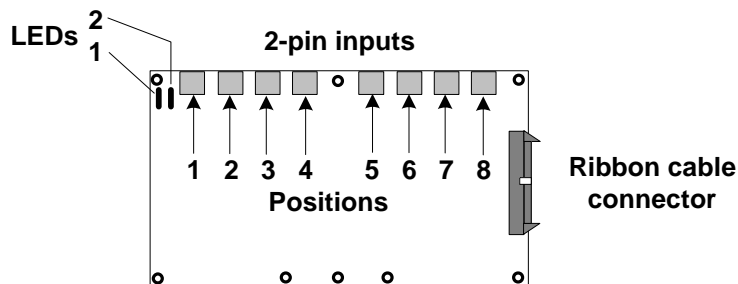
Relay output connectors are 3-pin. Both normally-open circuit and normally-closed circuit output devices are supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

Outputs require twisted, shielded 22 AWG Belden #9462 or equivalent wiring and may be no more than 2000 feet (610 meters) from the blade.

The relay output blade shall receive power via the ribbon cable bus directly from the Node.

f) Temperature Monitoring Blade

Each Temperature Monitoring Blade shall support up to eight analog temperature inputs.

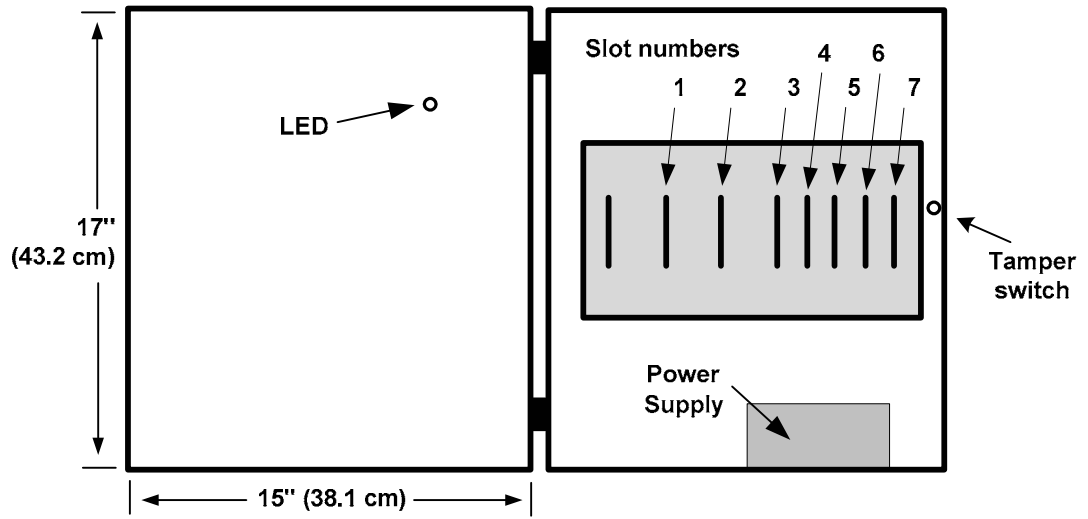


Temperature leads require category 3 cable for distances of up to 500 feet (152 meters). For distances of up to 1000 feet (305 meters), temperature leads require category 5 cable.

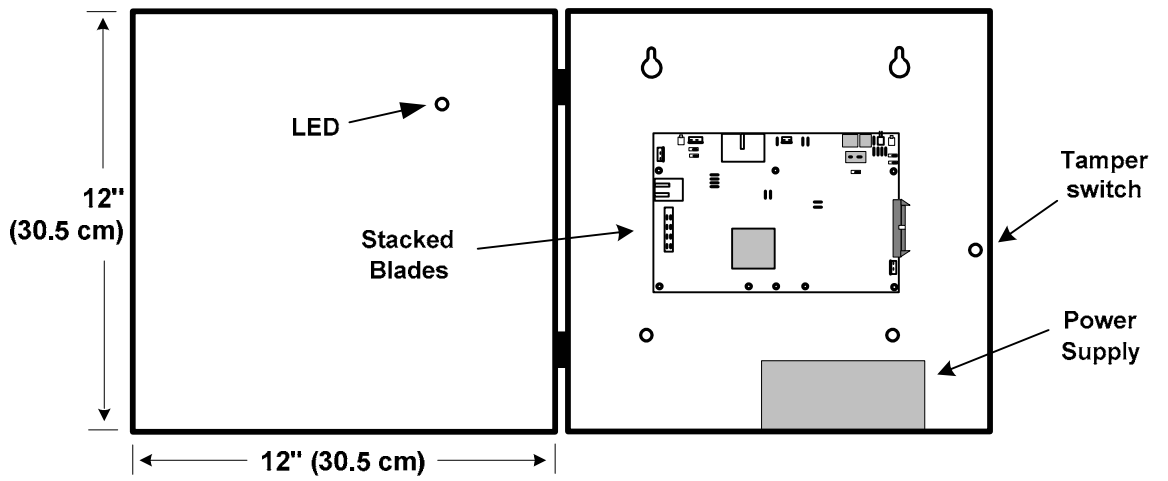
The temperature monitoring blade shall receive power via the ribbon cable bus directly from the Node.

g) System Enclosures

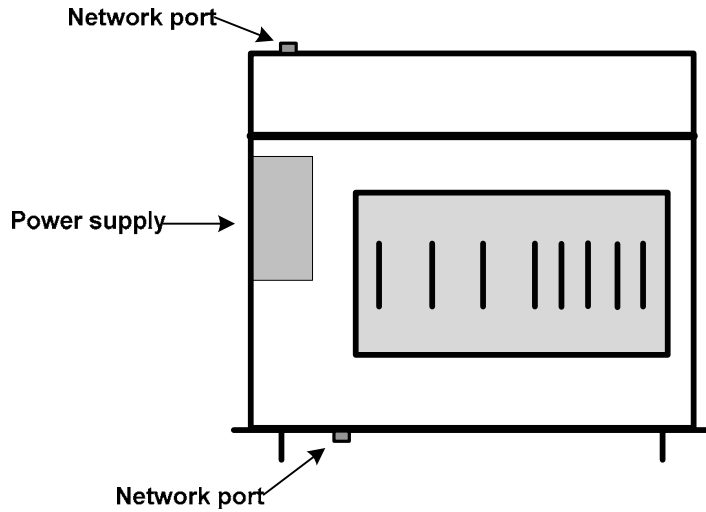
Each system enclosure shall contain up to one Controller/Node Blade and from two to seven application blades. System enclosures can be wall mounted or rack mounted units as shown below.



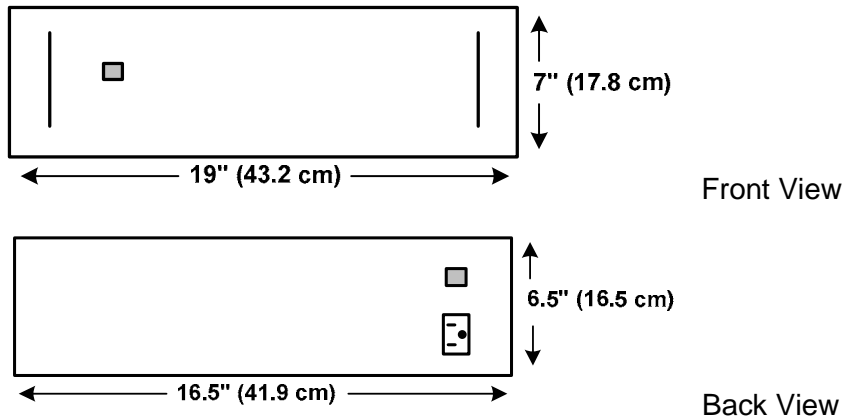
Wall mount cabinet.



Mini-wall mount cabinet.



4U rack mount cabinet



The enclosure shall have a locking mechanism and a cabinet door tamper switch.

The system shall be powered by either 100-240V AC at 50-60 Hz, or by 12V DC at a minimum of 3 amps. Power must come from a separate circuit with an isolated earth ground. If AC power is supplied it must be connected to the internal power supply. If DC power is supplied the internal power supply shall be bypassed. It shall be possible to backup power supplied to the system with an Uninterruptible Power Supply (UPS).

The internal battery backup, if supplied, shall provide sufficient power for an orderly shutdown of the system in case of loss of external power.

C. Part 3: Technical & Functional Specifications

1. System Overview

a) Design Elements

(1) Scalability

The system shall be scalable to support the growth of security system needs. Additional nodes can be added to a network controller up to a maximum of 32 nodes. Each of the nodes can carry an additional seven application blades. It shall not be necessary to reconfigure existing system resources when adding additional nodes, application blades and devices.

(2) Integration of Subsystems

All subsystems within the system, access control, video monitoring, digital video recording, alarm management, temperature monitoring, and management of personnel security data shall be integrated into one application interface for management, monitoring, and administration. In addition the personnel security database shall integrate by means of an API to existing personnel databases for purposes of auto-populating.

(3) Browser-based User Experience

The system shall be capable of being monitored, administered, and configured through a browser on any computer connected to the network. The web server on-board the network controller shall provide a rich graphic application for the management of the system.

(4) User Licensing

Software licensing shall be based upon the number of readers and cameras for one network controller board only. Software license upgrades shall be available if system reader and camera capacity must be raised. The user license shall be valid in perpetuity and shall include one year of software updates.

b) System Capacities

The system shall have the following capacities for each network controller:

- Network nodes 32
- Access control readers: 448 maximum, 140 certified
- Access cards: 60,000+
- Card formats 10
- Alarm input points: 500
- Control point outputs: 500
- Temperature monitor points: 500

- IP and DVR cameras: 32
- Intercom stations: 16
- Online event history log: 250,000 records
- Ethernet switch ports: 4
- Time specifications 100
- Threat Levels 8
- Holidays 30
- Access levels per person 6
- Cards per person 100

The System shall have the following single network node capacities:

- Application blades: 7
- Access control readers: 14
- Access levels 64
- Portals 14
- Portal groups 64
- Reader groups 64
- Input groups 64
- Output groups 64
- Elevators 14
- Floor groups 32
- Alarm input points: 56
- Control point relays: 56
- Temperature monitor points: 56
- Credential storage: 20,000
- Event log records: 27,000

c) *Internationalization/Localization*

(1) Supported Languages

The system shall provide user interface, online help, and printed documentation in English, Spanish, French and Italian. The system administrator shall be able to switch between languages through the application graphic user interface.

It shall be possible to translate the user interface and documentation into other languages.

(2) Date formats

The system shall support the use of globally appropriate date formats. The specific date formats available shall be:

- mm/dd/yyyy
- dd/mm/yyyy

- yyyy/mm/dd

The system administrator shall be able to switch between date formats through the application graphic user interface.

(3) Character Set Support

The System in English shall support the UTF-8 character set.

The System in Spanish and Italian shall support the ISO 8859-1 character set.

d) Online Documentation

The system shall have an online Help system to provide explanations and procedures for all monitoring, administrative, and system configuration and maintenance functions. The Help system shall have linked table of contents, index, and frequently asked questions pages. The Help shall be printable.

e) Access Control

The primary purpose of the system is to provide access control. The system shall be able to make access control decisions, define a variety of access levels, time specifications and threat levels, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs, and provide on-screen monitoring features.

f) Threat Levels

The system shall include configurable and settable threat levels. A threat level or a change in threat level shall be capable of effecting a change in the behavior of the security system. The areas of security system behavior that threat levels can change are portal unlock behavior, alarm event actions, and the function of access levels. A system administrator shall be able to configure threat levels, define behavioral changes based on the system threat level, and set the current threat level. Threat levels shall also be changeable in response to alarm events.

g) Alarm and Event Monitoring

The system shall be capable of monitoring, prioritizing, and acknowledging alarms. It shall be possible to associate specific actions with each alarm event. These actions may include but are not limited to sending pages and emails, energizing outputs to activate lights, locks, or alarms, changing the system threat level, switching to an appropriate video monitor, displaying ID photos, and flashing device icons on a graphic floor plan.

h) IP Camera Surveillance

The system shall provide IP video surveillance capability for up to 32 cameras. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

The system shall support IP video cameras from multiple manufacturers.

i) Video Management System (VMS) Integration

The system shall support the integration of a Digital Video Recorder system. The VMS shall support automatic video recording of events.

It shall be possible for the VMS to report camera up, camera down, and motion detection events to the network controller.

j) Graphical Map Management of Sites and Devices

The system shall provide graphic floor plan capability including graphic display of system devices such as card readers and IP video cameras. The Network Administrator shall be able to graphically configure device icons onto the floor plan images. The graphic floor plans shall indicate access activity and permit lock control.

k) System Administration

The system shall provide for the performance of system administration tasks from any network-connected computer with a browser. These administrative tasks shall include but not be limited to monitoring all system activity including IP video, generating reports, enrolling personnel and credentials, and configuring system devices, and arming alarm panels.

l) Person Management

The system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information. All person data in the system shall be integrated onto one page for viewing, editing, and deletion by system administrators. This data shall be kept on the network controller and shall not require the use of separate storage devices.

All decisions regarding persons in the system shall be made based upon this data. This includes access control decisions, system administrator privileges, and email or SMS notification of system alarm events.

m) Open Database Connectivity Compliance

The system shall be Open Database Connectivity (ODBC) compliant. The on-board DBMS shall be MySQL.

n) Data Import

The system shall support, via an API, the import of names, access levels, card numbers, card formats, and person IDs to facilitate the pre-populating of cardholders into the system database.

o) Warranty

Any hardware components proved defective in material or workmanship during a period of one year after the date of shipment, shall be replaced or repaired. Level 2 and Level 3 systems include an additional one-year warranty on hardware components.

The system warranty shall include 90 days from the date of shipment for all replacement parts and repairs.

2. Operating System

The operating system shall be Linux. The operating system kernel shall be open-source. No training or certification shall be necessary.

3. Hardware Capacities and Operation

a) Network Controller

(1) Network Communication

The system shall support the following networking, communication, and encryption standards and shall run on existing building network infrastructure:

- Network: NTP, TCP/IP
- Web: HTTP, HTTPS, XML
- Email: POP, SMTP
- Messaging: SMS
- Encryption: SSL, SHA-1

(2) Data Security

The system shall protect browser communications using SSL (128-bit) encryption. Administrative access to the security management application and the personnel security data shall also be password protected.

In addition, communication between the network controller and network nodes shall be authenticated using the SHA-1 algorithm.

(3) Database and Event Storage Capacities

Database and event storage capacities vary based upon the system configuration. Onboard memory on the network controller is dynamically allocated. In general, the network controller shall be capable of storing up to 250,000 records of system activity. This shall be settable by the system administrator.

It shall be possible to configure regular automatic database backups to onboard ROM and to save backups to separate network attached storage. It shall also be possible to setup regular automatic creation of database archive files. This shall be settable by the system administrator.

Each night the system shall truncate a sufficient number of the oldest records held onboard to reduce the database to its set limit. This shall create the needed storage space for additional system activity records.

b) Network Node

(1) Network Communication

Network nodes shall communicate with the network controller using TCP/IP. There shall be two types of communications. Initially nodes shall multicast non-encrypted communications for the purpose of discovery. Once communication is established all further communications shall be socket-to-socket from the node to the network controller. Socket-to-socket communications shall be encrypted and authenticated.

Communications to and from the node's application blades does not occur on the network. This communication occurs on the node's internal communications bus.

(2) Data Security

The system shall protect the security of data communicated between the node and the network controller using SSL (128-bit) encryption, and SHA-1 authentication.

(3) Application Blade Capacities

Each network node shall be capable of supporting seven application extension blades. The seven application blades can be any combination of alarm input, relay output, or access control blades.

(4) Database and Event Storage Capacities

Each node shall be capable of storing up to 20,000 credentials for access control decisions. In addition each node shall be capable of logging and storing up to 27,000 system events.

Each node shall, whenever network connectivity to the network controller is available, upload all logged system events currently held in its buffer. Nodes shall no longer store system activity logs once those logs have been uploaded to the network controller.

c) Access Control Application Blade

(1) Communication Format

Communication packets between the access control blade and the node shall not move over the network. This communication shall occur only on the node's internal communications bus and shall include only input state changes, output relay firing commands, and card information from a connected reader.

(2) Supported Readers, Input and Output Devices

The access blade shall support readers that use the Wiegand Reader Interface. Beeper and LED color control are also supported.

The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive, or 5.0 Amps non-inductive.

(3) Capacities

Each access control application blade shall support up to two readers, four alarm inputs, and four control point outputs.

Reader connectors shall have seven pins and be capable of LED color and beeper control. The access control blades shall be capable of providing a total of 400 milliamps of power for readers. Readers requiring more power shall have separate power supplies.

Input connectors shall have two pins and be capable of supporting normally-closed as well as normally-open circuits.

Output connectors shall be three pin and shall be capable of supporting both normally-energized and normally-not-energized output devices.

d) Alarm Input Application Blade

(1) Communication Format

Communication packets between the alarm input blade and the node shall not move over the network. This communication shall occur only on the node's internal communications bus and shall include only input resistance state changes.

(2) Capacities

Each alarm input application blade shall support up to eight alarm inputs. Input connectors shall have two pins and be capable of supporting normally-closed as well as normally-open circuits. Input devices can be no more than 2000 feet (610 meters) from the input application blade.

e) Control Point Relay Output Application Blade

(1) Communication Format

Communication packets between the relay output blade and the node shall not move over the network. This communication shall occur only on the node's internal communications bus and shall include only output firing commands.

(2) Supported Output Devices

The output blade shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive, or 5.0 Amps non-inductive.

(3) Capacities

Each control point output application blade shall support up to eight relay outputs. Output connectors shall be three pin and shall be capable of supporting both normally-energized and normally-not-energized output devices. Output devices can be no more than 2000 feet (610 meters) from the output application blade.

f) *Temperature Monitoring Application Blade*

(1) Communication Format

Communication packets between the alarm input blade and the node shall not move over the network. This communication shall occur only on the node's internal communications bus and shall include only temperature data.

(2) Supported Devices

The temperature monitoring application blade shall support the use of analog temperature sensors.

(3) Capacities

Each temperature monitoring application blade shall support up to eight analog temperature monitoring inputs. Temperature input connectors shall have two pins. Temperature sensors shall be no more than 1000 feet (305 meters) from the temperature monitoring application blade.

4. Software Features and Requirements

a) *Person Enrollment and Administration*

The system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information. All person data in the system shall be integrated onto one page for viewing, editing, and deletion by System Administrators. This data shall be kept on the network controller and shall not require the use of separate storage devices.

A system administrator holding at least an 'Administer' user role shall be able to create, delete, and modify person records, including access levels.

(1) Creating Person Database

A record for each enrolled person shall be created in the person enrollment database.

No database records will be created if required fields are empty.

(2) Using the API to Automate Enrollment

The system shall provide an XML API capable of batch addition, editing, and deletion of names, access levels, IDs, card numbers, and card formats into the system database.

Technical documentation for the API, with code examples, shall be provided upon request.

(3) Person Data

All person data entered into the system shall be held in the system database and shall be available only to system administrators holding at least the Administer user role. Person data can be added, deleted, and edited by such system administrators. Some person data shall also be included in certain

reports. These reports can only be accessed by a system administrator holding at least the Administer user role.

(4) Database Fields

The system person enrollment data fields shall include:

- Last Name (required entry), First Name, Middle Initial
- Activation Date/Time (required entry), Expiration Date/Time
- ID#, PIN, and Notes
- Card Format, Hot Stamp #, Encoded #
- Access Levels list
- 5 user-defined fields
- Office Phone, Email, SMS mail, Location
- Emergency contact Name, Telephone, Telephone2
- Parking Info for two vehicles including: Color, Make, Model, State, License #, Tag #
- User Interface User Name, Password, User Role

(5) Person Query

The security application shall support queries for individuals in the system by a wide variety of data in the person database record. It shall be possible to query the person database on the following data fields:

Last Name

First Name

Expiration Date after/before

ID #

User-defined fields

Access Level

Car license number

Car tag number

(6) Import Person Image

The system shall be capable of importing, storing and displaying jpeg, png, or gif images. These images can be displayed with a person's data on the personal information page, in reports, and on the monitoring desktop.

(7) User-defined Field Labels

The system person information record shall contain five fields that can be custom labeled and can contain any text or number data that needs be captured for individuals enrolled in the system.

(8) Required Fields

The system's person database shall require only last name and activation date/time entries. All other entries shall be optional.

(9) Activation/Expiration Date & Time

Activation date/time shall be a required entry for any person record in the system database. It shall be possible to select from a pop-up calendar the desired activation date. Activation time shall default to 00:00 (the beginning of the specified day) but can be set for any other time of day. This time setting shall be set based upon a 24 hour time format, e.g. 17:00 is 5:00PM.

It shall be possible to enter an Expiration Date/Time if you wish. The cardholder's access shall expire automatically at the specified expiration date and time. It shall be possible to select from a pop-up calendar the desired expiration date. Expiration time shall default to 24:00 (the end of the specified day) but can be set for any other time of day. This time setting shall be set based upon a 24 hour time format, e.g. 17:00 is 5:00PM.

NOTE: Activation date can be more recent than Expiration date. This may happen when re-activating a person's record after it has previously expired. The most recent date takes precedence. This record shall be active but it is recommended that the old expiration date be deleted.

(10) Revoke Card Command

Access cards shall be revocable at any time. A system administrator holding at least the Administer user role may perform this action. Revoked cards shall stop functioning immediately.

(11) Assigning Credentials

Access cards shall be assignable by the system administrator either by entering card data directly into the person record or by use of an enrollment reader. Access levels shall be assignable through the user interface by selection from a drop-down list.

(12) Enrollment Reader

The system shall accept the use of a designated enrollment reader in entering the card number, electronically encoded on the card, into the person enrollment database.

(13) Multiple Credentials

Persons enrolled in the system can be assigned up to six access levels and up to 100 access cards.

(14) System Administrator Logon ID and Password

Person data maintained in the system may also contain a user name and password for logging on to the security application website as a system administrator. It shall be required to enter the password twice for verification

purposes. Passwords may contain neither double-quote (") nor single-quote (') characters.

(15) User Roles

The system shall have four levels of permissions for system administrators. The assignable user roles shall be as follows:

1. **Monitor:** These users may only use the functions in the Monitor menu. Monitor functions shall include viewing the activity log, cameras, and floor plans.
2. **Administer:** These users may use the functions of both the Administration and Monitor menus. Administrative functions shall include adding and editing person information in the enrollment database, issuing and revoking cards, generating reports, and performing database backups.
3. **Setup:** These users may use the functions of the Setup, Administration, and Monitor menus. Setup functions shall include defining access control, alarm event behavior, camera settings, floor plan images and configurations, holiday and time specifications. Setup functions shall also include: designation of network resources such as time and DNS servers, email and network storage settings; performance of system maintenance such as database backup and restore, software updates and file cleanups; designation of time zone, daily backup schedule and enrollment readers.
4. **Define User Roles:** In addition to the roles above these users may also change user roles for other security application users.

(16) Recent Person Activity

This section of the person information record shall provide a report of the last ten (10) system events generated by this particular user.

b) Alarm, Event and Alarm Panel Functions

The system shall be capable of monitoring, prioritizing, and acknowledging alarms. It shall be possible to associate specific actions with each alarm event. These actions may include but are not limited to sending pages and emails, energizing outputs to activate lights, locks, or alarms, switching to an appropriate video monitor, displaying ID photos, changing the system threat level, and flashing device icons on a graphic floor plan.

The system shall also be capable of integrating alarm panels, arming the panels, and triggering events based upon alarm panel status.

A system administrator holding at least a 'Setup' user role shall be able to create, delete, and modify alarm system inputs, input groups, outputs, output groups, alarm panels, and events.

A system administrator holding at least an 'Administration' role shall be able to arm any alarm panel in the system.

(1) Alarm Panel

It shall be possible to name and configure alarm panels including inputs and an output for:

(a) Receive zone status

The security application shall provide a drop down for selecting an input to transmit the alarm panel zone status to the Network Controller.

(b) Receive Armed/disarmed State

The security application shall provide a drop down for selecting an input to transmit the alarm panel armed/disarmed state to the Network Controller.

(c) Toggle Armed State

The security application shall provide a drop down for selecting an output to enable the Network Controller to toggle the alarm panel armed state.

(d) Alarm Panel Auto Arm Behavior

The security application shall support:

Enabling or disabling automatic panel arming.

Configuration of a "panel arming" warning output and the warning duration.

Designation of a time specification for automatic arming of the panel.

Selection of a reader group that will automatically disarm the panel when a valid card is read.

Selection of a reader group that will be disabled whenever the panel is armed.

(e) Alarm Panel Events

The security application shall support the creation and selection of system events to execute when an attempt to auto arm an alarm panel has failed or when a zone event occurs on a panel that is armed.

(2) Events

It shall be possible to enter a name and text description for each event.

(a) Enable/Disable Toggle

The security application shall provide an enable/disable toggle for each event.

(b) Operator Short Message

For each defined event it shall be possible to enter an operator short message of up to 255 characters.

(c) Operator Long Message

For each defined event it shall be possible to enter an operator long message of up to 1024 characters.

(d) Enabled Time Spec

The system shall support the assignment of an enabled time spec to an event. The application shall provide a drop down pick list for the selection of this time specification.

(e) Priorities

The system shall support the assignment of up to 20 levels of priority. In cases of multiple simultaneous events the higher priority event shall take precedence. The application shall provide a drop down pick list for the selection of this priority.

(f) Acknowledgements

The system shall support the designation of alarm events as requiring acknowledgement. An alarm event shall remain active until it is acknowledged or until the maximum duration counter shall have expired.

The system shall support the specification of a maximum alarm event duration. This duration shall be set in seconds. If the duration timer expires the event will auto-acknowledge. If no duration is set the event actions shall continue until the event is cleared or the cause is resolved.

The system shall support the definition of alarm events as allowing event actions to be cleared by a system administrator. The system shall also allow the event to be defined to allow event actions to be cleared even while the cause of the event is still active.

(g) Actions

It shall be possible to enter a name for each action defined as part of an event.

The application shall provide a drop down pick list for the selection of actions to be included in an event. Potential actions for events shall include:

- Lock Portal
- Unlock Portal
- Activate relay
- Deactivate Relay
- Send Email
- Send SMS
- Move Camera to Preset
- Momentarily Unlock Portal
- Save to Activity Log

- Record video
- Set Threat Level

The system shall support the setting of priority for each action in an event. If simultaneous actions conflict the higher priority action shall take precedence.

The application shall provide an enable/disable toggle for actions included in an event.

The system shall support the specification of a maximum duration for an action. This duration shall be set in seconds. If the duration timer expires the action will end. If no duration is set the event actions shall continue until the event is cleared or the cause is resolved.

(3) Inputs

The system shall support up to 500 supervised and unsupervised inputs.

(a) Name and Description

It shall be possible to enter a name and text description for each input.

(b) Addressing

The application shall provide pick lists for specifically addressing each input to a node, blade slot, and position on the blade.

(c) Enable/Disable Toggle

The security application shall provide an enable/disable toggle for each input.

(d) Trigger Output

It shall be possible to assign to each input a trigger output. This output shall fire upon the input state change to the alarm, short, or open states. This action shall not be logged into the security activity log.

(e) Trigger Event

It shall be possible to assign to each input a Trigger Alarm Event. This alarm event shall execute upon the input state change to the alarm, short, or open states. The security application shall provide an enable/disable toggle for assigned alarm events.

(f) Input Supervision Types

The system shall support the use of a wide variety of input supervision types. The system shall support the use of input devices that have normally-closed-circuits as well as normally-open-circuits. Dual resistor, single resistor, and no resistor circuits shall be supported.

The system shall support the use of 1K Ohm resistors and two, three, or four input circuit states shall be detectable depending upon the

supervision type selected. Available input supervision types shall include:

Dual Resistor

Normally Closed Parallel Resistor

Normally Closed Series Resistor

Normally Closed Unsupervised

Normally Open Parallel Resistor

Normally Open Series Resistor

Normally Open Unsupervised

(g) Groups List

The input definition page shall display names of all input groups that contain that input.

(4) Input Supervision

The system shall supervise inputs by means of detecting resistance values.

(5) Input Groups

The system shall support up to 64 input groups per node.

(a) Name and Description

It shall be possible to enter a name and text description for each input group.

(b) Selection

The application shall provide a pick list for selecting individual inputs for inclusion in a group.

(c) Auto-arm Time Specifications

The security application shall support the assignment of an auto-arm time spec to each input group. This time specification shall determine the hours during which the inputs are armed.

(6) Virtual Inputs

The system shall support the use of camera up, camera down, and motion detection events from a Video Management System as alarm inputs.

It shall be possible to assign to each virtual input a Trigger Alarm Event. This alarm event shall execute upon the notification of the network controller by the VMS of an alarm condition. The security application shall provide an enable/disable toggle for assigned alarm events

(7) Outputs

The system shall support up to 500 relay outputs. The system shall support the use of output devices that have normally-closed-circuits as well as normally-open-circuits. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive

(a) Name and Description

It shall be possible to enter a name and text description for each output.

(b) Addressing

The application shall provide pick lists for specifically addressing each output to a node, blade slot, and position on the blade.

(c) Enable/Disable Toggle

The security application shall provide an enable/disable toggle for each output.

(d) Groups List

The output definition page shall display names of all output groups that contain that output.

(8) Output Groups

The system shall support up to 64 output groups per node.

(a) Name and Description

It shall be possible to enter a name and text description for each output group.

(b) Selection

The application shall provide a pick list for selecting individual outputs for inclusion in a group.

(c) Auto-activate Time Specifications

The security application shall support the assignment of an auto-activate time spec to each output group. This time specification shall determine the hours during which the outputs are active.

c) Event and Activity Monitoring

The system shall be capable of monitoring, prioritizing, and acknowledging alarms. It shall be possible to associate specific actions with each alarm event. These actions may include but are not limited to sending pages and emails, energizing outputs to activate lights, locks, or alarms, switching to an appropriate video monitor, digitally recording video, displaying ID photos, changing the system threat level, and flashing device icons on a graphic floor plan.

A system administrator holding at least a “Monitor” user role permission level shall be able to monitor the activity log, all cameras, floor plans, and use the monitoring desktop.

(1) Activity Log

The system application shall provide a page for viewing the activity log in real time. The network controller shall provide onboard memory sufficient for up to 100,000 activity log records. Regular backup and archive procedures for the activity log data shall be supported.

The Activity log shall record the following events:

- Valid access with portal or elevator name, user name, and PIN use
- Invalid access with portal or elevator name, user name, and PIN use
- Portal held open with portal name
- Portal forced open with portal name
- UI session expiration with user name and IP address
- System Administrator logins with user name and IP address
- Failed logins with IP address
- System Administrator logouts with user name and IP address
- Log archive events
- Node timeouts with node name
- Node connections
- Node resets with node name
- Controller response to nodes with node name and controller IP address
- Unlock requests
- Unlock event with portal name
- Alarm events with event name
- Alarm panel zone events
- Alarm panel arm and disarm with person name or event name
- DVR motion detection event and video recording
- DVR camera down/up event and video recording
- Changes in threat level
- Temperature rate of rise/fall exceeded
- Temperature high/low point exceeded

(2) Cameras

The system application shall provide a pick list of all configured IP and DVR cameras. When selected the application shall provide a page for display of the

camera monitor. That page shall also provide controls for pointing the camera, zooming in or out, and for selecting preset positions on the camera website.

It shall also be possible to create a thumbnail monitor of the current camera image. This thumbnail image shall be live and shall remain displayed on the screen until dismissed. Use of other applications and other functions of the security system application shall be possible while maintaining the thumbnail camera monitor display.

The system shall support the momentary unlocking of portals from the camera monitor page.

(3) Camera Views

The system application shall provide a pick list of all configured multiple camera views. When selected the application shall provide a page for display of the camera views. That page shall also provide controls for pointing the cameras, zooming in or out, and for selecting preset positions on the camera website.

The system shall support the creation of multiple camera views which may contain up to four cameras (Quad view). It shall also be possible to create picture-in-a-picture views of two cameras.

The system shall support the momentary unlocking of portals from the camera monitor page.

(4) Floor plans

The system shall support the import, configuration and display of site floor plans. The floor plans can be configured with cameras, portals, and alarm event icons. In addition the current system threat level shall display on a floorplan. The system application shall provide a dropdown pick list for selecting floor plans and a page for the display of floor plans.

The system application shall support selecting cameras on floor plans and displaying thumbnail monitors for the selected camera. The application shall also support the highlighting of alarm event icons when the alarm event is triggered. The application shall also support selecting portals on floor plans and momentarily unlocking the selected portal.

(5) Monitoring Desktop

The system application shall provide a page for mixing all monitoring functions together in one view. This view shall contain four panes.

(a) Alarms Pane

Active alarm events shall be displayed in bold text. The system shall list events in priority order.

The alarms pane shall provide a 'Details' button for each active alarm event. When clicked this button shall display the long message entered when the alarm event was created.

The alarms pane shall provide an 'Acknowledge' button for each alarm event that is configured to require an acknowledgement. When clicked

this button acknowledges the alarm and logs the action. If an event requires acknowledgement it will remain active until acknowledged or until the 'Maximum Duration' counter has elapsed.

The alarms pane shall provide a 'Clear Actions' button for each for each alarm event that is configured to allow event actions to be cleared.

(b) Portal Selection and Unlock Pane

The Monitoring Desktop shall provide a drop down pick list with all defined portals. The application shall support a selection from this list and provide an 'Unlock' button for momentarily unlocking the selected portal.

(c) Activity Log, Cameras, and Floor Plans Pane

The Monitoring Desktop shall provide a tabbed interface for this pane to allow the selection of one monitoring activity.

Clicking the Activity Log tab shall display the log in this pane. Color coding for messages, Valid Accesses, Invalid Access attempts, User login, logout, System messages, Person image verification on access Cardholder Image call up by hyperlink

Clicking the Cameras tab shall provide a pick list of all configured IP and DVR cameras. Once a selection is made the pane shall provide a display of the camera monitor. The display shall also provide controls for pointing the camera, zooming in or out, and for selecting preset positions on the camera website. The system shall also support the momentary unlocking of portals from the camera tab of the monitoring desktop.

Clicking the Camera Views tab shall provide a pick list of all configured multiple camera views. When selected the pane shall provide a display of the camera views. That display shall also provide controls for pointing the cameras, zooming in or out, and for selecting preset positions on the camera website. The system shall support the momentary unlocking of portals from the camera tab of the monitoring desktop.

Clicking the Floorplans tab shall display the default floor plan in this pane and provide a dropdown pick list for selecting floor plans. The system application shall support selecting cameras on floor plans and displaying thumbnail monitors for the selected camera. The application shall also support the highlighting of alarm event icons when the alarm event is triggered. The application shall also support selecting portals on floor plans and momentarily unlocking the selected portal.

(d) Two Camera Live Video Display and Photo ID Pane

The Monitoring Desktop shall provide a two-camera real time live video display. Each camera display shall also provide controls for pointing the camera, zooming in or out, and for selecting preset positions on the camera website.

Viewing live streaming video from DVR cameras shall require the Java™ 2 Runtime Environment version 1.4.2 or version 5.0.

Each camera display shall provide a clickable icon for taking a snapshot of the current camera image. This snapshot shall be static and shall be placed in a thumbnail window.

Beneath the camera displays the monitoring desktop shall provide a photo ID display area. With each valid access the photo ID of the credential holder shall be displayed. Photo IDs of credential holders shall also be displayable by clicking any hotlinked user name in the activity log.

d) Access Control

The primary purpose of the system is to provide access control. The system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs, and provide on-screen monitoring features.

The System Administrator, holding at least a “Setup” user role, shall be able to create, delete, and edit access control specifications and configurations.

(1) Time Specifications

The system shall be capable of storing up to 100 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and an end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.

Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.

(2) Card Formats

The system shall support the use of readers that use the Wiegand Reader Interface. The system shall default to the Wiegand 26 bit format unless a different bit length format is created in the system. The system shall support but not require the use of the card facility code.

It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 10 card formats.

(3) Access Levels

The system shall be capable of storing up to 64 access levels. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or

reader group, and a time specification. It shall be possible to also assign an elevator floor group to an access level.

Up to six access levels shall be assignable to any person ID in the system.

(4) Holidays

The system shall be capable of storing up to 30 holidays. Each holiday must be assigned a unique alphanumeric name of up to 64 characters. The definition of a holiday shall require a start date and an end date. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated then the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

Holidays can be assigned to up to three holiday groups. The system shall support the use of a pop-up calendar from which System Administrators can select dates for holidays.

(5) Portals

A portal is any access point and each portal supports up to 2 access reader devices. The System Administrator, holding at least a "Setup" user role, shall be able to view current portal definitions, change portal definitions, delete portals, and create new portal definitions. Creating a portal defines the access and alarm behavior of the access point. This can include:

- card readers and keypads
- an output for locking
- an input for monitoring the door switch (DSM)
- an input for the Request-to-Exit (REX) function
- local alarm outputs and system alarm events.

(a) Portal Required Information

Portal name and node address shall be the only required fields in a portal definition. However, for a portal to function for access control it shall be necessary to assign at least a reader and lock output.

(b) Portal Alarm Conditions

Portals shall have four alarm conditions. The four alarm conditions are as follows:

1. Forced: When a portal is opened and there has been no card read, nor request to exit.
2. Held: When a portal is held open past the expiration of the shunt timer.
3. Invalid: When the portal reader reads a card for which there is no entry in the database.
4. Valid: When the portal reader reads a card for which there is a valid entry in the database.

(c) Unlock, Request to Exit Modes

- Unlock Time: Unlock duration, set using seconds, shall be settable and editable.
- Shunt Time: Shunt time duration, set using seconds, shall be settable and editable.
- Relock on open: It shall be possible to set portals to relock immediately once opened.
- Unlock on Rex: It shall be possible to set portals to unlock when a REX is initiated.
- REX Mode: The Request to Exit mode shall be settable to either motion mode (motion detection) or push mode (manual switch). Once a REX is initiated alarms are suppressed for the duration of the shunt timer, allowing the individual to exit without triggering an alarm.
- Accept read while open: It shall be possible to set portal readers to accept card reads while the door is open. Unless this is set, portal readers will not accept card reads until the door is closed.

(d) Portal Alarms

- Local to Node: Output responses to alarm states shall be settable for any of the four portal alarm conditions: Forced, Held, Valid, and Invalid. Outputs shall be selectable from dropdown lists for each condition and the duration of the output function shall be settable in seconds. These responses to alarm conditions shall be managed by the node and shall not require network connectivity. These events shall not be logged in the system activity database.
- Alarm Events: Alarm events shall be assignable to each of the four portal alarm conditions: Forced, Held, Valid, and Invalid. Events shall be selectable from dropdown lists for each condition and it shall be possible to enable or disable these events using a checkbox without un-assigning or reassigning events. These events can include multiple actions and shall be logged in the system activity database.

(e) Portal Groups

It shall be possible to create groups of portals and to assign an unlock time specification to the entire group. All the portals in the group shall remain unlocked during the time specified.

It shall also be possible to assign a group of threat levels to a portal group. An unlock time specification will function to unlock the portals in the group only if the current system threat level is one of the threat levels assigned to the portal group.

(f) Portal Readers

It shall be possible to assign two readers to a portal. The reader(s) and portal must both be on the same node. The reader(s) shall send card data to the node whenever a card read is performed.

(g) Portal Keypads

It shall be possible to assign two keypads to a portal. The keypad(s) and portal must both be on the same node. The keypad(s) shall send card data to the node whenever a card read is performed. It shall be possible to require a 4-digit PIN entry on the keypad for verification prior to allowing access.

(h) Reader Definitions

The only required entry for a reader shall be a name. However, it shall be necessary to designate a node, slot and position for the reader if it is to function as part of a node or access level definition. It shall also be possible to enter a text description of the reader. The reader definition screen shall display names of all reader groups that contain that reader. It shall not be possible to delete a reader if it is part of a reader group or access level. A checkbox shall be provided to enable or disable the reader without having to delete or alter its definition.

(i) Reader Groups

It shall be possible to create groups of readers and assign the group to an access level. Readers and reader groups cannot be deleted while they are part of an access level definition.

(6) Floorplans

The system shall be capable of displaying active graphic floor plans and configuring each floor plan with icons representing system resources: cameras, portals, and alarms. A network administrator holding at least a 'Setup' user role shall be able to upload floor plan images and graphically configure device icons onto the floor plan images. Viewing floor plans will require the Macromedia Flash Player 7.0 plug-in for the browser.

(a) Upload

Floor plan images may be uploaded to onboard memory on the network controller in jpeg format. Maximum size for a floor plan image shall be 256K.

(b) Configure

Floor plans shall be configurable with icons of system resources. The functions of these icons shall include selecting and unlocking portals, selecting a camera to view a thumbnail image, alarm highlighting to indicate an event in progress.

(7) Elevator Control

The system shall be capable of controlling elevator access to floors. Required entries for creating an elevator definition shall include only name, node, and button activation time. However, it shall be necessary to designate a reader and floor to output mappings for access control to function. It shall be possible to enable or disable the elevator definition using a checkbox without altering or deleting the elevator definition. Button activation time shall be entered in seconds.

Floor names: It shall be necessary to name all floors requiring access control. Once the floors are named it shall be possible to map (assign) each floor to a specific output for a specific elevator button. This output shall control whether or not a particular button in a defined elevator shall be active.

Floor groups: It shall be possible to create, change, or delete floor groups. It shall be possible to assign a free access time specification to a floor group. The floors in this group will be freely accessible during the times defined by the chosen time specification.

e) Threat Levels

It shall be possible to configure up to eight threat levels. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be assigned to portal groups, access levels, and event actions. The behavior of portal groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.

It shall also be possible to change the system threat level in response to an alarm event.

By default the system contains 6 threat levels: Default, Low, Guarded, Elevated, High, and Severe. Levels "Low" through "Severe" are named and color-coded to follow the United States Department of Homeland Security threat level designations. These can be edited or deleted.

Threat level "Default" shall not be editable nor can it be deleted.

The current system threat level shall display in the title bar of the security application interface and on floor plans.

f) Reports

The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy to use query language shall be included for the use of the System Administrator in creating ad hoc reports. The query language shall be documented in an on-line help system. Alternatively, it shall be possible to specify a query by use of point-and-click.

Report generation shall not affect the real-time operation of the system.

The specific reports provided shall include the following:

(1) Configuration Reports

1. **Cameras:** Displays all camera configuration information including control address, IP port, and camera type.
2. **Camera Presets:** Displays configured presets for each camera in the system.
3. **Elevators:** Displays elevator configuration information including Node, Reader, and Floor to output mappings.
4. **Floor Groups:** Displays all configured floor groups for use in elevator control.
5. **Holidays:** Displays holiday specification information.
6. **Network Nodes:** Displays all nodes in the system with IP addresses and UID (unique ID).
7. **Portals:** Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.
8. **Portal Groups:** Displays a list of all defined portal groups.
9. **Reader Groups:** Displays defined groups of readers.
10. **System Resources:** Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.
11. **Threat Level Groups:** Displays all configured threat level groups and the threat levels assigned to them.
12. **Threat Levels:** Displays all configured threat levels including the description and color assignment.

(2) History Reports

13. **Access History:** Displays access history based on an entered query. The system Administrator can specify the query using either the keyboard or point-and-click selection.
14. **General Event History:** Displays time, type of activity, and activity details for a variety of event types. The System Administrator can select the specific event types for the report.
15. **Portal Access Count:** Display how many times users have used a portal.

(3) People Reports

16. **Access Levels:** Displays all access levels entered into the system including time specification, reader/reader group, and floor group.
17. **Access Validity:** Displays all permitted access locations and time specifications for the person named.
18. **Current Users:** Displays a list of all security system users currently logged in to the security system website.
19. **Photo ID Gallery:** Displays all the photo ID pictures in the system and the person's name.

20. **Photo ID Requests:** Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.
21. **Portal Access:** Lists people with access for a selected portal.
22. **Roster:** Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.
23. **Time Specifications:** Displays all defined time specifications currently in the system.

g) Network TCP/IP based Video Surveillance

The system shall provide IP video surveillance capability for up to 32 cameras. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

(1) Definitions

The system shall support the naming and definition of IP cameras. Required data for defining a camera shall include:

- Name
- Browser IP Address
- Control IP Address
- IP Port
- Camera Type

(2) Menu Order

The application shall provide a page for setting the order of the configured cameras on menus and pick lists.

(3) Presets

The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.

Camera preset positions must first be set at each camera web site. For setting up camera presets in the system it shall be necessary to enter the preset name and preset number exactly as it is entered on the camera's web site.

The application shall provide a toggle for designating a home preset position.

(4) Types

The system shall support IP video cameras from multiple manufacturers. The application shall provide a drop down pick list for selecting the camera type or creating a new type. Motion JPEGs shall be supported.

The system shall support at least the following camera types:

- Panasonic NM 100

- Panasonic NS 324
- Sony SNC-DF40N/P
- Sony SNC-P1
- Axis 2130
- Axis 205
- Axis 206
- Vivotek

The application shall provide fields for entering and editing camera command URLs. The command URLs that the application shall support include:

- Pan/Scan URL
- Pan URL
- Tilt URL
- Pan Tilt URL
- Zoom URL
- Preset URL
- Brightness URL
- Image URL
- Motion JPEG URL
- Assign Preset URL

(5) Views

The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras), and picture-in-a-picture (two cameras).

The application shall provide a drop down pick list for selecting current views or naming of new views. The application shall also provide a drop down pick list for the selection of the view type.

The application shall provide a pick list for selecting individual cameras for inclusion in a view.

(6) Video Management System

The system shall support the integration of digital video recorders supporting analog video cameras. This integration shall allow the viewing of live streaming video in the browser interface. Viewing live streaming video shall require the Java™ 2 Runtime Environment version 1.4.2 or version 5.0.

Events in the alarm subsystem can initiate video recording. Video motion detection, camera up and camera down messages from the VMS can initiate alarms.

It shall be possible to monitor DVR cameras in the same views as IP cameras. VMS events shall be logged in the system activity log. It shall be possible to view recorded video of events from the Activity Log.

h) System Administration

The system shall provide for the performance of system administration tasks from any network-connected computer with a browser. These administrative tasks shall include but not be limited to database backups, software updates, file cleanup, and configuring network resources. Most of the administrative, maintenance, and configuration utilities and functions shall require a system administrator with at least a "Setup" user role. Information from the network administrator shall, in many cases, also be required.

(1) Network Architecture

The system shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network connected PC with a browser. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

(2) Database Backups

The system shall create database backups each night at 00:15 hours. These backups shall be stored in ROM onboard the network controller, and written to network attached storage if such storage has been configured in the system. It shall also be possible to use FTP servers for these backups.

It shall also be possible for the system administrator to create such database backups at any time. Any database backups onboard the network controller may also be downloaded to off board storage by the system administrator at any time.

(3) Database Restore

The system shall be able to restore its database from a backup. Restoration of the system database shall only be possible from a backup copy onboard the network controller. It shall, therefore, be possible to upload a copy of a database backup from any network attached storage.

It shall be possible to review backups by date and description and select the desired backup for upload to the network controller or restoration as the current system database.

(4) Badge Design and Printing

The system shall include an integrated badging function. It shall be possible to design badge layouts, upload badge layouts for badge printing, capture ID photo images, print badges, and delete uploaded badge layouts.

It shall be possible for the system administrator to manage all badging functions entirely from within the browser.

(5) Card Format Decoding

The system shall include a card format decoding utility that presents a graphical view of the data on each card and assists in the discovery of card numbers, facility codes, and formats.

(6) Upgrades and Patches

Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these .tgz files. Update of the application software shall only be possible from an update file onboard the network controller. It shall, therefore, be possible to upload a copy of the software update from any network attached storage.

Software updates may involve the network controller only or may include updates for the node(s) also. The security system may be unavailable for several minutes during this process.

(7) File and Image Uploads

The system shall support uploads of files for use in and with the system. Files which shall be uploadable include:

- Floorplans in jpg format
- Badge layouts
- ID photos in jpg, gif, or png format
- Database backups
- Support.html to display installer and support contact info
- Software license files
- Software updates
- Threat level icons in jpg format

(8) File Cleanup

A utility shall be provided to assist in file cleanup. This utility will display for review and deletion all floor plan jpeg files, photo IDs, database backups, badge layouts, and software updates.

(9) System Shutdown

A utility shall be provided to perform an orderly system shutdown. The current security database will be stored onboard in ROM. The system will remain stopped until power is removed and reconnected. When the system reboots the security database image in ROM is read and used as the current database.

This function is intended for use when physically moving the system or performing hardware service requiring the disconnection of power.

(10) System Reboot

A utility shall be provided to perform a system reboot. Before the system shuts down it will store the current security database in ROM. When the system comes back up the security database image in ROM is read and used as the current database.

(11) Network Node Refresh

A utility shall be provided to refresh security database and configuration data to all nodes. Nodes will normally be refreshed automatically whenever the network controller has new data. However, it will be possible to force an immediate refresh of node data after changes have been made to the security database or configurations.

(12) Test Network Connection

A utility shall be provided to ping a known network IP address to check for connectivity between the security system network controller and other network devices.

(13) Get Node Messages File

A utility shall be provided that will fetch node messages files. These files may be requested by system support for diagnostic purposes.

(14) Reset AlarmTables

A utility shall be provided to reset all alarms and clear all event actions. Normally this should not be necessary. However, if an alarm persistently reappears then the alarm inputs involved should be investigated as they may have wiring problems. In such a case the system administrator may need to clear all alarms.

(15) Repair Database Tables

It shall be possible for a system administrator to execute a MySQL Repair Database Tables command. This command is designed to repair some data table corruptions that can occur.

(16) Backup System Files

The system shall contain a utility that backs up all system data files including the security database, uploaded ID photos, uploaded badge layouts, floorplan images, the uploaded support.html file and its image files, and configuration files. The system administrator shall be able to execute this backup.

(17) FTP Backup

The system shall support the use of an FTP Server for backups. Once configured, backups are automatically saved to the FTP server each night.

(18) Designating Domain Name Servers

The system shall support setting IP addresses for up to two domain name servers.

(19) Email Settings

The system shall support the use of email notifications of alarm events. The system administrator must setup the email server IP address or DNS name and the email address of the network controller. A network administrator must setup the network mail server to relay email for the IP address of the network controller.

(20) Defining Network Storage Locations

The system shall support the use of network attached storage devices. The network administrator must create a domain user account for the network controller and a password. The system administrator must configure the network attached storage in the system including the domain name, server IP address, share name, and the directory where the network controller may store data.

The system shall use the configured network attached storage for database backups, ID photos, database archives, and software updates.

It shall also be possible to setup FTP servers for backup storage.

(21) Setting Time Zone, Time Servers, and System Time

The system shall support the setting of time zones by selection off of a drop down pick list. An extensive list of world-wide time zones shall be provided. Adjustments for daylight savings time (summer time) shall be automatic.

The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the network controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

It shall also be possible to manually set the system date and time.

(22) Changing Operator Passwords

Person data maintained in the system may also contain a user name and password for logging on to the security application website as a system administrator. The system shall support the changing of administrator passwords. It shall be required to enter the password twice for verification purposes. Passwords may contain neither double-quote (") nor single-quote (') characters.

(23) Session Limits and Restrictions

The system shall support the restricting of system administration sessions to one IP address only. This shall ensure that if an IP address changes during a session that the user will be required to login again. This makes individual administrative sessions more secure.

The system shall support the setting of session timeout durations. If no monitoring or system administration activity is detected for the period of the session timeout duration then the administrator will be automatically logged off of the system. The duration for session timeout may be set to 30 minutes, 1, 2, 4, 8, or 24 hours.