INTRUSION/ACCESS/FIRE/INTEGRATED SYSTEM PERFORMANCE SPECIFICATION FOR DMP MODEL XR150/XR550 SERIES

1.0 GENERAL

1.1 Manufacturer

A. The manufacturer shall have at least forty (40) years of experience in the role of fire and security control manufacturing, and a proven track record of forward and backward compatibility for a minimum of thirty (30) years for its product's auxiliary devices, including system keypads, annunciation devices, zone expansion modules, and addressable detection devices.

B. The manufacturer must also manufacture receiving equipment that is compatible with standard dial-up telephone lines, network, and cellular network monitoring equipment that is compatible with a LAN, WAN, and the Internet. The receiving equipment shall be capable of receiving all status and alarm messages generated by the system. The receiving equipment shall be capable of updating the panel operating program and the system date and time.

C. Commercial/Residential Intrusion detection/Access Control /Household Fire Alarm Control Panelequipment manufacturer shall be:

Digital Monitoring Products, Inc. (DMP)
2500 N. Partnership Boulevard, Springfield, MO 65803
Telephone (417) 831-9362 FAX (417) 831-1325

1.2 Installer

A. The installing company shall show proof of having regular experience with design, installation, service, and maintenance of manufactured systems for a minimum of the last twelve (12) calendar months from the project start date. Each system installer and service person must provide manufacturer certification of technical training for installation, service, and system maintenance. Certification shall be proven with an official document issued by the manufacturer.

B. The installing company shall provide a minimum of 8 (eight) verifiable references from its clients where the manufacturer's system has been installed within the last twelve (12) calendar months from the project start date.

C. The installing company shall furnish and install a complete electrically supervised DMP panel, as detailed in this specification. The system shall be inclusive of all necessary function, monitoring, and control capability as detailed herein and on accompanying shop drawings.

E. The installing company shall become familiar with all details of the work, verify all dimensions in the field, and shall advise the Architect of any discrepancy before performing the work. Materials shall be installed in strict compliance with local building codes. All work shall be performed in accordance with Digital Monitoring Products, Inc. instructions. Components must be installed and serviced by a dealer in good standing that is factory-trained by Digital Monitoring Products.

1.3 Central Reporting Station

A. The central reporting station contractor must possess an Underwriter's Laboratory (UL) listing as a "Mercantile Police Station" or "Mercantile Burglar Alarm Systems" company. A copy of the listing shall be attached as apart of this bid package.

B. The actual alarm signal receipt and processing is a significant portion of the scope of work. Third party and/ or contract stations are permitted. UL must list the monitoring station for Protective Signaling Services or Central Reporting Station Signaling Services. A copy of the station UL listing shall be attached as part of this bid package.

C. The monitoring station must provide openings/ closing activity reports, activity day and time, authorized individual, office name and account number and the system type being monitored. These reports are to be mailed to the user's office at the end of each month. The Office Manager or Contract Administrator may request an additional report if an incident occurs.

D. The contractor must have a valid Alarm Operator License. A copy of licenses shall be attached as part of this bid package.

E. The contractor may be required to monitor a portion of the alarm systems by way of the end user data network.

F. The Contractor shall become familiar with all work details, verify all dimensions in the field, and shall advise the Architect of any discrepancy before performing the work.

G. The end user shall not incur any central station setup charges by the contractor to receive alarm signals by way of the end user data network.

2.0 SCOPE

2.1 Requirements

A. Furnish and install a complete Intrusion Detection/ Access Control system with the performance criteria detailed in this specification. The system shall be inclusive of all necessary functions, monitoring, and control capability as detailed herein and on accompanying Shop drawings.

On-site or remote video monitoring
Temperature threshold detection and monitoring
Pressure threshold detection and monitoring
Leak detection and monitoring
Tank level threshold detection and monitoring
Heating, air conditioning, and lighting management
Humidity threshold detection and monitoring
Power loss detection and monitoring, generator switching
Carbon Monoxide detection and monitoring

B. This specification document provides the requirements for the installation, programming, and configuration of a complete DMP panel. This system shall include, but not be limited to:

Control panel
System cabinet
Power supply
Digital Signaling Line Circuits (SLC)
Notification Appliance Circuits (NAC)
Annunciator/keypad bus
Batteries
Wiring
Conduit
Associated peripheral devices
Other relevant components and accessories required to furnish and install a complete and operational addressable system.

2.2 Standards

The system shall be listed as a Power Limited Device and be listed under the standards below. Each system shall be supplied with complete details on all installation criteria necessary to meet all of the listings.

Burglary Listings	**U.S. Government Standards/Listings**
• UL 1023 Household Burglar Alarm System Units	• Meets ICD 705 Chapter 7 Intrusion Detection Systems (IDS)
• UL 1076 Proprietary Burglar	• Meets DoD/NIST SCIF Standards
• UL 1610 Central Station Burglar Alarm Units	•NIST Validated XR550E Encrypted Panel
• UL 1635 Digital Burglar Alarm Communicator System Units	**Intertek (ETL) Certifications**
Fire Listings	• EN 50130-4 EMC Product Family Standard: Immunity Requirements for Components of Fire, Intruder and Social Alarm Systems
• UL 985 Household Fire Warning	• EN 50130-5 Environmental Standards
• UL 864 Commercial Fire Warning	• EN 50131-1:2006+A1 Intrusion and hold-up systems
Access Control Listings	• EN 50131-3:2009 Control and Indicating Equipment
• UL 294 Access Control System Units	• EN 50131-5 Interconnections Equipment using Radio Frequency techniques
Related Standards	• EN 50131-6:2008 Power Supplies
• NFPA 70 National Electric Code (NEC)	• EN 50133-1:1997 Access Control Systems
• NFPA 72 Household Fire Warning	• EN 50136-1 Alarm Transmission Systems and Equipment
• System Monitors	• EN 50136-2:2013 Supervised Premises Transceiver
• System Events	• EN 50136-3 Receiving Centre Transceiver
	• EN 50131-6 Power Supplies

International Standards

The system shall carry the Intertek Tick mark with the following standards in the scope of the certificate. The system shall meet Grade 3 requirements.

2.3 Americans with Disabilities

All indicating and notification appliances shall comply with the Americans with Disabilities Act (ADA) requirements.

3.0 SUBMITTALS

3.1 General Requirements

The contractor shall submit three (3) complete sets of documentation within thirty (30) calendar days after contract award date. Indicated in the document shall be the manufacturers' names, catalog number, type, size, style, rating, and catalog data sheets for all items proposed to meet these specifications.

3.2 Shop Drawings

Shop drawings shall be submitted in accordance with Section 3.0 Submittals and shall consist of a complete list of equipment and materials, including manufacturer's descriptive and technical literature, performance charts and curves, catalog cuts, and installation instructions.

3.3 As-Built Drawings

The contractor shall provide a complete set of as-built drawings for the entire system upon installation completion. These drawings shall include, but not be limited to, the exact locations of all equipment, connections between all equipment, and wiring for all equipment as the system is installed.

3.4 Spare Parts Data

After shop drawings are approved, and not later than thirty (30) calendar days prior to the date of beneficial occupancy, a list of spare parts data for each item of specified materials and equipment shall be submitted. The data shall include a complete list of parts and supplies with current unit prices and source of supply. Spare parts shall consist of, but not be limited to, five (5) percent of all initiating and notification appliances with a minimum of one (1) each. All spare parts shall be on site prior to commencement of acceptance testing. Depleted spare parts shall be replaced prior to beneficial occupancy.

3.5 Operating Documents

The contractor shall furnish to the architect operating instructions outlining the step-by-step procedures required for system start-up, operation, and shutdown at least thirty (30) calendar days prior to acceptance test. The instructions shall include the manufacturer's name, system model number, service manual, parts list, and a description of all equipment and their basic operating features.

3.6 Maintenance Documents

The contractor shall furnish maintenance instructions listing routine maintenance procedures, possible breakdowns and repairs, and troubleshooting guides at least 30 calendar days prior to acceptance test.

3.7 Performance Test Reports

Upon the installed system completion and testing, test reports shall be submitted in booklet form showing all field tests performed to prove compliance with specified performance criteria.

3.8 Warranty

A copy of the manufacturer's warranty for all equipment and materials shall be provided. Warranty shall be for all equipment, materials, installation, and workmanship for a minimum of three (3) years, unless otherwise specified.

4.0 GENERAL COMPONENT REQUIREMENTS

4.1. Component Enclosure

Housings; power supply enclosures, terminal cabinets, control units, and other component housings, collectively referred to as enclosures shall be so formed and assembled as to be sturdy and rigid. If sheet steel is used in the fabrication of enclosures, it shall be not less than an 18-gauge door with a 20-gauge box frame. Where exposed pins, the hinges shall be of the tight pin type or the ends of hinge pins shall be tack welded to prevent ready removal. Doors having a latch edge length of less than 24 inches shall be provided with a single lock. Where the hinged door latch edge is 24 inches or more in length, doors shall be provided with three-point latching device with lock; or alternatively with two locks, one located near each end. For SCIF and High Security applications an attack proof enclosure with proper tampers listed for use with the XR150/XR550 with Network and Encryption shall be used.

4.2 Electronic Components

A. All system electronic components shall be solid-state type, mounted on printed circuit boards. Light duty relays and similar switching devices shall be solid-state type or electromechanical.

B. The panel shall have an over current notification LED that lights when devices connected to the Keypad Bus and Loop Expansion LX-Bus(es) draw more current than the panel is rated for. When the over current LED lights, the Loop Expansion LX-Bus (es) and Keypad bus are shut down.

4.3 Control Unit

A. A battery test shall be automatically performed to test the integrity of the standby battery. The test shall disconnect the standby battery from the charging circuit and place a load on the battery. This test shall be performed no more than every 180 seconds.

B. The control unit shall be capable of operating and supervising notification appliance devices as well as addressable initiating detection devices and an integrated supervised dual line digital communicator.

C. Control unit must be “Flash ROM” updatable, and program must be held in non-volatile RAM. The panel shall be able to function while the update is in process.

D. Control unit shall be capable of operating using an optional built in Encrypted Alarm Router for SCIF (Sensitive Compartmented Information Facility) applications that is certified by NIST (National Institute of Standards and Technology) for 128- & 256-Bit AES (Advanced Encryption Standard) Encryption communications.

E. The optional built-in Encrypted Alarm Router shall be capable of compliance with ICD 705 Chapter 7 Intrusion Detection Systems (IDS) and UL 2050 standards.

4.4 Remote Annunciators

A. The system shall support a maximum of sixteen (16) supervised remote annunciators with the identical capabilities, functions and display layout. Operation of the remote annunciators shall be limited to authorized users by the use of a code or key.

B. The remote annunciators shall be capable of operating at a maximum wiring distance of 15,000 feet from the control unit on unshielded, non-twisted cable.

4.5 Control Designations

Controls shall be provided to ensure ease of operation of all specified characteristics. Where applicable, clockwise rotation of controls shall result in an increasing function. Controls, switches, visual signals and indicating devices, input and output connectors, terminals and test points shall be clearly marked or labeled on the hardware to permit quick identification of intended use and location.

4.6 Test Modes

A. The system shall include a provision that permits testing from any alphanumeric keypad. The test shall include standby battery, alarm bell or siren, and communication to the central station.

B. The system shall include a provision for an automatic, hourly, daily, weekly, thirty (30) day, or up to sixty (60) day communication link test from the control panel installation site to the central station.

C. The system shall include a provision for displaying the internal system power and wiring conditions. Internal monitors shall include the bell circuit, AC power, battery voltage level, charging voltage, panel box tamper, phone trouble line 1, phone trouble line 2, transmit trouble, and network trouble.

4.7 Power Supplies

A. Power supplies for the control unit shall operate from 120 VAC, supplied at the respective protected areas. Standby batteries shall be supplied to power the system in the event of a utility power failure. Batteries shall be sized to provide 105% capacity for eight hours. Standby batteries shall be sealed lead-acid. Power supplies shall be all Solid State.

B. Controls shall be designed to maintain full battery charge when alternating current is available. Batteries shall be recharged to 85% capacity within 24 hours from battery use. The system shall be automatically transferred to battery power upon loss of alternating current power and return to alternating current power upon restoration. Intrusion alarms shall not be initiated during switch over; a signal shall be initiated upon failure of battery or alternating current power.

C. Approved power supplies shall meet or exceed the following power supply model specifications:

UL Listed DMP 505-12: 12VDC 5 Amp with transformer and enclosure.

4.8 Software

A. The system shall interface with computer software with the capability to fully program the panel by connecting to the panel through:

Direct cable connection interface card

Receiver phone line connection

Standard phone line connection

Ethernet network connection

Network connection across the Internet

B. The system shall interface with computer software capable of locking down all controlled doors.

C. The system shall interface with computer software capable of monitoring and logging all events.

D. The system shall interface with computer software or Cloud-based managed software or mobile app accessible by a standard web browser using a login and password and requiring the system user code or PIN code upon remote login to be capable of exporting reports in the following file formats:

Excel spreadsheet (*.xls)	Comma-separated (*.csv)

E. The system shall interface with computer software capable of printing custom, filtered reports including:

All Events	Door Access Granted
Zone Action	Door Access Denied
Arming/Disarming	Opening/Closing Schedule Changes
Area Late to Close	System Monitors
User Code Changes	System Events

4.9 Graphic User Interface (GUI)

Entré – Access and Security Management Software

System Features:

A. The software shall be available in three package sizes.

Entré Lite™: Shall have 16 doors included, and a maximum of four XR150/XR550 Series panels, personnel management, full reports, and event management.

Entré Business™: Shall have the same features as Entré Lite with the option of expansion to 96 doors maximum and up to 24 XR150/XR550 Series panels.

Entré Enterprise™: Shall have the same features as Entré Business with 96 doors included with the ability to expand to an unlimited number of doors, users and XR150/XR550 Series panels.

B. Shall have simple user management, with the ability to import users from existing databases.

C. Shall be able to assign user access by group, facility or other parameters.

D. Shall have drop down lists for devices, user data and other information to facilitate fast and accurate searches.

E. Shall be able to view system status in one of a variety of views for simplified alarm monitoring management.

F. Shall have the capability to customize reports for added flexibility.

User Management:

A. It shall have the ability to import into Entré from existing systems via standard comma-separated value (CSV) format files. It shall easily add new users, capture and edit their photo for badging or visual verification from within the application.

B. User fields shall be fully customizable. Assign specific rights or events by user or by group. The software shall be able to create effective/expiration time for users, limiting access to only certain times of the day, and only certain days, or for only a defined period of time.

AES Encryption:

A. Entré Enterprise shall support the XR150/XR550 Series with Encryption panel AES (Advanced Encryption Standard) strong data security for sensitive personnel and facility data.

Highly Customizable:

A. The software shall be extensively customizable to create a system that matches the end user's application's needs.

B. Shall define what events are considered "alarms," and what response is required from the system operator.

C. Shall be able to tailor user data with up to 20 available user-defined fields.

Hierarchical Views:

A. The software shall have the ability to select from four different system views, with the ability to have multiple views open simultaneously. Select the graphical Map view, tabular Event view, or hierarchical Tree view.

B. The software shall be able to click on a device or alert to access additional information and process the event. In text-based views, software shall have simple drill downs to allow fast navigation to the desired item.

Powerful Search:

The software shall employ industry standard SQL database for quick and easy search to identify any desired device or user which is compatible with nearly any database.

Single-System Control:

The software shall employ a network solution to manage installations and users from any location. A single, unified database means there's one badge, one face or one fingerprint, worldwide.

Entré – Access & Security Management Software

Features Included:

Automation Module

Single Sign-SO

Personnel Image Capture

Badge Designer

Signature Capture

Optional Modules:

ENTRE-4DR Additional 4-Doors

ENTRE-16DR Additional 16-Doors

ENTRE-32DR Additional 32-Doors

ENTRE-64DR Additional 64-Doors

ENTRE-128DR Additional 128-Doors

ENTRE-BADGE Badge Designer

ENTRE-CLIENT Operator Concurrent License

ENTRE-xxxxxx (EXACQ, 3 VR, VERINT) DVR Modules

ENTRE-PART Database Partitioning

ENTRE-LANG Multi-Language Module

Optional System Modules Features:

A. Shall be able to Point-and-click control of alarms and devices.

B. Shall have a modular design to enable customization, with optional modules for added features.

C. Shall be available in French, Spanish, or English, with dual- language operation mode.

D. Shall have full reporting, including at-a-glance dashboard graphics and charts or traditional tabular displays, with the ability to produce reports in a variety of file types.

E. Shall have DVR integration.

F. Shall have image management of users and event photos.

G. Shall have a custom badge builder and video badging.

Door Modules:

The software shall allow for the addition of additional doors to support Entré Business or Enterprise systems.

Alarm Graphics:

A. The software shall allow for the addition of additional doors to support Entré Business or Enterprise systems.

B. Shall have the ability to give graphical representation of events and alarms at-a-glance and give feedback of system status.

C. Shall have the capability to upload an unlimited number of graphical images of protected facilities in a variety of file formats.

D. System maps are linked from level to level, allowing drill down from a macro view to a specific room or area.

E. View alarm status at every level of zoom.

F. User-defined layers representing different alarm types allow you to customize the graphical interface to meet application needs.

G. Once loaded, it shall have the ability to plot alarm devices on the graphics using drag-and-drop selections from a hierarchical list of hardware. Identify the areas on your site maps, defining them by Classification, Entrances, Zones, and Partitions.

H. It shall have total picture-based monitoring and control of the system. It shall from facility-wide views be able to click to zoom in on any area of the facility and view the real-time status of any device.

I. The software shall be able to click on the alarm display icon to acknowledge an alarm or to request additional information

Automation Module:

A. The software shall be able to give advanced users the power to create automated system actions.

B. The software shall be able to define automatic responses to any system alarm or events. These include generating a report, generating an alert email, or sending commands to selected devices.

C. Shall be able to create scheduled system actions to run once at a specified time and date, or scheduled events that repeat at user defined time and date intervals.

D. System automation enables configuration of unattended activities, freeing system managers from many routine responsibilities.

DVR:

A. The software shall be able to quickly connect to a DVR to review video based on a received alarm from a control panel.

B. Connect to DVR from a graphical map of the area to review activity.

- Verint

  NetDVR I, firmware 6.47.x or higher

  NetDVR II, firmware 8.7.x or higher

  EdgeVR, all firmware versions

- 3VR

  E-Series P-Series S-Series ServerClass

  3204 Digital Video Recorder (3000 Series)

  4000 C NVR (4000 C Series)

- Exacq

Database Partitioning:

A. The software shall allow system information to be contained in a single unified database allowing system managers to limit user access to only certain areas of the database to partition the information.

B. The software shall allow organization of data into separate collections by physical area, hardware types, events, or other parameters.

Multi-Language:

A. The software shall support multiple languages enabling multiple operators to select a language during their login process. The software shall allow text shown both in English and a second selected language.

B. Available languages shall include:

English French Spanish

Single Sign-On:

A. The software shall provide single sign-on for users, enabling them to use one password to access multiple system services.

B. Badge Image Capture:

The software shall allow the transfer of pictures of users from a digital camera directly onto a badge. Select a TWAIN source to capture the image to allow up to date images on employee badges.

Badge Designer:

A. The software shall have the ability to create one or more badge designs, customizing badges by facility, user level, or other parameters.

B. When badging employees or visitors, select the desired badge template from library. The template automatically populates with the appropriate data, ready for printing.

Signature Capture:

Shall use a signature capture device to provide the ability to capture employee or visitor signatures and store the images.

Reporting Dashboard:

A. The software shall have interactive graphics for instant feedback on system activity.

B. The software shall be able to choose a number of charts for functions such as Access Granted / Denied at a particular access point or an entire facility to get a snapshot of activities within any defined time period.

C. Shall have ability to filter through user, activity, or event data to narrow results and show precisely the information needed.

D. Shall have the ability to view reports from within the application, or saved and exported to PDF, HTML, XLS, CSV, or XML format for distribution.

E. Shall automate custom reports to generate and distribute each day at desired times.

4.10 Control Panel Capability

A. The basic control panel shall provide:

Expansion to a total of at least 10,000 user codes with 99 user profile definitions.

Temporary user codes that can be entered with a finite date and specific time to expire.

Sixteen (16) independent door/keypad addresses, each with four zones on XR550 with eight (8) on the XR150.

Thirty-two (32) doors of access expandable to ninety-six (96) doors of access from one XR550 Control Panel.

A total door access granted event buffer of at least 10,000 events.

Anti-pass back access control selectable by area and user.

A total of at least 99 programmable Schedules for output relay schedules, area schedules, door schedules, holiday schedules, and user profiles. The same schedule may be assigned to more than one area, door, or output, making them reusable. There shall be at least two schedules per user profile with up to four profiles per user. Up to 8 Schedules per user, per door, per area, and per output.

Eight Areas (8) individual reporting areas XR150, and thirty-two (32) individual reporting areas XR550.

Built-in bell and telephone line supervision.

B. The networked control panel shall provide the entire above plus:

All of the above features plus.

Require Dual Authority. Require two user code entries to disarm and/or allow door access to this area.

Support programming to require the same or different access code entered within a programmed delay time of 1 to 15 minutes after disarming before activating a silent ambush alarm.

Early Morning Ambush. Must disarm a second time with in a programmed period of time or an early morning ambush silent alarm is sent.

Bank Safe & Vault features. Schedules set for this area and the time of day cannot be changed while the area is armed.

C. The encrypted control panel shall provide the entire above plus:

All of the basic and network features listed plus.

Built-in Encrypted Alarm Router.

Certified operation that meets 128- & 256-Bit AES (Advanced Encryption Standard) Encryption.

Certified operation that meets SCIF (Sensitive Compartmented Information Facility) application needs.

Certified operation that meets NIST (National Institute of Standards and Technology) standards.

- Certification that encrypted panel is capable of meeting ICD 705 Chapter 7 Intrusion Detection Systems (IDS) Standard.

Certification that encrypted panel is capable of meeting UL 2050 standards.

Card plus Pin for High security card access is provided by the Card Plus Pin feature that requires both a card read and a PIN (4-6-digit user ID) entry for arming/disarming and access by area. This Card Plus Pin operation complies with the ICD 705 requirement for dual id authentication and operates with a DMP Prox Keypad and a Prox reader with the keypad connected to a DMP Wiegand Interface module.

Panic Test allows the panic zone test verification and failure results to be sent to the central station receiver.

Passphrase of 8-16 characters to validate encryption between the XR550 with Encryption and the Central Station Receiver.

5.0 FUNCTIONAL DESCRIPTIONS

5.1 System Description

A. The system areas and zones shall be programmable, and the system shall store, log, display, and transmit specific custom designations for system areas, zones, and user names.

B. To ensure continued, one-call support, the system shall be constructed of sensing components provided directly by the system manufacturer, such as power supplies, motion detectors, door and window position switches, glass break detectors, or other sensing devices that the manufacturer offers.

C. The system controller, user interfaces, zone input devices, relay output devices, and the system signal receiving equipment shall be engineered, manufactured, assembled, and must be distributed from a location within the United States of America.

D. The system shall support user interaction by way of a keypad, web browser, system software, key switch, or radio frequency wireless control, Text messaging, or Smart Phone Application using integrated or auxiliary devices provided by the system manufacturer.

E. The system shall support controller zone input connections, system keypads, system zone expansion modules, and wireless zone input modules, and must support zone input connections by way of at least two competitive products. The system shall offer a seamless integrated compatibility with hard-wire and/ or wireless zone expansion equipment for at least 500 wireless zones and/ or a maximum of 574 hardwired zones.

F. The system shall be capable of offering up to five zone expansion buses, each of which can support the connection of up to 15,000 feet of four-wire cable. Zone expansion and keypad data buses that exceed 2,500 feet of cable must include splitter/repeater modules to boost data voltage and maintain data integrity.

G. The system shall provide a seamless capability to provide up to 506 addressable relays, which can be located at any connection location upon a zone expansion bus.

H. System relay outputs shall have the capability of being triggered as a result of a command from the user interface, changes in system status, changes in zone status, or by a programmable schedule.

I. System relay output states shall be programmable for momentary, maintained, pulsed, or must follow the state of an associated system zone input.

J. The system shall be completely programmable either locally from a keypad or remotely through a standard dial-up, and network connections by way of a LAN, WAN, and/or by way of the Internet, cellular communications paths.

K. The control unit shall be completely programmable remotely using remote annunciators, and/ or using upload/ download software that communicates using SDLC 300 baud, 2400 baud, or IP Addressed data network. On-site programming from a personal computer shall also be permitted.

L. The control unit shall be equipped with an anti-reversing circuit breaker to prevent damage due to accidental reversal of battery leads.

5.2 Input/output Capacity

A. This system shall be capable of monitoring a maximum of 574 individual zones and controlling a maximum of 506 output relays.

B. The control panel shall have, as an integral part of the assembly, 2 SPDT Form C relays rated at 1 Amp at 30 VDC and four open collector 12 VDC outputs rated at 50mA each. It shall also have the capacity of a maximum of 125 output expander modules with 500 switched ground, open collector outputs, 50mA maximum and 506 auxiliary relays (Form C rated at 1.0 Amp at 30 VDC).

C. The panel shall also provide 99 programmable output profiles for schedules, and include an integral bell alarm circuit providing at least 1.5 Amps of steady, pulsed, or temporal bell output. Output type shall be programmable by zone type. Relays and voltage outputs shall be capable of being independently programmed to turn on and/or off at selected times each day.

D. The system shall be capable of supporting and controlling up to 140 Z-Wave devices and up to 20 Z-Wave Favorites for group control.

5.3 User/Authorization Level Capacity

The system shall be capable of operation by 10,000 unique Personal Identification Number (PIN) codes with each code having one (1) of ninety-nine (99) custom user profiles. This allows for limitation of certain functions to authorized users. The operation of all keypads shall be limited to authorized users.

5.4 Keypads

A. The system shall support a maximum of sixteen (16) keypads on XR550 or eight (8) keypads on XR150 series with alphanumeric display. Each keypad shall be capable of arming and disarming any system area based on a pass code or Proximity key authorization. The keypad alphanumeric display shall provide complete prompt messages during all stages of operation and system programming and display all relevant operating and test data.

B. Communication between the control panel and all keypads and zone expanders shall be multiplexed over a non-shielded multi-conductor cable, as recommended by the manufacturer. This cable shall also provide the power to all keypads, zone expanders, output expanders, and other power consuming detection devices.

C. If at any time a keypad does not detect polling, the alphanumeric display shall indicate “SYSTEM TROUBLE”. If at any time two devices are programmed for the same address, the alphanumeric keypad shall display “4 WIRE BUS TROUBLE”. If at any time a keypad detects polling but not for its particular address, the alphanumeric display shall indicate “NON POLLED ADDR”. The system shall display all system troubles at selected keypads with distinct alphanumeric messages.

D. The keypad shall include self-test diagnostics enabling the installer to test all keypad functions: display test, key test, zone test, LED test, relay test, tone test, and address test.

E. The keypad shall provide an easy-to-read English text display. The text shall exactly match the text seen in all software reports, keypad displays, and central station reports.

F. The keypad user interface shall be a simple-to-use, menu-driven help system that is completely user friendly.

G. The control panel shall support a keypad interface accessible on the World Wide Web in a browser window. The web-accessible keypad interface shall provide at least five (5) programmable hyperlinks for camera access or other use.

5.5 Zone Configuration

A. A minimum of 4 Class B ungrounded zones shall be available at each keypad or zone expander on the system. The system shall have the capacity for a maximum of sixteen (16) keypads and a maximum of 125 four (4) zone expanders or 500 single zone expanders on the XR550. It shall also have the capacity of a maximum of 125 supervised relay output expanders. The XR150 shall have the capacity for a maximum of eight (8) keypads and a maximum of 25 four (4) zone expanders It shall also have the capacity of a maximum of 25 supervised relay output expanders. All Class B zones shall be 2-wire, 22 AWG minimum, supervised by an end-of-line (EOL) device and shall be able to detect open and short conditions in excess of 500ms duration.

B. Each zone shall function in any of the following configurations: Night, Day, Exit, Fire, Supervisory, Emergency, Panic, Auxiliary 1, Auxiliary 2, Fire Verification, Cross Zone, Priority, and Key Switch Arming.

C. The digital SLCs and the annunciator/keypad bus shall be able to operate at a maximum wiring distance of 2500 feet from the control panel on unshielded, non-twisted cable. This distance may be extended to a total of 15,000 feet when bus repeater modules are installed.

D. Each zone shall function in any of the following configurations:

Night	Supervisory	Auxiliary 1	Cross-Zone
Day	Emergency	Auxiliary 2	Priority
Exit	Panic	Fire Verification	Arming
Fire	Doorbell	CO	

5.6 Communication

A. The system shall be capable of signaling to as many as 8 remote monitoring station receivers. Seven (7) of the eight (8) paths shall be capable of being assigned as either a “primary” or “backup” path. In such a manor the system shall have multiple primary paths to multiple remote monitoring stations as well as multiple backup paths to multiple monitoring stations.

B. The system shall employ Adaptive Technology that allows a Backup communication path programmed for Network or Cellular to automatically ADAPT to the faster check-in rate of the Primary path should the Primary path become unavailable. This creates a seamless transition for communication.

C. The system shall be capable of dialing up to (2) remote monitoring station receivers, four telephone numbers of 32 digits each using two separate switched telephone network lines such that if two unsuccessful attempts are made on the first line to the first number, the system shall make two attempts on first line to the second number. If these two attempts are unsuccessful, the system shall make two further attempts on the first line of the first number. After the tenth unsuccessful attempt, dialing shall stop and the alphanumeric keypad shall display trouble. Should another event occur that requires a report to be transmitted, the dialing sequence shall be repeated. The system shall have a programmable option to dial a second set of telephone numbers after the first ten attempts using the same sequence.

D. The system shall be capable of communication using the IBM Synchronous Data Link Control format, and at least one other standard industry format.

E. The system shall be capable of supporting Network communication with digital dialer backup, existing Ethernet data networks, satellite communication, fiber optic networks, local area networks, wide area networks, cellular communication, and retail data networks.

5.7 Network Communication

A. The control panel shall be capable of asynchronous network communication with a retry time between 2 and 240 minutes and a fail time of 2 and 240 minutes. If communication is unsuccessful the control panel shall be capable of attempting backup communication through any of the available communication methods to the same receiver or a backup receiver.

B. The control panel shall employee adaptive communication technology. Adaptive Technology allows a Backup communication path programmed to use Network or Cellular to automatically ADAPT to the faster check-in rate of the Primary path should the Primary path become unavailable, creating a seamless transition for communication of messages. Select Adapt when programming the Checkin option. This allows a system to be fully supervised even if a path fails, while also keeping wireless charges low when the network is good.

C. Network communication between the control panel and the receiver shall be in a proprietary communication format.

D. The control panel shall be capable of supporting Dynamic Host Communication Protocol (DHCP) Internet Protocol (IP) addressing.

E. Underwriters Laboratories (UL) shall list network communication by the control panel for Standard or Encrypted Line Security.

F. The control panel shall be capable of two-way network communication using standard Ethernet 10/100 BaseT in a LAN, WAN, or Internet configuration.

G. The control panel shall be capable of communication by means of a 128- & 256-Bit AES (Advanced Encryption Standard) Encryption process certified by NIST (National Institute of Standards and Technology) to an SCS-1R receiver with a built-in Encryption Alarm Router or SCS-VR.

H. The control panel shall be capable of meeting ICD 705 Chapter 7 Intrusion Detection Systems (IDS) and UL 2050 standards.

I. The control panel shall be capable of sending text messaging to up to three Cellular Phone Numbers using cellular communications.

J. The control panel shall be capable of sending the following Text messages:

Zone Alarms by Zone Name	AC Power Trouble and Restoral
Zone Troubles by Zone Name	System Low Battery
Zone Bypass by User	Ambush
Arming (Closings) by User	Abort, Cancel and Alarm Verified by User
Disarming (Openings) by User	Check-in by user
Late to Close	

5.8 Cellular Communications

A. The control panel shall have the capability to communicate with a plug-in cellular communicator model number 263LTE-V or 263LTE-A that shall plug into the control panel J24 connector which shall supply full data communication and power to the cellular communicator. The cellular communicator shall be capable of communicating full panel alarm and auxiliary messages to the DMP SCS-1R Central Station or SCS-VR Receiver as well as SMS text messaging to a PC, PDA, or Cellular telephone.

B. The control panel shall be capable of sending the following SMS messages

Zone Alarms by Zone Name	AC Power Trouble and Restoral
Zone Troubles by Zone Name	System Low Battery
Zone Bypass by User	Ambush
Arming (Closings) by User	Abort, Cancel and Alarm Verified by User
Disarming (Openings) by User	Check-in by user
Late to Close	

5.9 TCP/IP Network Trapping

A. The control panel shall be capable of having communication set to Network operation. When a trap is set in Remote Link, the software shall be capable of sending a panel trap message with the panel account numberto the SCS-104 installed in an SCS-1R receiver.

B. The receiver SCS-104 shall store the trap and monitor the panel for the next message. When the panel sendsits next message, the receiver SCS-104 shall then send a message to the panel to contact Remote Link at the IP address contained in the original trap message.

C. The trap message shall be stored in the receiver SCS-104 for up to four hours. If the trap message is not sent to the panel within the four-hour window, the panel trap message shall be discarded and a new trap messagemust be sent from Remote Link.

D. The user shall be able to view the trap status in the receiver SCS-104 in Remote Link using the Trap Query function.

6.0 INTEGRATED INTRUSION ALARM AND ACCESS CONTROL OPERATION

6.1 Access Authority Levels

The system shall be capable of programming access credentials authority levels to check whether the user has access to a specific area and also has the authority to disarm or arm the area. If the user access credential has access and disarm/arm authority the system shall provide the user the option to disarm the area simultaneously upon opening the door, or to open the door and begin an entry delay timer. With the timer option the user then disarms the area using an intrusion control keypad inside the area. If the user only has access authority to the area and the area is in an armed condition, the user is denied access to the area.

6.2 Door Open Schedule Override

The system shall be capable of programming certain area doors to be scheduled to unlock and lock at specific times of the day or night. The lock/unlock function shall be capable of an override option depending upon the area armed/disarmed status. If the area remains in an armed status at the scheduled unlock time the armed status overrides the unlock schedule ensuring the doors remain locked and armed in situations where the business might open late, close early, is affected by inclement weather, or another emergency.

6.3 Common Area

The system shall be capable of programming a common area to be armed when the last area in the system is armed and disarmed when the first area in the system is disarmed. To ensure the common area works properly it shall not have any user codes assigned to the common area. The system shall also be capable of programming multiple common areas.

6.4 Area Access Control

A. The system shall be capable of integrating area access control capability where specified into the same control panel with the ability to have up to 10,000 user credentials. User access is limited to custom profiles and/or schedules. Anti-passback shall be available. The networked version shall support a Two-Man Rule feature. The system shall support up to ninety-six (96) access doors, connected to the system using a manufacturer-approved interface module.

B. Area door access products shall meet or exceed features offered by the following products:

1. Keypad reader/administration device – DMP Model 7063/7063A, 7073/7073A, 7163/7173, 7872, 7873, 1301I, 1301N, 1301P
2. Access Control Module – DMP Model 734, 734N, 1134, 734N-POE
3. Reader – DMP Model PP-6005B, PR-5455, MP-5365, P-300-H-A, P-500-H-A, P-640-H-A, PR-5355-AGK14, Farpointe Data Readers: DMP Model P-300-H-A, P-500-H-A, P-620-H-A, Reader & Keypad – DMP Model P-640-H-A, Contactless Smartcard Reader – DMP Model Delta3, Delta5 and Delta 6.4
4. Cards or credentials – DMP Model 1326/10, 1306P/10, 1346, 1386/10, PSC-1-H/10, PSC-1-H/100, PSK-3-H/10, PSK-3-H/100, PSM-2P-H/10, Farpointe Data: MIFARE DesFire EV1 Smartcard – DMP Model DE2, Bluetooth Reader – DMP Model CSR-35P, Mobile Access Credential – DMP Model CMC-2

6.5 Access Control Equipment

Access Control equipment shall communicate to the system by way of the control panel keypad bus. The equipment shall have a three (3) year warranty and meet or exceed features offered in the products listed in Section 11.5 of this document.

6.6 Early Morning Ambush (XR550 only)

A. The system shall be capable of programming an area to require two user codes be entered within a programmed number of minutes to prevent an ambush message from being sent to the Central Station Receiver. If both user codes are not entered within the time an ambush message is sent to the central station receiver.

B. Both user codes shall have the authority to disarm the specific area and must be entered at the same keypad or reader. The keypad shall not display any indication that the ambush timer is running.

C. The system shall be capable of programming an output to provide an external indicator that an ambush situation is taking place.

6.7 Dual Authority (XR550 only)

The system shall be capable of programming an area to require two separate user codes be entered in order to disarm and/or allow access to a specific area. Both required codes shall have at least the same or greater authority level. Both required codes shall be entered within 30 seconds or an alarm shall activate.

6.8 UL Bank Safe & Vault Operation (XR550 only)

The system shall be capable of being programmed to only be disarmed during scheduled times regardless of the authority level of any user code or user profile in the system. The schedule and time and date set for this area shall not be capable of being changed while the area is armed. Zones assigned to Bank Safe and Vault areas shall not be able to be bypassed or force armed.

6.9 Panic Button Summary Test

A. The system shall have the ability to test panic buttons without sending a panic alarm to the Central Station Receiver.

B. The system shall also have the ability to send panic zone test verification and failure results to the Central Station Receiver.

C. During the test, each time a panic zone trips, the display number shall increment and the keypad buzzer sound for two seconds.

D. The number of panic zones tripped shall constantly display until the test ends or no panic zone activity has occurred for 20 minutes.

E. When the Panic Zone Test ends and a zone failed (did not trip) during the test, the keypad shall be able to display the zone name and number and have the buzzer sounds for one second. Additional zone failed zones shall display when a button is pressed.

6.10 Panic With Credential

The system shall support a one-button key fob with a built-in proximity credential that shall also be used to send a panic alert. Its primary function shall be for regional personnel who work at multiple locations. This device shall be supervised at a single monitoring center using an SCS-VR Virtual Receiver. Panic Supervision shall be enabled in Panel Programming and each fob's serial number shall be programed into the appropriate work location's panels. This device shall send a "Key Fob is Alive" message every seven days to any panel in which it is programmed. If no check-in message is received from the fob after 30 days, the monitoring center shall send a "Key Fob is Missing" alert. "Low Battery" messages shall also be received at the monitoring center.

6.11 One-man Walk Test

A special code is also available for installers to test the system. The One-Man Walk Test feature allows a single technician to check the panel response to burglary, fire, panic, and supervisory zones.

6.12 Multi-lingual Display Option

The system shall be programmed to display the User Menu and Status Display text in multiple languages.

6.13 User Inactivity Audit

System shall allow user code inactivity to notify the central station after a programmable period of days of no activity. The system shall be programmable from 0-425 days.

6.14 Lock Down

The system shall for emergency situations, a lock down command can be issued from the keypad menu or via remote command and locks all doors designated as public.

6.15 Communication Function Diagnostics

The system shall have enhanced diagnostic menu that enables technicians to check network and cellular communication status and cell signal strength from the keypad.

6.16 GUEST Operation

The system shall be capable of in the Home/Sleep/Away with Guest House operation, create up to three separate systems (main and two guests). Keypads in each system can selectively arm the perimeter, interior, or bedrooms for only their protected areas. Main system users can add authorized users to all protected areas, but guests can add users only for their protected system.

7.0 FALSE ALARM REDUCTION FEATURES

The system shall be capable of providing false alarm reduction features, functions, capabilities, or processes that either require alarms be verified or potential alarms be corrected before a system or zone can be placed into an armed state.

7.1 Exit Error Alert and Reporting

The panel shall be able to provide an automatic function to prevent a false alarm from occurring if an exit door does not properly close after the system is armed.

7.2 Entry and Exit Delay Annunciation

A. When arming, the system shall provide clear annunciation indicators to the user about the need to exit the premises prior to the exit delay time expiring.

B. When disarming, the system shall notify the user the need to disarm the system prior to the entry delay time expiring.

7.3 Remote Annunciation

The system shall be able to provide entry and exit delay time period notification. This notification can be from DMP keypads, remote annunciators, or bell tests.

7.4 Abort Reporting

The system shall be capable of sending an Abort report to the central station if the system is disarmed while the alarm is still sounding. The Abort report shall be sent after the alarm report to notify the central station that an authorized user has cancelled the alarm.

7.5 System Testing

The system shall offer testing features that are simple, quick, and complete and provide the highest measure of safety by ensuring that alarm conditions are detected and communicated to the proper authorities in a timely manner and on a regularly scheduled basis.

7.6 Ambush Code

The system shall offer ambush codes for those dangerous encounters where the user is instructed to either arm or disarm the system under threat of harm. The duress code shall disarm the system without giving local indication of an alarm that might put the user well-being in jeopardy.

7.7 Two-Button Panic Feature

The system shall support DMP keypads that provide the option to use only two-button panic codes. The user shall be required to press and hold two designated keys for approximately two seconds before the system generates a panic alarm.

7.8 Fire Verify Zones

The system shall support Fire Verify zones to help the panel verify the existence of an actual fire condition before it sends an alarm report to the central station. The Fire Verify zone shall require the panel to perform a Sensor Reset whenever a device connected to a Fire Verify zone initiates an alarm. This shall begin a verification period during which the panel waits for a second alarm initiation. If the original zone or any other Fire Verify zone on the panel initiates an alarm within the next 120 seconds, the panel shall recognize this as an actual alarm and send an alarm report to the central station.

7.9 Cross-Zoning Protection

The system shall support cross-zoning as a means of requiring two device trips to occur within a short period of time before sounding an alarm and sending an alarm report to the central station. Supported device trips shall be from one device that trips two times, or from two devices that each trip once.

7.10 Swinger Zone Bypassing

The system shall be capable of automatically bypassing a zone if it goes into an alarm or trouble condition a specified number of times within a one-hour period. The panel shall be able to track the number of times the zone trips while armed and compare that against a programmed number. When that number is reached, the panel shall be able to automatically bypass the zone. The panel shall be capable of resetting the zone when the area to which it is assigned disarms, is manually reset from the keypad or remotely, or remains normal for one hour.

7.11 Recently Armed Report

The system shall be capable sending a System Recently Armed report, along with a zone alarm report, to the central station any time an alarm occurs within five minutes of the system arming. The System Recently Armed report allows the central station operator to follow a “call the subscriber first” procedure instead of immediately dispatching the police to what could be a false alarm.

7.12 Transmit Delay

The system shall be capable of programming the panel to wait up to 60 seconds before sending burglary alarm reports to the central station. If an alarm is accidental, the user shall be able to disarm the system within the programmed Transmit Delay time. An Abort report shall be sent in place of an alarm report after the system disarms. During the alarm, sirens and panel relay outputs shall not be delayed and shall still provide local condition annunciation.

7.13 Call Waiting Cancel

The system shall be capable of being programmed to cancel call waiting any time the panel dials the receiver number to send a report.

7.14 Cancel/Verify

The system shall be capable of sending either a Cancel Report or Verify Report to the Central Station to signify that the end user has Canceled an Alarm or Verified an Alarm condition. Also, the system shall be programmable to instead of Cancel/Verify show “IS THIS A FALSE ALARM? NO YES”. If YES send validation of alarm to Central Station, if NO send alarm cancel.

8.0 FIRE CONTROL SPECIFICATIONS

8.1 FACP Standards

The Fire Alarm Control Panel (FACP) system shall be listed as a Power Limited Device and be listed under the standards below. Each system shall be supplied with complete details on all installation criteria necessary to meet all of the listings.

Fire Listings	• FDNY – Fire Department New York City
• UL 985 Household Fire Warning	Related Standards
• UL 864 Commercial Fire Warning	• NFPA 70 National Electric Code (NEC)
• California State Fire Marshal	• NFPA 72 National Fire Code

8.2 Fire Annunciator Keypads

A. The control unit shall be completely programmable remotely using remote annunciators, and/ or using upload/ download software that communicates using SDLC 300 baud, 2400 baud, 9600 baud, IP Addressed data network, or cellular communications network. On-site programming from a personal computer shall also be permitted. Programming changes shall comply with NFPA 72 for acceptance or re-acceptance testing.

B. The system shall include a menu selected “SENSOR RESET” option. This option shall operate without disarming and re-arming the fire system, with use of any pass code or function key controlled by a key switch, shall reset smoke detectors after they have been tripped.

C. System shall be restricted from remote software connection unless on-site authorization is given by means of lock code entered at a 630F Fire Annunciator to comply with NFPA 72 requirements.

8.3 Zone Configuration

A. The FACP system shall have a minimum of two (2) Class B ungrounded 2-wire smoke detector zones available from the control panel.

B. The system shall be capable of providing a maximum of 562 independent, 2-wire, and 12 VDC powered zones to power smoke detectors.

C. Zones on the digital SLC buses (LX buses) shall be capable of supporting 500 DMP Model 2W-BLX and/or 2WT-BLX addressable smoke detectors.

8.4 Fire Annunciators

A. If at any time a remote annunciator does not detect polling from the intrusion detection/ access control or FACP, the remote annunciator shall indicate “SYSTEM TROUBLE” on its alphanumeric LCD display within 200 seconds. If at any time the remote annunciator detects polling, but not for its particular address, the alphanumeric display shall indicate “NON-POLLED ADDR”.

8.5 Fire Control Equipment

A. Fire Control detection equipment shall communicate to the system by way of the control panel loop expansion bus or 900MHz receiver. The detection equipment shall have a three (3) year warranty and meet or exceed features offered in the products listed in Section 11.0 of this document.

B. Wireless detection equipment shall be supervised at a maximum of once every 3 minutes to comply with NFPA 72 Standard and UL Listed for Commercial and Residential Fire Applications.

C. All detection equipment shall be listed by a Nationally Recognized Testing Laboratory (NRTL) for the intended purpose and meet NFPA 72 Standards.

9.0 BURGLARY CONTROL SPECIFICATIONS

9.1 Burglary Standards

The Burglary system shall be listed as a Power Limited Device and be listed under the standards below. Each system shall be supplied with complete details on all installation criteria necessary to meet all of the listings.

Burglary Listings	U.S. Government Standards
• UL 1023 Household Burglar Alarm System Units	• Meets ICD 705 Chapter 7 Intrusion Detection Systems (IDS)
• UL 1076 Proprietary Burglar	• Meets DoD/NIST SCIF Standards
• UL 1610 Central Station Burglar Alarm Units	
• UL 1635 Digital Burglar Alarm Communicator System Units	

9.2 Area System Mode

A. The system user shall be capable of selectively arming and disarming any one or more of 32 areas within the intrusion detection system based on the user PIN code and/or keypad used. Each of the 574 zones shall be able to be assigned to any of the 32 available areas. The system shall be capable of having up to a thirty-two (32) character length name programmed for each area.

B. The system user shall be capable of assigning an opening and closing schedule to all areas or to each of the 32 areas separately. Each area shall be able to arm or disarm automatically by a schedule. The system shall have the capacity for common areas that automatically disarm when any other area disarms and that automatically arm when all others areas arm.

C. The networked system shall have the ability to comply with Bank Safe & Vault application. The networked system shall also have the ability to use a two-man rule for disarming or allowing door access to an area. The system shall have the ability to operate a Common Area application.

D. The Encrypted system shall have the feature of Card Plus Pin by area High security card access is provided by the Card Plus Pin feature that requires both a card read and a PIN (4-6-digit user ID) entry for arming/disarming and access by area. This Card Plus Pin operation complies with the ICPG 705 requirement for dual id authentication and operates with a DMP Prox Keypad and a HID ProxPro reader with the keypad connected to a DMP Wiegand Interface module.

9.3 Home/Sleep/Away Mode

A. The system shall be capable of being configured in a Home/Sleep/Away configuration for Residential application consisting of a Main House system and up to two Guest House systems with in one single control Panel. Each House being controlled with its own keypad as if it were separate alarm systems.

9.4 All/Perimeter Mode

A. The system shall be capable of being configured into the All/Perimeter mode to enable the selective arming of both the interior and perimeter when armed “All” or arming just the perimeter devices if arming “Perimeter”.

9.5 Zones

The system shall have a minimum of eight (8) grounded burglary zones available from the control panel, and two floating ground powered zones for two wire type compatible smoke detectors. The system shall have the ability to expand using the panel’s keypad bus for up to sixty-four additional zones. The system shall also have five built in Zone expansion bus (LX Bus) for an additional 500 zones of expansion. The system shall have the ability to integrate up to 500 wireless zones for a total of 574 zones overall.

9.6 Burglary Equipment

Burglary detection equipment shall communicate to the system by way of the control panel loop expansion bus or 900MHz bi-directional spread spectrum receiver. The detection equipment shall have a three (3) year warranty and meet or exceed features offered in the products listed in Section 11.0 of this document.

9.7 Z-Wave Equipment

The system shall be capable of 140 Z-Wave devices by means of the use of the model 738Z+ module. The system shall have the capability of up to 20 Z-Wave favorites for grouping Z-Wave devices into a favorite response or control.

10.0 ACCESS CONTROL SPECIFICATIONS

10.1 Access Control Standards

The access control system shall be listed as a Power Limited Device and be listed under the standards below. Each system shall be supplied with complete details on all installation criteria necessary to meet all of the listings.

Access Control Listings	U.S. Government Standards
• UL 294 Access Control System Units	• Meets ICD/ICS 705 Chapter 7 Intrusion Detection Systems (IDS)
	• Meets DoD/NIST SCIF Standards

10.2 Keypad

A. The system shall display a message at any keypad when any system area remains disarmed past the scheduled closing time. The message shall be displayed at one minute past the scheduled closing time. A pre-warn tone shall also begin sounding. If the system is not armed or a schedule extended within ten minutes past the scheduled closing time, the system shall provide the option of sending a Late to Close report to the central station.

B. The keypad shall include a door strike relay capable of sending a report to the central station when activated.

C. The keypad shall be capable of proximity arming and disarming functions.

D. The keypad shall display red backlighting when in alarm condition notifying an individual of an unacknowledged alarm condition.

E. The keypad shall annunciate when canceling an alarm condition the words “Cancel” or “Verify” to allow the end user the ability to cancel a user generated alarm or to select verify to send a message to the central station that the alarm has been verified by the end user and to send emergency response personnel. This is to comply with Alarm Verification.

10.3 Area Access Control

A. The system shall be capable of integrating area access control capability where specified into the same control panel with the ability to have up to 10,000 user credentials. User access is limited to custom profiles and/or schedules. Anti-passback shall be available. The networked version shall support a Two-Man Rule feature. The system shall support up to thirty-two (32) access doors expandable to 96, connected to the system using a manufacturer-approved interface module.

B. Area door access products shall meet or exceed features offered by the following products:

1. Keypad reader/administration device – DMP Model 7063/7063A, 7073/7073A, 7163/7173, 7872, 7873, 1301I, 1301N, 1301P
2. Wiegand Interface – DMP Model 734, 734N, or 734N-WIFI
3. Reader – DMP Model PP-6005B, PR-5455, MP-5365, P-300-H-A, P-500-H-A, P-640-H-A, PR-5355-AGK144.
4. Cards or credentials – DMP Model 1326/10, 1306P/10, 1346, 1386/10, PSC-1-H/10, PSC-1-H/100, PSK-3-H/10, PSK-3-H/100, PSM-2P-H/10

10.4 Access Control Equipment

Access Control equipment shall communicate to the system by way of the control panel keypad bus. The equipment shall have a three (3) year warranty and meet or exceed features offered in the products listed in Section 11.5 of this document.

11.0 COMPILED DETECTION EQUIPMENT LISTING

11.1 Hard-wired

Hard-wired detection equipment shall communicate to the system by way of the control panel loop expansion bus. The equipment shall have a three (3) year warranty as stated in the current DMP Product Catalog and meet or exceed features offered in the following products:

Bus Splitter/Repeater Module – DMP Model 710

Door Contact – DMP Model SM-20WG (surface applications – requires DMP zone expander)

Output Expansion Module - DMP Model 716

Graphic Annunciator Module - DMP Model 717

Other product types shall connect directly to zone expansion modules such as:

Manual Fire Alarms – DMP Models 850S, 850D

Addressable - DMP Model 711

Addressable - DMP Models 714, 714-8, 714-16

Addressable - DMP Models 712-8

Addressable - DMP Models 715, 715-8, 715-16

Addressable - DMP Models 850S/711, 711S, 850D/711, 2W-BLX, 2WT-BLX

11.2 Wireless

Wireless detection equipment shall communicate to the system by way of a compatible 900MHz receiver utilizing two-way communications, capable of receiving up to 500 wireless zones. The wireless system shall be programmed directly from the control panel, and shall not require a separate device programmer. The wireless detection equipment shall have a one (1) year warranty. It shall be capable of sending transmitter and battery status to the control panel's compatible receiver up to once every 60 seconds and must meet or exceed the following products:

Wireless Receiver – DMP Model 1100X-W or 1100XH-W

Wireless Repeater – DMP Model 1100R-W

Universal transmitter – DMP Model 1101-W, 1102-W

Universal Transmitter – DMP Model 1103-W

Universal Transmitter – DMP Model 1106-W

Wireless Window Transmitter – DMP Model 1107-W

Wireless Zone Expander – DMP Model 1114-W

Wireless Temperature Sensor and Flood Detector – DMP Model 1115-W, 1115-W/470PB, 1115-W/T280R

Wireless Relay Output – DMP Model 1116-W

Wireless LED Annunciator – DMP Model 1117R-W

Wireless Remote Indicator Light – DMP Model 1118R-W

Wireless Door Sounder – DMP Model 1119-W

Motion Detector – DMP Model 1121-W, 1126R-W, 1127W-W, and 1127C-W

Glass Break Detector – DMP Model 1128

Recessed Contact – DMP Model 1131-W

Wireless Siren – DMP Model 1135-W

Wireless Remote Chime – DMP Model 1136

Wireless LED Emergency Light – DMP Model 1137-W

Bill Trap – DMP Model 1139

Panic Transmitter – DMP Model 1142, 1142BC

Wireless Wall Button – DMP Model 1141-W

Pendant Panic Transmitter – DMP Model 1144-1, 1144-1P, 1144-2, 1144-2P, 1144-4, 1144-D, 1148-G

Wireless Four-Zone Input Module – DMP Model 1154

Wireless 8-Zone Input Module – DMP Model 1158

Smoke Detector Transmitter – DMP Model 1164-W, 1164NS-W, 1168

Wireless Heat Detectors 1183-135F and 1183-135R

Wireless Carbon Monoxide Detector 1184-W

11.3 Power Supplies and Transformers

Power supply and transformer shall maintain system operation. The batteries shall be checked and replaced every three to five years. The equipment shall have a three (3) year warranty as stated in the current DMP Product Catalog and meet or exceed features offered in the following products:

Power Supply – DMP Model 505-12, 115 VAC, 12 VDC
Power Supply – DMP Model 505-12LX, 115 VAC, 12 VDC
Power Supply – DMP Model 505-12L-R or 505-12L-G 12 VDC
Transformer - DMP Model 327, 16.5 VAC 50 VA, Plug-in
Transformer - DMP Model 322, 16.5 VAC 56 VA, Wire-in
Transformer - DMP Model 323, 16.5 VAC 56 VA, Wire-in
Transformer – DMP Model 324, 16.5 VAC 100 VA, Wire-in
Transformer – DMP Model 324P, 16.5 VAC 100 VA, Wire-in

11.4 Access Control Equipment

Access control equipment shall provide access control functions between the panel and controller door access points. The equipment shall have a three (3) year warranty as stated in the current DMP Product Catalog and meet or exceed features offered in the following products:

Interface Module – DMP Model 734, 734N, or 1134
Egress Module – DMP Model PB-2 REX Button
Reader – DMP Model PP-6005B Proxpoint Plus©
Reader – DMP Model MP-5365 Miniprox©
Reader – DMP Model MX-5375 Maxi-Prox™
Reader – DMP Model TL-5395 Thinline II™
Reader – DMP Model P-500-H-A Prox Reader, Single-Gang
Reader – DMP Model P-640-H-A Prox Reader, Keypad, Single-Gang
Reader – DMP Model P-300-H-A Prox Reader, Mullion Mount
Door Credential – DMP Model 1306P Prox Patch™
Door Credential – DMP Model 1306PW Prox Patch™
Access Card – DMP Model 1351 ProxPass© Card
Access Card – DMP Model 1326 Proxcard II© Card
Access Device – DMP Model 1346 Proxkey II™ Keyfob
Access Card – DMP Model 1386 ISO Prox II©
Access Card – DMP Model PSC-1-H/10 (Clamshell Card / 10 Pack)
Access Card – DMP Model PSC-1-H/100 (Clamshell Card / 100 Pack)
Access Card – DMP Model PSC-3-H/10 (Prox Key Ring Tag / 10 Pack)
Access Card – DMP Model PSC-1-H/100 (Prox Key Ring Tag / 100 Pack)
Access Card – DMP Model PSM-2P-H/10 (Prox Card, PVC Printable-10 Pack)
Farpointe Data Prox Reader – DMP Models P-300-H-A, P-500-H-A
Farpointe Data Prox Reader and Keypad – DMP Model P-620-H-A, P-640-H-A
Farpointe Data Contactless Smartcard Reader - DMP Model D3
Farpointe Data Contactless Smartcard Reader and Keypad – DMP Model D6.4
Farpointe Data Presentation Mobile-Ready Contactless Smartcard Reader – DMP Model CSR-35P
Farpointe Data Smartcard – DMP Model DE2 MIFARE DESFire EV1
Farpointe Data Conekt Mobile Access Credential – DMP Model CMC-2 (10 or 100 Pack)
Farpointe Access Card – DMP Model PSC-1, PSM-2P
Farpointe Data Prox Key Ring Tag – DMP Model PSK-3

11.5 Cellular Communications Equipment

Cellular Communications equipment shall plug directly into the XR150/XR550 J24 connector and shall be supervised by the XR150/XR550 Control Communicator. The Cellular Communications Equipment shall be of a low current draw and powered directly by the XR150/XR550 Control Communicator.

The Cellular Communicator shall communicate in the SDLC Serial 3 Format for communications directly to a SCS-1R or SCS-VR DMP Central Station Receiver. The equipment shall have a three (3) year warranty as stated in the current DMP Product Catalog and meet or exceed features offered in the following products:

263H/381-2 HSPA+ Digital Cellular Communicator with 18" Coax Extension Cable

263C/381-2 CDMA Digital Cellular Communicator with 18" Coax Extension Cable

263LTE-A/263LTE-V/381-2 LTE Digital Cellular Communicator with 18" Coax

Extension Cable 380-400 Level 400 SIM Card (263H only)

381-2 18" Coax Cable

381-12 12' Coax Extension

381-25 25' Coax Extension

383 Rubber Duck Antenna

386 Wall Mount Antenna Bracket

387-1 3DB Fiberglass Antenna w/Bracket

387-3 3DB MEG Antenna

387-4 SMA to N Cable, 4ft LMR195

387-8 SMA to N Cable, 8ft, LMR195

387-25 SMA to N Cable, 25ft LMR195

387-50 SMA to N Cable, 50ft LMR195

11.6 Z-Wave Wireless Devices

The system shall be capable of 140 Z-Wave devices by means of the use of the model 738Z+ module. The following are compatible Z-Wave devices.

738Z+ Z-Wave Plus Interface Module

Z-5010T Z-Wave Thermostat

Z-45742 Z-Wave Light Control Module with Dimmer

Z-PS15EMZ5-1 Z-Wave Light Control and Appliance Module

Z-14319 Z-Wave Switch, Toggle On/Off

Z-45741 Z-Wave Toggle Style Auxiliary Switch

Z-PD300EMZ5-1 Z-Wave Light & Appliance Module with Dimmer

Z-39723 Z-Wave LED Light Bulb

Z-99100-077 Z-Wave Door Deadbolt, Polished Brass

Z-99100-078 Z-Wave Door Deadbolt, Satin Nickel

Z-99100-079 Z-Wave Door Deadbolt, Venetian Bronze

Z-GD00Z Z-Wave Garage Door Controller

736-Q myQ Garage Door Interface Module

12.0 INSTALLATION

12.1 System Component Installation

Materials shall be installed in strict compliance with all local, state, county, province, district, federal and other applicable building, safety, and fire standards, laws, codes, regulations, and guidelines including, but not limited to, all appendices and amendments and the requirements of the local authority having jurisdiction (AHJ).

12.2 Lightning Suppression

The system shall include an optional lightning suppressor module that intercepts and directs lightning, transient, and RF interference to ground.

13.0 SYSTEM COMPARISON

13.1 Basic Comparison Items Table

The table below lists features or points found necessary for successful installation and continued service of an integrated system. Compare your current system with the listed items. Please provide a certification document providing a clear and truthful statement that agrees with your response to each question.

Important Points	Explanation	Response	
Designed, Engineered, Manufactured Location	Is your system engineered, designed, manufactured, assembled, and distributed from a location within the United States of America using U.S. and global components?	**Yes**	No
Forward and Backward compatibility	Because we want to preserve a maximum portion of our investment over time, can your system manufacturer certify that it has practiced forward and backward compatibility of main system components such as the panel, keypads, zone expansion devices, and relay output devices for a minimum of the last thirty (30) years?	**Yes**	No
Manufacturer Experience	Because we require extensive manufacturing experience, has your system controller manufacturer's primary role been in the security industry for a minimum of thirty-five (35) years?	**Yes**	No
System Messaging Compatibility	We require the maximum capabilities in communication offered by the manufacturer. Does your system controller manufacturer also engineer, and manufacture a receiver that receives all messages in less than six seconds? If so, can this receiver receive each and every status message that the controller sends?	**Yes**	No
Experience in Network Monitoring	Has your manufacturer been providing TCP/IP network monitoring for a minimum of thirty (30) years?	**Yes**	No
No Invasive systems on our network	Because our network is so important to the operation of our business, We require that no additional PCs or terminals be allowed upon our network. Does your manufacturer require additional software or PC terminals in order to program or maintain operation of network monitoring functions?	Yes	**No**
Network monitoring flexibility and compliance	Because we require confirmation of the fitness of your monitoring capabilities, the system must be listed by approved compliance agencies. Can your manufacturer's controller provide UL Standard Line Security network monitoring over a network that uses either DHCP, or static IP address?	**Yes**	No
Easy operation	Because we manage so many people, the system must be easy to operate. Does your system manufacturer offer keypads with integrated proximity identification capabilities?	**Yes**	No
Seamless Integration with Access Control	Because we are aware of false alarm activations that may occur when using a security system and access control system, we require that these two systems be designed into one control panel. Does your system offer intrusion detection and door access control functions that allow the user to disarm selected areas, and open an access door with a single presentation of a proximity identification device?	**Yes**	No
Distribution of relay outputs	Because we intend to integrate this system with many of our other electronic systems within the building, we require that the placement of triggering relays be as flexible as possible. Does your system have the ability to provide relay outputs in a central location, and distributed across a data bus which extends at least 15,000 feet?	**Yes**	No
Relay triggering capabilities	Because we intend to integrate this system with many of our other electronic systems within the building, we require that the triggering of relays be as flexible as possible. Can your system trigger relay outputs based upon zone status or system status, and can relays be triggered by way of keypad commands, software commands, Web browser commands, RF remote, and a pre-determined schedule?	**Yes**	No

INTRUSION/ACCESS/FIRE/INTEGRATED SYSTEM PERFORMANCE SPECIFICATION FOR DMP MODEL XR150/XR550 SERIES

Important Points	Explanation	Response	
Relay states when triggered	Because we intend to integrate this system with many of our other electronic systems within the building, we require that the triggering of relays be as flexible as possible. Can your system's relay outputs be selected for status to follow zone input status, pulsed output, and maintained outputs.	**Yes**	No
Relay states according to the state of the zone input	Because we intend to integrate this system with many of our other electronic systems within the building, we require the triggering of relays be as flexible as possible. Can your system's relay outputs be configured for different responses based upon the zone armed state?	**Yes**	No
Relay associations to zones based upon system and zone states.	Because we intend to integrate this system with many of our other electronic systems within the building, we require that the triggering of relays be as flexible as possible. Can you assign different relays for each zone based upon whether the system is armed and the zone is open, the system is disarmed and the zone is open, the system is armed and the zone is shorted, and the system is disarmed and the zone is shorted?	**Yes**	No
Common descriptions for zone, area, and user designations.	Because we wish to minimize confusion in various ways that we use reporting, we require that descriptions for areas of our building, users of the system, and zone inputs connected to the system offer at least sixteen (16) characters to maximize user understanding. These descriptions must be programmed and stored in one location, and appear exactly the same in stored events, printed logs, and remotely at the central monitoring station. Does your system provide this capability?	**Yes**	No
Flexible user interface capabilities	Because we may use the system from many locations, in many ways, we require that the system offer user interface capabilities from local keypads, web browsers, software packages, radio frequency remote arming stations, and offer the capability to use any zone input for arming and disarming. Does your system offer all of these capabilities?	**Yes**	No
Economical system additions for access control	Because we are looking for a cost-competitive system design, the system shall be capable of adding up to ninety-six (96) door access locations without requiring additional control panels. To minimize cabling costs, the system wiring must support a single four-wire cable, and must use remote intelligent devices to collect door status, user identification devices, and triggers to unlock distant doors. Does your system offer this capability?	**Yes**	No
Contractor experience	Because we require that the installing company is experienced and factory trained. We require each installer and service person who works on our system to be factory trained and must submit a certificate issued by the factory as proof of this training. Can your company provide these certification documents?	**Yes**	No

866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877