PARADOX™
IMPERIAL

Paradox Imperial Integrated System

With MAMA Building Automation

Architectural and Engineering Specifications

PARADOX®
SECURITY SYSTEMS

Table of Contents

1.0 SCOPE OF THIS DOCUMENT

The following document is formatted for the use in a tender specification for a 384-zone, 32 partition expandable security, access control, and building automation system using Paradox Security Systems products. This document does not detail any specifications required for the installation of equipment or programming of devices.

This document covers V32 Main Controller version 1.10 and may be revised according to new developments or changes in the released product. For the latest A&E Specifications, see www.paradox.com. Paradox Security Systems reserves the right to change this document without notification.

2.0 SYSTEM DESCRIPTION

The Imperial 384-zone Paradox Imperial Integrated System, hereafter referred to as “the system”, shall meet or exceed the requirements detailed within this section.

2.1 General System Overview

[2.1.1] The system shall be a modular-based system equipped with alarm monitoring, built-in access control capability, and building automation.

[2.1.2] The system shall be expandable to 511 modules that can be connected in a star or daisy chain configuration at any point and in any combination on the digital four-wire bus up to 1000m (3,000ft) from the main controller using 18AWG or up to 305m (1000ft) using 22AWG. This expandable, secured and encrypted communication bus provides reliable communication for building automation and security.

[2.1.3] The system shall include an independent RS485 communication bus for access control expansion.

[2.1.4] Communication between the system’s security and building automation modules shall be carried out via 13.8 Vdc 4-wire bus at 500bps. The bus shall provide two-way data exchange by using a specialized proprietary communication protocol to constantly convey information between the modules and the Main Controller.

[2.1.5] All programming shall be done using the system's proprietary PC software. No keypad programming shall be necessary.

2.2 Hardware

[2.2.1] All system modules shall be in standard 33 x 7.5 mm (1.38 x 0.3 in.) DIN rail (top-hat) format.

[2.2.2] An adequate lockable metal DIN box shall be available for installation of DIN modules. As well, individual DIN rails shall also be provided for localized installation of modules.

[2.2.3] The system shall be in-field firmware upgradeable. This shall allow the system’s firmware to be upgraded using firmware upgrade software. Firmware files shall be available on Paradox’s website for download. For module firmware upgrades, the bus shall automatically switch to RS-485 at 57.6 Kbps. The system shall be capable of performing firmware upgrades locally as well as remotely via TCP/IP.

[2.2.4] For landline reporting, a main telephone line shall be connected directly to the main controller or though a CA38A or RJ31. The main telephone line shall be supervised. The main controller shall include a digital CTR-21 approved dialer.

[2.2.5] The main controller shall include a 1.7A switching power supply, and have an electrical rating of 16-24 VAC; 50 or 60Hz or 18-24 VDC; 75VA; 50W. The system’s transformer sharing feature enables modules to share a central AC or DC supply throughout the system.

[2.2.6] The battery charging current shall be programmable at 300mA or 850mA.

[2.2.7] In the event of complete battery and AC power loss in the system, all main controller and module programming shall be retained in the system’s non-volatile memory as well as in the system programming software.

[2.2.8] LCD Keypad modules shall display the date and time, partition and zone status, the alarm memory and any troubles in the system unless Confidential Mode or the Shabbat feature are enabled.

[2.2.9] The main controller shall employ a trouble latch feature, ensuring that system troubles are displayed until manually cleared by the user.

[2.2.10] The main controller shall incorporate a built-in RTC (Real-Time Clock) that will save the main controller's internal clock for up to 10 days when both AC and battery power are lost.

2.3 Programming Methods

[2.3.1] Installer/end user uploading/downloading software shall be available for main controller and module programming, on-line monitoring, searching and displaying events, and printing reports. The software shall provide on-site connection or remote connection through an IP network. The software shall provide programming, control, and monitoring of the site and include features such as complete backup utilities, troubleshooting and support tools.

[2.3.2] The software shall be available in several languages, such as English, Spanish, and French, and a translation tool shall be provided which can be used to translate the software interface as required.

[2.3.3] The software shall be available to enable users to set user codes and options, to monitor live system status and to search and print events without compromising security operation and central station communication. Up to 8 PC computers shall be able to connect to the TCP/IP port of the main controller simultaneously.

2.4 Keypads

[2.4.1] The Grafica Color LCD Keypad modules shall display up to 384 zones on up to 32 partition, and include one keypad zone/temperature input. The keypad module shall use simple text- and icon-driven menus as well as incorporate alarm clock and special reminder features. The keypad module shall provide 15 tunes for use with entry delay, exit delay, burglar alarm, fire alarm and special events. The keypad module shall incorporate a 6.6 x 6.6cm (2.6 x 2.6 in.) color graphic LCD with a resolution of 320 x 240 pixels and with adjustable backlight, contrast and volume. The keypad module shall support up to eight built-in, user selectable languages.

[2.4.2] The 32-character LCD Keypad modules shall include one keypad zone, AC, locate, bus fault, status and trouble indicators. The LCD Keypad module shall be able to display the status of 384 zones on up to 4 partitions. The on-board tamper switch shall not occupy a zone and tamper supervision shall be done through the bus. The keypad's Super Twisted Nematic LCD shall have a wide viewing angle, two lines of 16 characters, adjustable scrolling speed, backlight, dimming delay, dimming value and contrast. The keypads shall provide three keypad-activated panic alarm keys, seven installer function keys, individually programmable chime zones, chime on zone closure, a confidential mode with a timer, keypad muting, and audible trouble indicators. The keypad shall be able to display the 16-character labels assigned to zones, users and partitions.

2.5 Monitoring and Access Modules

[2.5.1] The system shall support addressable indoor or outdoor digital motion detectors with or without pet immunity. An addressable ceiling mounted motion detector shall be available. Detectors shall provide sabotage-proof protection and individual tamper supervision by connecting directly to the bus without using resistors or additional wiring. Signals received by the motion detectors shall be completely converted, amplified and processed in the digital domain without using analogue circuitry. The motion detectors shall be fully software driven and employ innovative digital processing technologies to effectively eliminate false alarms. The modules' sensitivity shall be adjustable.

[2.5.2] The system shall support 8-, 16- and 32-zone hardwire expansion modules. The 32-zone expansion module shall also include a 2.85A switching power supply.

[2.5.3] The access control modules connected to the bus shall support 26-bit Wiegand readers (using a RS-485 Converter), 4-wire readers, electric door locks, door contacts and Request-for-Exit devices. The access control modules shall support transformer sharing. The module shall support automatic unlocking schedules, safe mode options and unlock door options with buttons, system events or during a fire alarm. The access control module shall be in-field firmware upgradeable.

[2.5.4] Two types of 4-wire card readers shall be available for easy connection to an access control module. One reader shall be available with an integrated 12-key keypad. Both readers shall be weather resistant and shall be usable for indoor and outdoor installation.

2.6 Communication Accessories

[2.6.1] The system shall allow the user to control and monitor the system through an IP network. The system shall be able to communicate with the software through the internet. It shall support a DNS service for dynamic IP addresses. Data transmitted by the module shall be encrypted by using 128-bit (MD5 and RC4) or 256-bit (AES) data encryption. The module shall support two-way dynamic authentication.

2.7 System Accessories

[2.7.1] A 2.85A switching power supply shall be available which supplies four auxiliary outputs at 500 mA each. Outputs can be wired in parallel to increase output current. The power supply shall include an LCD screen to display voltage and amperage of each output as well as the sum of all outputs. Standard power supplies shall also be compatible with the system.

[2.7.2] A wireless system shall include a transceiver for two way communication, a di-pole antenna, error correction algorithm, a choice of either 433MHz or 868MHz frequencies, up to 32 PIRs and/or door contacts with range (line of sight) of 70m (230ft), up to 4000 remote controls with range (line of sight) of 60m (200ft), Reflow design, one on-board tamper switch, full system supervision (check-in, low battery and tamper) and a transmitter signal strength indicator. The module shall be in-field firmware upgradeable.

[2.7.3] Optional hub and bus isolator modules shall divide the bus into four completely isolated output ports. Each output port shall provide communication over a distance of up to 900m (3000ft) and include opto-isolated protection from high-voltage spikes.

3.0 SECURITY

This section covers the features associated with the burglar alarm portion of the system.

[3.0.1] The system shall provide eight on-board hardwired inputs that shall be expandable to 384 addressable inputs (zones) that can be assigned to one of 32 independent partitions.

[3.0.2] The system shall support up to 4000 users codes (250 security and access control / 3750 access control only). One user code shall be designated for the system owner code.

[3.0.3] User codes shall be fixed at four or six digits in length.

[3.0.4] The system shall include a memory buffer for up to 2000 security events.

3.1 Zones

[3.1.1] The system shall include the following zone definitions: two Entry Delays with timers set by partition, two Stay Delays with timers set by partition, Follow, Instant, 24hr. Buzzer, 24hr. Burglary, 24hr. Hold-up, 24hr. Gas, 24hr. Heat, 24hr. Water, 24hr. Freeze, Delayed 24hr Fire and Standard 24hr Fire, and Virtual Zone. Each zone, except for the Virtual Zone, shall be assigned to one of the partitions.

[3.1.2] Zones shall include the following options: Auto Zone Shutdown, Bypass, Stay, Force, Steady Alarm, Pulsed Alarm, Silent Alarm, Report Only, and Delay before Alarm Transmission.

[3.1.3] Zones shall be continually supervised. The system shall optionally restrict arming on wireless module supervision loss, tamper, AC failure, battery trouble or failure, bell or auxiliary failure, TLM failure and module troubles. The system shall be monitored for system, communicator, module, bus, zone tamper, zone low battery, zone fault and clock loss troubles.

[3.1.4] Only inputs that shall be used in the system need be assigned to zones. Inputs shall be assigned to zones as required to enable flexible configurations without relocating devices.

[3.1.5] The input speed on the panel shall be set between 30 and 3000 milliseconds. The input speed on the zone expansion module shall be set between 15 milliseconds and 255 minutes.

[3.1.6] The system shall support four-wire smoke detectors. Smoke detectors shall be reset on any keypad in the system by simultaneously pressing two keys for two seconds.

3.2 Reporting Features

[3.2.1] The system shall have the capability to report system events to a central monitoring station via landline using the system's built-in dialer and/or via IP using the system's built-in TCP/IP port. If both reporting methods are enabled, the system shall have the capability to report both methods sequentially.

[3.2.2] The system shall support SIA, Ademco Contact ID 2000 edition, Contact ID Pager, Pager and most standard report code formats.

[3.2.3] Each partition shall have a 4-digit account number. Main controller events shall be divided into three event groups for each partition and two global event groups. Each event group shall be programmed to dial up to 16 different monitoring station telephone numbers with two that can be used as backups. The main controller shall dial the backup telephone number after every failed attempt to contact the monitoring station or only after the maximum dialing attempts to one monitoring telephone number has failed.

[3.2.4] Several reporting features shall also be provided by the system, such as recent close delay, pager delay, power failure delay, disarm reporting options, zone restore report options and auto report code programming.

[3.2.5] The Auto Test Report feature shall transmit a report code at a specified time over a cycle of several days, at the same minute every hour, or at regular intervals while the partition is armed or disarmed.

[3.2.6] The system shall provide the capability to identify when a partition should be armed and disarmed and enable the main controller to communicate deviations from the normal schedule to the monitoring station.

3.3 Arming and Disarming features

[3.3.1] The system shall be able to provide no-movement and timed automatic force or stay arming/ disarming, one-touch commands, keypad lockout, bell or keypad ring-back options set by partition, maximum bypass entries set by partition, and bell squawk options set by partition for disarming, arming, auto-arming, exit delay, entry delay, and remote arming/disarming.

[3.3.2] A partition shall be able to follow the arming and disarming status of one or more partitions.

[3.3.3] The system shall include 32 exit delay timers programmable from one to 255 seconds with the following features set by partition: exit delay termination, no exit delay on remote arm and switch to stay arming. A special exit delay shall be available for auto-arming, and software arming.

[3.3.4] The system shall employ a closing delinquency feature that will verify the last time the system was armed. If the last time the system was armed is greater than the delinquency timer, a Closing Delinquency event will be transmitted to the central monitoring station.

[3.3.5] An armed follow zone shall be able to switch to an entry delay if the follow zone opens without an entry being triggered.

3.4 Alarm Features

[3.4.1] The main controller shall be able to toggle the on-board bell/alarm output for each partition. The bell cut-off timers shall be set by partition between one and 255 minutes with each providing no bell cut-off on fire alarm, re-verification of zone status during an alarm, and a recycle delay.

[3.4.2] The system shall possess five wireless transmitter supervision options, two supervision bypass options, five tamper recognition options, two tamper bypass options, three keypad panic alarms per partition programmable as audible, silent or fire alarms.

[3.4.3] False alarm prevention shall be achieved by the following features: audible exit delays, bell squawk options for disarming, arming, auto-arming, exit delay, entry delay and remote arming/disarming, rapid keypad beeping during the last 10 seconds of the exit delays, automatic zone shutdown, alarm transmission delay, confirmation of the alarm situation before generating an alarm, recent close delay, exit delay termination, delayed 24hr. fire zones, stay delays, programmable input speeds, switch to stay arming, follow zone switches to entry delay, maximum bypass entries, arming and disarming report schedules, arming/disarming schedule tolerance windows, power failure report delay, automatic trouble shutdown, force on stay arm, and stay arming with delay.

3.5 User Codes

[3.5.1] User codes shall be programmable with the following options: regular, master, full master, duress, bypass, arm only, stay & instant arming, force arming and regular arming.

[3.5.2] Users shall be able to access all the partitions assigned to their user codes.

[3.5.3] Users shall be assigned to one or more partitions and can only arm, disarm and view the status of the partitions assigned to their user codes.

[3.5.4] The main controller shall include an option to allow the user code to unlock an access control door only during the assigned schedule or at any time.

4.0 ACCESS CONTROL

This section covers the features associated with the access control portion of the system.

4.1 Access Control Doors

[4.1.1] The system shall support 64 access control doors with programmable labels connected anywhere on the access bus. Each access control door shall use an access control module to support any 26-bit Wiegand reader (using a RS-485 Converter) or 4-wire reader, an electric door lock, a door contact, and a Request-for-Exit device. The 4-wire readers shall be connected up to 300m (1000ft) from the access module.

[4.1.2] The access control module shall support 24V locks when using external power.

[4.1.3] The system shall use 64 programmable access levels to determine which access control doors the users can access. Access levels containing from one to 64 access control doors shall be assigned to users through their user codes.

[4.1.4] Door access shall be granted by presenting a valid card to the door’s reader and/or entering a valid user code on the door’s keypad or PIN and Proximity Reader. For higher security areas the access control door shall be programmed to require both a valid card and valid user code for access to be granted.

[4.1.5] Doors shall be assignable to one or more partitions in the security system. Arming and disarming shall be capable of being programmed as accessible for users assigned to at least one of the door’s partitions or only if the user is assigned to all partitions assigned to the door.

[4.1.6] Arming using a card shall be possible by presenting a valid card twice to a reader within five seconds.

[4.1.7] The system shall support an automatic unlocking schedule per door consisting of four programmable time periods that determine the hours, days, and holidays that the door will remain unlocked. During the schedule, users shall not have to present their cards to the reader in order to gain access. The door shall be capable of being set to remain locked until the first valid card is presented and remain unlocked until the end of the schedule.

[4.1.8] Each door shall provide timers from one to 255 seconds to control the unlock period and extension, the door left open interval and audible feedback, the pre-alarm, and the door forced open audible feedback.

[4.1.9] The access control door shall be assignable to a zone through its access control module. If the access control door is forced open or left open, the main controller shall generate a burglar alarm and report to the monitoring station. The Door Forced Restore and Door Left Open Restore events shall be programmed to be recorded in the event buffer.

[4.1.10] The main controller shall be capable of preventing a card from arming or disarming the partition(s) assigned to the door even if the card is programmed to permit access to the door.

[4.1.11] For high security installations, the system shall be capable of door trap applications, where the system prevents one door from opening before another is closed.

4.2 Schedules

[4.2.1] The system shall support up to 256 access schedules. Each schedule shall include a start and end time, the days, and the holidays when the schedule will be valid. Access schedules can be set per door and are part of the access level.

[4.2.2] The system shall support a 365-holiday schedule.

4.3 Cards

[4.3.1] The system shall support 4000 cards programmable with multiple partition assignment, one of 64 access levels, one of 256 schedules.

[4.3.2] The access control door shall allow cards to disarm and/or regular, stay or force arm assigned partitions and omit the exit delay when arming. The system shall have an option to allow a valid card to unlock the door with or without disarming assigned partitions.

5.0 BUILDING AUTOMATION

This section covers the features associated with the building automation portion of the system.

5.1 Automation Capabilities

[5.1.1] The system shall include high-voltage, low-voltage and dimmable outputs with a maximum of 512 outputs.

[5.1.2] Relay outputs shall be programmed using the system software. Following the initial installation, authorized end users shall have the ability to modify building automation programming using the system software.

[5.1.3] Using the system software, automation outputs shall have the option of being grouped to create macros. Macros can be activated manually or by a system event, schedule, sunset/sunrise, or sensor. Authorized end users shall have the ability to modify and create macros for custom automation.

[5.1.4] By default, macros programmed in the system shall be defined as sprinkler, lights, shutter, or custom macros. Each output can be assigned to up to 16 macros.

5.2 Automation Control Hardware

[5.2.1] High-voltage addressable relay output modules shall be available which shall be capable of driving incandescent lights of up to 10A per channel @ 110 VAC / 230 VAC (on/ off operation), or 0.5hp shutter motors of up to 8 A per channel @ 110 VAC / 230 VAC (variable positions).

[5.2.2] Low-voltage addressable relay output modules shall be available which shall be capable of driving up to 500mA each @ 0 to 24V AC/DC. Each set of 4 relays shall have a jumper-selectable power source. Power can be supplied by either 12 VDC bus power or an external 0-24V AC/DC power source.

[5.2.3] Dimmable addressable relay output modules shall be available which shall be capable of driving 0-10V fluorescent lights as well as high-voltage devices, including incandescent lights, low-voltage halogen lights, and ceiling fans. The load can be either 110 VAC or 230 VAC, 50 or 60 Hz with a maximum output rating of 4.5 A (500 W @ 120 VAC / 1000 W @ 230 VAC). When used with Imperial dimmer wall switches, the system provides up to 32 dimming steps.

[5.2.4] The system's building automation outputs shall be controlled using Imperial wall switches. Switches shall be available in 4-button, 8-button, 2-dial (dimmer) and 4-button/1-dimmer formats. Buttons can be set in toggle mode (1 button on/off) or switch mode (1 button on / 1 button off). Each button/dial shall include an LED display to communicate output state. Each button shall include a backlit label for button programming identification.

[5.2.5] In the case where communication is lost between system modules, switches, and/or system software, all output modules shall include a physical button for emergency operation of each output.