



SECTION 28 10 00
ACCESS CONTROL

Copyright 2019 - Honeywell, Inc. - All rights reserved

PART 1 GENERAL

1.1 SECTION INCLUDES

- A. Web based access control system. (MPA2 Access Control System)

1.2 RELATED SECTIONS

- A. Section 26 05 00 - Common Work Results for Electrical.
- B. Section 27 11 23 - Communications Cable Management and Ladder Rack.

1.3 REFERENCES

- A. Electronic Industries Alliance (EIA):
 - 1. RS232C - Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange.
 - 2. RS485 - Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems.
- B. Federal Communications Commission (FCC):
 - 1. FCC Part 15 - Radio Frequency Device.
 - 2. FCC Part 68 - Connection of Terminal Equipment to the Telephone Network.
- C. Federal Information Processing Standards (FIPS):
 - 1. Advanced Encryption Standard (AES) (FIPS 197).
 - 2. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors.
- D. National Fire Protection Association (NFPA):
 - 1. NFPA70 - National Electrical Code.
- E. Homeland Security Presidential Directive 12 (HSPD-12).
- F. Underwriters Laboratories (UL):
 - 1. UL294 - Access Control System Units.
 - 2. UL1076 - Proprietary Burglar Alarm Units and Systems.

1.4 SUBMITTALS

- A. Submit under provisions of Section 01 30 00 - Administrative Requirements.
- B. Product Data: Manufacturer's data sheets on each product to be used, including:
 - 1. Preparation instructions and recommendations.
 - 2. Storage and handling requirements and recommendations.
 - 3. Installation methods.
- C. Verification Samples: For each finish product specified, two samples, minimum size 6 inches (150 mm) square representing actual product, color, and patterns.

- D. Manufacturer's Product Data: Submit manufacturer's data sheets indicating systems and components proposed for use.
- E. Shop Drawings: Submit complete shop drawings indicating system components, wiring diagrams and load calculations.
- F. Record Drawings: During construction maintain record drawings indicating location of equipment and wiring. Submit an electronic version of record drawings for the Security Management System not later than Substantial Completion of the project.
- G. Operation and Maintenance Data: Submit manufacturer's operation and maintenance data, customized to the Security Management System installed. Include system and operator manuals.
- H. Maintenance Service Agreement: Submit a sample copy of the manufacturer's maintenance service agreement, including cost and services for a two year period for Owner's review.

1.5 QUALITY ASSURANCE

- A. Manufacturer: Minimum ten years of experience in manufacturing and maintaining Security Management Systems. Manufacturer shall be Microsoft Silver Certified.
- B. Installer must be certified by Honeywell Integrated Security Dealer Service Certification Program (DSCP).

1.6 DELIVERY, STORAGE, AND HANDLING

- A. Store products in manufacturer's unopened packaging until ready for installation.

1.7 PROJECT CONDITIONS

- A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's recommended limits.

1.8 WARRANTY

- A. Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

PART 2 PRODUCTS

2.1 MANUFACTURERS

- A. Acceptable Manufacturer: Honeywell Security and Fire, which is located at: 2700 Blankenbaker Pkwy. Suite 150; Louisville, KY 40299; Toll Free Tel: 800-323-4576; www.security.honeywell.com
- B. Substitutions: Not permitted.
- C. Requests for substitutions will be considered in accordance with provisions of Section 01 60 00 - Product Requirements.

2.2 WEB BASED ACCESS CONTROL SYSTEM

- A. The Access Control System shall function as a Web-based open-architecture facility management system that tracks individuals, defines and controls access levels, monitors alarms, and generates reports. The system shall include the capability to configure alarms

and incorporate scheduled events that may be activated by either time or a specific programmed event. Access shall be controlled through a password-protected user interface. Operators can communicate with the system either through a host software system or by connecting to the Web server through an Ethernet connection.

- B. The MPA2 Door Access System shall include, as a minimum, the following performance:
1. The MPA2 Door Access System shall be protected by the most extensive support services in the industry, including Customer Service, Pre-Sales Applications Assistance, After-Sales Technical Assistance, access to Technical Online Support, and Online Training using web conferencing.
 2. The MPA2 Door Access System and its components shall be thoroughly tested before shipping from the manufacturer's facility.
 3. The door access system shall support easy remote management anywhere with an Internet connection.
 4. The door access system shall allow you to purchase the exact amount of access control doors immediately required, and to easily add more access controlled doors in the future.
 5. The MPA2 Access Control system shall support the bidirectional encrypted 128 AES OSDP:V2 AND/OR the standard Wiegand protocol to/from Access Control readers.
 6. The door access system shall be capable of being web based and controlled using a web browser, and seamless integration with Honeywell's MAXPRO Cloud and/or WIN-PAK XE, WIN-PAK SE, Win-PAK PE, and WIN-PAK CS access control software.
 7. The door access system web user interface shall support Google Chrome™.
 8. The door access system shall support SSL and SHA-1 secure socket layer encryption.
 9. The door access system shall allow each TCP/IP network connected door controller to support connection of up to 31 downstream door controllers by way of a standard RS485 data bus, for control of up to 62 (124)(*) downstream doors in a single web interface.
 10. The door access system shall support up to 100,000 user cards and up to 128 unique card formats up to 128 bits, and eight site codes.
 11. The door access system shall support up to 128 time zones, 65536 access levels, and 255 holidays.
 12. The door access system shall maintain up to 100,000 status event logging.
 13. The door access system shall provide a number of door control modes including Card only, card and PIN, PIN only, lockdown, disabled, supervisor, escort, limited use card, expire on date, first card rule, snow day rule, time zone toggle, local and global anti-pass-back, duress and others.
 14. The door access system shall support interlocks for custom actions.
 15. The door access system shall include integrated basic reports, import/export of the card database, and Alarms and event exporting to offline storage in a CSV database.
 16. The door access system shall be designed to be user friendly and shall be easily to train the system user.
 17. The door access system shall feature dynamic screen updating over a web connection, continually collecting and displaying door and system status for immediate display.
 18. The door access system browser shall feature full control of the system to monitor and view live events and to manually control doors and readers.
 19. Door access system status shall include the door state, alarms, events, inputs, outputs, power and other operational status.
 20. The door access system shall feature a Supervisor First capability that allows a supervisor to present his ID card once to the reader and to give individual access. If a supervisor presents a card twice, this shall enable access for their team, allowing members of the team to gain access during a specified time zone.
 21. The door access system shall feature an Escort mode for a Non-supervisor cardholder. The system allows the supervisor to first present his card, and then an

escorted person to present his card to maintain accompanied access while in the escort mode.

22. The door access system shall offer options to be powered by PoE (PLUS) (Power over Ethernet), or to be powered by way of an external power supply.
 23. The door access system enclosure shall offer connection to one, two, three(*) or four(*) doors by simply modifying configuration and optional licenses to accommodate the door control requirement.
 24. The door access system processors shall feature a System MTBF (Mean Time between Failure) of 250,000 hours.
 25. The door access system shall provide a multi-lingual user interface, including English, Italian, French, Dutch, Spanish, German, Czech, Simplified Chinese and Arabic.
- C. The MPA1002PPS(*) Door access Controller shall have the following mechanical specifications:
1. Unit Dimensions: 9.45 inches H x 11.40 inches W x 1.75 inches D (240 mm H x 290 mm W x 45 mm D).
 2. 2 X Ethernet Connector: RJ45 (1X PoE PLUS).
 3. 2 X USB Connector (Virtual LAN; FW Update).
 4. 3 X RJ45 Connector (RS485 Interface Bus; Downstream Bus IN/OUT).
 5. 8 X RJ45 Connector (Door/reader connections – Click ‘n Done)
 6. Enclosure Type: High Impact Plastic.
 7. Wiring Access Holes: 13 (Clean wall-mounting without removing cable knockouts possible).
- D. The MPA1002MPS Door Access Controller shall have the following mechanical specifications:
1. Unit Dimensions: 16.2 inches H x 13.7 inches W x 4.3 inches D (412 mm H x 350 mm W x 110 mm D).
 2. 93VAC to 264 VAC IEC socket (**) mains inlet.
 3. 2 X Ethernet Connector: RJ45 (1X PoE PLUS).
 4. 2 X USB Connector (Virtual LAN; FW Update).
 5. 3 X RJ45 Connector (RS485 Interface Bus; Downstream Bus IN/OUT).
 6. 8 X RJ45 Connector (Door/reader connections – Click ‘n Done)
 7. Enclosure Type: Metal.
 8. Wiring Access Holes: 24.
- E. The MPA1002PPS(*) access door controller shall have the following electrical specifications:
1. Voltage: 450mA @ 12 VDC.
 2. Power over Ethernet (PLUS) 802.3at.
 3. Power Consumption: < 6 Watts.
- F. The MPA1002MPS access door controller shall have the following electrical specifications:
1. Voltage: 93VAC to 264 VAC, 50/60 Hz, 13.8VDC @ 4A.
 2. Power Consumption: < 50 Watts.
- G. The MPA2 Door Access System shall be designed to meet the following environmental conditions:
1. Operating Temperature: 32 to 120°F (0 to 49°C).
 2. Storage Temperature: -67 to 185°F (-55 to 85°C).
 3. Emissions: FCC: Part 15, Class B.
 4. CE: EN55013.

PART 3 EXECUTION

3.1 EXAMINATION

- A. Examine site conditions to determine site conditions are acceptable without qualifications.

Notify Owner in writing if deficiencies are found. Starting work is evidence that site conditions are acceptable.

3.2 PREPARATION

- A. Clean surfaces thoroughly prior to installation.
- B. Prepare surfaces using the methods recommended by the manufacturer for achieving the best result for the substrate under the project conditions.

3.3 INSTALLATION

- A. System, including but not limited to access control, alarm monitoring and reporting, time management, and user identification cards shall be installed in accordance with the manufacturer's installation instructions.
- B. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the installation of the System.

3.4 FIELD TESTING AND CERTIFICATION

- A. Testing: The control, alarm monitoring and reporting, time management, and user identification cards shall be tested in accordance with the following:
 - 1. Conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing and verifying connection to equipment of other divisions such as life safety and elevators.
 - 2. Provide staff to test all devices and all operational features of the System for witness by the Owner's representative and authorities having jurisdiction as applicable.
 - 3. Correct deficiencies until satisfactory results are obtained.
 - 4. Submit written copies of test results.

3.5 PROTECTION

- A. Protect installed products until completion of project.
- B. Touch-up, repair or replace damaged products before Substantial Completion.

(*) Future Development

(**) USA version only

END OF SECTION