

Specifications and Terms Of Reference

For the supply and installation of Access Control System at

Definitions

Access control system is an integrated solution that consists of hardware and software designed to control entry into selected areas and manage movement of people/vehicles within. The system is designed to increase security by defining access permissions based on area and time for each user and maintaining a log of all events.

Components of an access control system:

Software: Used to adjust all parameters of the system, control hardware, display events related to movement of users, alarms, and operation of hardware devices. The software is also used for storing all events in the database and generating reports based on requirements defined by an operator.

Electromechanical hardware:

- Electric locks
- Parking barriers and garage gates
- Turnstiles

Electronic hardware:

- Controllers: receive settings from software and control the electromechanical hardware of the system.
- Contactless readers: read unique numbers of identification cards/tags and forwards the numbers to controllers.
- Fingerprint readers: scan fingerprint images, compare them with the templates stored in the internal reader database (or on a smart card) and send the verification results to controllers.

System users:

- Operators: responsible for administrating the system, creating new users, issuing cards and performing other regular daily tasks.
- Users: regular staff of the company, with permanent or long-term ID cards (or PINs), who use the system to gain access to certain building areas as configured by operators.
- Visitors: people that are not employed by the end-user company, but still have rights to access certain areas (contractors, visitors, delivery people, etc.).
- Vehicles (or other equipment): are accounted for and their in/out movements are controlled and tracked by the system, in order to prevent unauthorized vehicles from entering parking areas, or valuable equipment from being taken without authorization.

Technical requirements

A. Software

1. The number of cards/users shall be limited only by memory available in hardware.
2. At least 1 active cards per user shall be supported.
3. At least 2 access levels per user shall be supported.
4. Access levels should be assigned to a user, not to a card, in order to help issue a new card in a fast and easy manner, without reassigning access levels.

6. The software shall have the ability to produce the following report types: system and alarm event reports, user reports, access level reports
7. The reports shall be available in Adobe PDF and MS Excel formats.
8. The software shall have the ability to automatically display photos and additional information about users as they enter/exit through doors.
9. The software shall be available in the official language(s) of the country where it is being installed. If such language is not included in the standard installation, the software shall support user friendly translation method: simply replacing program text directly in the software (“on the fly”), without the need of sending any files to the manufacturer for compiling.
10. The software shall have a modern interface, attractively designed and convenient to use.
11. The software shall be adapted for operators who have not received any special training related to management of integrated security systems. Graphical user interface shall be intuitive. Introducing the system to a new operator shall not take more than 1 hour.
12. In order to reduce the amount of work done by an operator, the software shall incorporate an option to copy objects: users, doors, floor plans, time schedules, access levels and holidays.
13. The software shall facilitate integration with other systems of the building.

B. Hardware

1. The hardware shall support open architecture. Communication protocols shall be available to system integrators and software development companies in order to protect end-users from being constrained to a single brand of hardware or software.
2. The hardware shall support all industry standard readers that output information in Wiegand or Clock/Data formats (up to 128 bits).
3. There shall be at least 2 types of controllers: (a) for one door with an entry reader and an exit button and (b) for one door with two readers (entry and exit) or for two separate doors with entry readers and exit button.
4. There shall be an IP-reader available. The IP-reader shall integrate a contactless card reader and controller in a single body, designed for surface mounting on a wall or a door frame eliminating the need for enclosures.
5. Each controller and IP-reader shall have a standard RJ-45 network port for communication with software and other controllers.
6. Controller and IP-reader shall support standard Ethernet 10/100BaseT network and TCP/IP communication protocol.
7. Systems using Ethernet converters, adapters, or terminal servers that enable network connectivity for legacy controllers by tunneling RS-232/485 serial data over Ethernet shall not be acceptable.
8. Single-door controller and IP-reader shall have at least 32Mb SDRAM operating memory and 8 MB Flash memory for database and events. Two-door controller shall have an option for expanding Flash memory to 32MB.
9. All controllers and IP-readers shall use a 32 Bit 100 MHz RISC processor (or better) in order to enable fast execution of advanced functions.
10. Controllers and IP-readers shall use Linux operating system and accept firmware upgrades via network.
11. All system parameters including card numbers, PINs, access levels, time schedules, holidays and operations modes shall be stored in controller and IP-reader memory and not affected in case of a power loss.
12. Single-door controller and IP-reader shall have enough memory to store at least 40,000 users. Two-door controller shall have enough memory to store at least 250,000 users.
13. In case communication with the host PC is interrupted, the controller and IP-reader must have enough memory to store at least 5000 latest events (FIFO buffer).
14. Operation of controller and IP-reader shall be completely independent of the PC or "Master controller". Should the PC or the communication link fail, the users should not be affected in any way and all functions should continue working.
15. IP-reader shall have the following inputs and outputs:
 - i. Exit button input
 - ii. Door contact input
 - iii. Auxiliary alarm input
 - iv. Tamper sensor and tamper input
 - v. Inputs for monitoring AC power and backup battery state. There should be an option to reconfigure these inputs to function as general purpose inputs.
 - vi. Relay for controlling an electric lock.
 - vii. General purpose auxiliary output relay.
16. One-door controller shall have the following inputs and outputs:
 - i. Power output for the reader
 - ii. Outputs for controlling LEDs and beeper of the reader

- iii. Wiegand or Clock/Data input
- iv. Exit button input
- v. Door contact input
- vi. Auxiliary alarm input
- vii. Tamper input
- viii. Inputs for monitoring AC power and backup battery state. There should be an option to reconfigure these inputs to function as general purpose inputs.
- ix. Relay for controlling an electric lock.
- x. General purpose auxiliary output relay.

17. Two-door controller shall have the following inputs and outputs:

- i. Power output for two readers
- ii. Outputs for controlling LEDs and beepers of the readers
- iii. Two Wiegand or Clock/Data inputs
- iv. Two exit button inputs
- v. Two door contact inputs
- vi. Two auxiliary alarm inputs
- vii. Tamper input
- viii. Inputs for monitoring AC power and backup battery state. There should be an option to reconfigure these inputs to function as general purpose inputs.
- ix. Two relays for controlling an electric lock.
- x. Two general purpose auxiliary output relays.

18. Relays of controllers and IP-readers should support two modes of operation: (a) dry contact and (b) powered mode, whereas power to the lock is provided via relay contacts this way simplifying wiring and eliminating the need for an additional power supply.

19. Controllers and IP-readers shall have an RS-232/485 communication port that would act as a backup communication channel in case the network connection was interrupted.

20. Controllers and IP-readers shall have a built-in PoE capability, in order to reduce wiring and provide backup power effectively. PoE feature must comply with the 802.3af standard.

21. Controllers and IP-readers shall be capable of supplying up to 600mA @ 12VDC to peripheral devices: readers, electric locks, sirens, detectors, etc.

22. Controllers and IP-readers shall accept the standard 12VDC power input in case an existing network infrastructure does not support PoE.

23. In case the main PC of the system fails, controllers and IP-readers shall accept a connection from a laptop in order to diagnose the problem, change settings or control peripheral devices.

24. In case of an alarm controllers and IP-readers shall initiate communication and provide timely notifications to operators. Hardware that does not initiate communication and needs to be polled frequently will not be acceptable due producing needless traffic on the network and processing load on the PC.

25. The system shall support biometric IP-readers with the following or better specifications:

- i. min. 25,000 fingerprint template storage capacity
- ii. 1-to-many verification in less than 1 second (with the database of 3000 users)
- iii. 1-to-many verification with the database of 9000 users.
- iv. min. 500,000 event storage
- v. Built-in USB, RS-232/485, LAN and WLAN communication ports
- vi. Selectable operation modes: fingerprint, fingerprint + card, fingerprint + PIN.

- viii. Microphone, speaker and 2.5" QVGA color LCD
- ix. min. 72MB flash memory
- x. Door contact and exit button inputs
- xi. Lock control relay

Notes:

- can obtain all inputs and records of using the card reader.
- Card Readers:
 - Outdoor weather resistant
 - Networkable; PoE, control panel installed and connected to a fixed workstation.
 - Card reader can open with a card, push button (see next) or a computer override.
- Exit Push Buttons:
 - Outdoor weather resistant
- 7 Automated Locks:
 - Electromagnetic locks, strong enough to hold up to 280 Kg resistance
- Door Closers:
 - Heavy duty, open and close more than 100s times per day, well calibrated and easy to maintain.
- Wiring:
 - Outdoor weather resistant wiring (pipe) linear wiring between all 7 readers locations and the control panel.
 -