ARCHITECTURAL AND ENGINEERING SPECIFICATION

Access Control System

ACTpro

Vanderbilt Industries,
Clonshaugh Business and Technology Park,
Dublin, D17 KV84,
Ireland

TABLE OF CONTENTS

PART 1: GENERAL

1.1 System Summary

The Access Control system shall comprise of a scalable multi-client software application whose primary function is to regulate access through specific portals (doors, gates or barriers) to secured controlled access points. The system will provision for the capturing of cardholder images for printing of photo ID access cards. The system will support an integrated network of TCP/IP controllers and proximity card readers. A dedicated server will allow remote clients (workstations) access using modern client server protocol. Access to the security application software shall be password protected.

1.2 Manufacturer

The hardware and software must be designed and manufactured by Vanderbilt Industries, Clonshaugh Business and Technology Park, Dublin, D17 KV84, Ireland. The manufacturer will be an ISO 9001:2015 registered company.

1.3 Warranty

The product shall be under warranty for a minimum of three years from the date of purchase. Third party products not manufactured by Vanderbilt Industries, the manufacturer's warranty will apply. Software developed by Vanderbilt Industries is governed by the End User License Agreements.

Part 2: HARDWARE

2.1 Access Control Units (ACU) Controllers

Access Control Units (ACU) shall be Single Door TCP/IP based. ACUs shall support Power over Ethernet (PoE++). The system shall employ distributed intelligence where controllers can operate in standalone operation or connected over TCP/IP or RS484 communication protocol. Controllers shall support at least four Weigand and OSDP entry and exit readers per door and be capable of differentiating between valid entry and exit events. The system shall support up to a maximum of 4000 doors. ACU's will support the following;

- Card Holders: 60,000 Maximum
- Credentials per user 4
- User Groups: 1,024 Maximum
- Local Event Buffer 5,000 Maximum

2.2 Communications

ACU devices will use TCP/IP communications protocol over Ethernet. ACU's will be discoverable using NetBIOS over TCP/IP name resolution. In the event of communication failure or interruption, the local ACU shall continue to operate independently using criteria held in non-volatile memory. Events and logged usage shall be stored locally until communication has been restored. The system shall employ a distributed architecture so that all access decisions are made locally. ACUs shall support direct IP 100mbs Ethernet connection for connection with the software.

2.2.1 ACU Communications

Controllers shall be configurable for inter-controller communications when using features such as Global Anti Pass Back, System Lockdown, I/O Control. In the event of a loss of communication with the software, features requiring inter controller communications will be unaffected.

2.2.2 Dual Ethernet Ports

Each ACU shall have onboard dual ethernet ports. The ACU will support LED indication of transmit and receive activity for the Ethernet communications port.

2.3 Power Requirements

ACU controllers will include an integrated 2AMP 12V DC Power Supply Unit (PSU). A Power over Ethernet variant will be available (PoE 802.3bt input PoE++). PSU output shall be monitored and regulated. Both variants shall provide sufficient charge for one 7AMP hour stand by back up battery. ACU will provide 12VDC to connected proximity readers.

2.4 Structured Cabling

ACU controllers shall be networked over TCP/IP or RS485 protocol. ACU controllers shall be connected to standard proximity readers using an eight-core screened twisted cable. The maximum distance between reader and controller will be 100m. Connection to Open Supervised Device Protocol (OSDP) readers will use standard RS485 protocol.

2.5 Wireless Locks

Each ACU Single Door IP Controllers shall have the capacity to manage up to 16 ASSA ABLOY Aperio wireless locks (range dependent). Up to eight Aperio wireless locks will communicate via a single wireless communication hub. Each ACU controller will support up to four communication hubs. Communication hubs will connect to the ACU controller over RS485 protocol.

Wireless Locks shall support the following features;

- Real-time reporting to ACU
- 13.56 MHz MIFARE and DESFire EV1/2 card formats
- Key override (optional)
- 72mm Euro profile key locks.

2.6 Fire Override / Alarm Notification

ACU's shall unlock all doors automatically on Fire Alarm activation. When the ACU receives an input from the fire alarm panel it shall automatically release all specified doors. ACU's shall be hard wired and operate independently of software. ACU's may be configured to activate alarms based upon inputs. Each ACU will generate the following alarm outputs;

- Door Ajar / Door Forced
- Door opened under duress
- Enclosure Tampering
- Voltage Irregularity
- Door break-glass alarm activation

2.7 Input / Output (I/O Module)

An input / output module shall provide additional inputs and output to the ACU. Modules shall support up to 8 supervised timed inputs or outputs. A maximum of four i/0 modules can be connected to ACU controllers over RS485 protocol. Outputs shall be programmed through the application software.

2.8 Housing and Equipment Tamper Switches

ACU controllers shall be housed in a metal container which will allow for 7AMP battery storage. Housings are fitted with equipment tamper switches which consist of a spring-loaded switch assembly. The opening of an ACU enclosure may be configured to trigger an alarm output.

PART 3: CARD READING TECHNOLOGIES

3.1 Proximity Readers

Card reading devices shall be available in Proximity and Pin and Proximity formats. A mullion variant will be available with pin and proximity options. Readers shall be tested to withstand 5 joules of impact to IK08 Standard. Configurable light bar indicators shall indicate power status, valid and invalid reads. The card reader will give an audible indication of each read. Readers will have a minimum read range of 25mm in normal operating conditions. Readers shall be suitable for indoor and outdoor use with a rating of IP55 or greater.

3.2 Reading Protocols

Card reading devices shall read contactless Smart Card 13.56MHz MIFARE DESFire EV1 and EV2 technology conforming to standards compliant ISO/IEC 14443-4. Proximity readers will support Open Supervised Device Protocol (OSDP). Proximity readers will also be available to support 125KHz standard PROX formats.

PART 4: SOFTWARE

4.1 System Architecture

Access Control Software (ACS) shall be Microsoft Windows based and provide a multi-tasking environment that allows operators access the system from a server or client PC. An Enterprise level system will provide the standard IT tools and innovative distributed architecture. The software provides the functionality to control up to four thousand doors and up to fifty PC client work stations.

4.2 Modular Based

The application shall have true multi-tasking, multiprocessor and remote client support allowing independent activities and monitoring to occur simultaneously at multiple locations. The operator workstation (Client) shall be user friendly, employing icon-based menus and providing a mouse-driven interface for system operation and the creation of color graphic maps. It shall be an intuitive user interface that is similar to Microsoft's Outlook and Explorer with easy navigation with tree structures.

The application shall optimize the following role-based access modules;

- Installation Module
- Manager Module
- Monitoring Module

4.3 Multi Tennent

Systems with a large number of doors and users can be partitioned into smaller manageable systems (Sites). Operators can view and configure attributes (access rights, alarm events, time zones etc.) that belong to their site. Operators shall not see attributes from other sites. As new items are added to the database, the administrator can assign the items to appropriate sites.

4.4 User Authentication and Password

The application shall support Microsoft Windows Active Directory authentication single sign on (SSO). When not using SSO operator passwords shall be encrypted in the database to prevent it from being easily copied. The clients shall support the use of strong password authentication.

When defining operators' access levels, the system shall allow the level of assignment to be specified. These levels include the following;

- Full access
- Modify access
- Read only access

4.5 Rules Mapping

The application shall include a rules-based engine allowing operators to automate actions based on customized trigger events or outputs. Rules can be created using an analyzer logic feature to issue commands to doors AND/OR users. Analyzers are used to trigger a rule when it is evaluated as TRUE or FALSE. The rules engine shall be intuitive and easy to use and include email notification as standard. The application shall include intrusion alarm integration as per the manufacturer's specification.

4.6 Interactive Site Map

The application shall support the use of interactive Site Maps. Graphics and floor plans shall be configured in a JPEG, GIF or Bitmap format to allow for the importing of existing site drawings. Upon activation of a selected alarm, the system shall automatically display the associated graphic / floor plan on the PC monitor. The operator shall use the mouse to click on an icon on the graphic and acknowledge / cancel alarm events as well as operating the door.

4.7 Mobile APP

Operators can access the application from an IOS and Android mobile application. Features include;

- Instant system status report
- Real time Muster reporting
- Quick access to notifications, card users and doors

4.8 Lockdown

Designated doors may be locked remotely in the event of an emergency using software application or from a dedicated card reader. When the emergency is resolved, lockdown may be cleared returning doors to prior status. Doors that are in lockdown will be displayed by a large red icon.

4.9 Intruder Alarm Integration

The system shall have the capability to be integrated with the manufacture's intrusion detection systems. Intrusion panels may be monitored audibly and visually and from the application site maps tool. The operator shall have the ability to arm / disarm areas and inhibit / disable zones. Alarm events can be acknowledged and take the appropriate action. The operator shall be able to limit the display of alarms to just those that apply to the client workstation.

4.10 Video Integration

The application software shall interface with video management systems including Vanderbilt Eventys, HIK Vision (HIKCentral version 1.2) and Milestone XProtect software platform or Physical Security Information Management (PSIM) systems.

4.11 Elevator / Destination Control

The software shall include a destination control module which integrates with Kone Group Controller system. Generated events will be intercepted and will cause a message to be passed to the Kone lift system with an appropriate destination mask. This causes the elevator panel to light up available floors to the user.

4.12 Backup and Recovery

All system data must reside on a SQL database on the network and must be accessible in real-time to every / any system workstation. This allows for automatic change propagation to all workstations on the system as well as a common database to consolidate all information and allow for efficient disaster recovery.

4.13 API

The application software shall have an open standard API available to developers for third-party integration. The types of application supported include HR systems, Payroll, and Video surveillance systems. Third party developers will require a licensed API supplied from the manufacturer.

4.14 Card Design and Printing

The application software shall facilitate the design and printing of Photo ID cards which shall allow the operator to create unlimited card templates which may be printed from the software. The card templates may be configured to display the card holder's photo, company logo, user details etc. Card design will include barcode printing and magnetic stripe encoding.

4.15 Hardware Requirements:

Server

1. Windows Server 2016/14/12/08
2. Microsoft Windows 10
3. Microsoft Windows 7 Professional 32 bit or 64 bit
4. Microsoft SQL Server 2016/14/12/08 Express or Professional

Hardware

1. Processor: P4 2.4 GHz, Memory; 4GB Ram Min

PART 5: SUPPORT RECOURCES

5.1 Contact Details

Ireland

Michael Byrden
Telephone: +353 1 9601100
Email: michaelbyrden@vanderbiltindustries.com

Address: Clonshaugh Business and Technology Park
Dublin
D17 KV84
Ireland

5.2 Support Details

Ireland

Michael Byrden
Telephone: +353 (1) 9601100
Email: michaelbyrden@vanderbiltindustries.com

Address: Clonshaugh Business and Technology Park
Dublin
D17 KV84
Ireland

UK

Michael Byrden
Telephone: +44 (0) 2036 300 670
Email: michaelbyrden@vanderbiltindustries.com

Address: Vanderbilt International (UK) Ltd.
Suite 7, Castlegate Business Park
Caldicot
South Wales
NP26 5AD
UK