QUANIKA (Compact) A&E Specification

May 20th , 2019

Document Control Information

Document Title: Quanika (Compact) A&E Specification **Doc version:1.0**

Revision History

Version	Date	Primary Author	Description
DOC-V 1.0	05/08/2019	Ef	Initial Document
DOC-V 1.0	19/08/2019	EF	Revision 1
DOC-V 1.0	20/08/2019	EF	Revision 2

Table of Contents

A Revolution at the Door

IP opens doors to a new world of physical access control. It is no exaggeration to say that network video has revolutionized the world of CCTV. Now the access

Control industry is on the verge of a similar, groundbreaking development. Once again, the driving force is the transition to TCP/IP-based systems.

Since the introduction of the first network camera by Axis Communications in 1996, digital network video surveillance systems have developed fast and now delivers a wide variety of advanced features that never could have been be attained by solely relying on analog technology. Today, distributors, integrators and, not the least, end users have come to expect a wide range of useful functionalities, such as remote accessibility, high image quality, event management and intelligent video capabilities along with easy integration, better scalability, greater flexibility and cost-effectiveness.

Quanika Access Control System (QAC)

Quanika Access Control System (QAC) Overview

Scalability

The QAC shall support small two-reader access systems up to medium size, multi-building, multi-site systems supporting up 128 number of doors and unlimited card holders using a single suite of software.

Available software modules shall include

1. Access Control Software Module.
2. Alarm Management & Reporting Software Module.
3. Interactive Graphical Floorplans Software Module.
4. Identity Management Software Module.
5. Q-Vision Video Integration module.
6. Elevator Control.
7. Time & Attendance Reporting Software Module.
8. Auto Import/Export Software Module.
9. Database Integration Software Module.
10. Mobile Identification and Verification Software Module.
11. Report Generation Software Module.

System requirements

The QAC software shall be designed as a fully integrated, full featured, Security Management System software package. The QAC software shall be fully compatible with x86 and x64 versions of all approved operating systems.

In order to run the Quanika Compact Software, following should be the minimum system requirements

1. Quad Core Processor or better (core Ix or XEON)
2. 16 GB ECC SD RAM minimum
3. 300 GB minimum disk drive
4. 10/1000 Ethernet NIC

The following are the supported operating systems of Quanika application

1. Windows 7
2. Windows 8
3. Windows 8.1
4. Windows Server 2016
5. Windows Server 2016 R2
6. Windows Server 2014
7. Windows Server 2014 R2
8. Windows Server 2012
9. Windows Server 2012 R2

10. Windows Server 2008
11. Windows Server 2008 R2

The QAC software is fully compatible with the following SQL database engines:

1. SQL Server 2017 (Express, Standard, Enterprise (x86, x64)
2. SQL Server 2016 (Express, Standard, Enterprise (x86, x64)
3. SQL Server 2014 (Express, Standard, Enterprise (x86, x64)
4. SQL Server 2012 (Express, Standard, Enterprise (x86, x64)
5. SQL Server 2012 R2 (Express, Standard, Enterprise (x86, x64)
6. SQL Server 2008 (Express, Standard, Enterprise (x86, x64)
7. SQL Server 2008 R2 (Express, Standard, Enterprise (x86, x64)

System Overview

The QAC software shall be of an open architecture design. The QAC software shall be ODBC compliant; supporting industry standard, off-the-shelf, relational databases. It is compatible with standard network communications, field controller hardware, and other standard- based systems and devices. It can be easily integrate/interface with 3rd-party software and hardware through the use of available SDK's and/or API's.

The QAC is a true multi-user, multi-tasking operation software. The host server and client workstations include an operator interface supporting full system command & control functionality, database configuration and reporting capabilities. The functionality of the software is not limited in any way except by user authentication and individually defined operator permissions.

The QAC software dashboard screen provides the system monitoring and control functions including an alarm log window, a transaction log window, interactive graphical plans, system statistics window, cardholder picture, live camera video and other supporting functions.

The QAC access control software supports the creation and configuration of an unlimited number of schedules. Each schedule shall define specific day and time criteria applicable to various hardware & software time-controlled functions within the system, including cardholder access privileges at doors, scheduled override commands to system devices.

The QAC access control software supports Elevator control using I/O Peripheral devices. The elevator access for cardholders are manageable and can be configured through a dedicated interface.

The QAC access control software supports Mustering system. Using Mustering feature, multiple areas can be monitored. The statistics & reporting is available for operational and security staff.

The system functions and features are explained in detail below.

Dashboard

Alarm Monitoring

The QAC software provides full featured alarm monitoring and control of alarm, trouble, and off-normal conditions from various devices including card reader-controlled doors and any other type of alarm sensor connected to inputs on the system

The alarm log window provides real time alarms from controllers. The number of real time alarms in the list can be increased or decreased through a selection from dropdown list. Real time transaction logs can be extracted from the log list in the formats of csv, txt and pdf. The operator with the valid privileges can acknowledge or delete alarms. Alarm notes can be added to each alarm which can be used for reporting purpose in future. Alarm events are reported and listed in the alarm log in the order of priority and date/time and number of occurrences.

Transaction logs

The transaction logs are separately getting recorded and shown in the software. The number of real time transaction logs in the list can be increased or decreased through a selection from dropdown list. Real time transaction logs can be extracted from the log list in the formats of csv, txt and pdf.

Cardholder Picture

The cardholder picture window displays the picture of respective cardholder against every transaction. This can facilitate security staff identifying an individual without going into the details of transaction details.

Live Camera

Operators can select a camera of their choice to be viewed on dashboard all the time. The same live camera window can be used to show video related to transaction.

Plan Manager

The QAC support the interactive graphical plans and maps. The plans configuration shall allow for the linking of maps via navigation Icons, allowing the QAC user to move from map to map with single mouse click. There shall be no limit to the number of plans that can be used in the QAC. The plans allow for the assignment of interactive Icons for the following

1. Doors
2. Inputs (sensors).
3. Outputs.
4. Outputs Groups.
5. CCTV

The interactive Floor plans allow the system operators through Icons to perform functions like

1. Unlock doors,
2. Lock doors
3. Momentary Unlock Doors,
4. Lockdown doors
5. Lockdown Clear doors

6. Acknowledge alarms
7. Delete Alarms
8. Add Alarm Notes
9. View Camera
10. Switch On/Off Outputs
11. Access Intercom
12. Plan Navigation

The following options of the plan is configurable from the settings

1. Plan manager is a floating window and provide flexibility to set it up on a separate window.
2. Default plan can be selected through settings.
3. The time out settings that a plan will remain displayed after alarm is received and before returning to the default plan.
4. 'Jump' to the specific plan after alarm is received.
5. Set the icon size
6. Show the name and status of a point on a plan if the cursor is placed over the icon (tooltip).

Q-Vision Video Integrator

The Q-Vision is a Video Integration Interface built to have flexibility to integrate with any video management software. With this interface the QCS has got a powerful and integrated interface where security staff can relate alarms with video.

Q-vision communicate and extract the list of cameras from the video management systems and provide operators the following features

1. Create Views
2. Create Matrix
3. Playback videos
4. Transaction Search
5. PTZ Control
6. Presets

Access Controllers and Door Controllers

The QAC are integrated to Axis A1001 & A1601 controllers. It communicates with the controllers via standard TCP/IP Ethernet via standard TCP/IP Ethernet. All Access controllers are fully intelligent and distributed processing controllers. The applicable system database and operating parameters are downloaded from the QAC host server to the access controllers and stored locally in its local memory. All access requests from card readers, local linkage parameters, and scheduled functions are processed locally at the access controller with no assistance required from the QAC host server.

If any loss of communication occurs between the System and the Controller, the controller will continue to validate local transaction decisions, and stores all events within its own internal

database until communication is restored. Once communication is restored the stored events are uploaded to the database along with actual time stamp of the event occurrence.
The QAC support multiple card technologies, including 125Khz proximity, 13.56Mhz smart card technologies (iClass, Mifare, desfire etc.), Wiegand, magnetic strip, keypads, biometric devices, bar code, QR code. Data interface to the card readers shall support standard Wiegand Data1 / Data0, as well as Clock/Data protocols.
All operational parameters for the door controllers and the specific card readers are completely configurable.

Data Exchange Application (DXA)

The DXA is an interface between controller and the Database Server.

1. It has a two-way communication.
2. It keeps the controller up to date with the latest information by fetching updates from database server and at the same time fetching transactional data from controllers and update database server.
3. It monitors and report the real time status of the network devices.
4. It acts as a dashboard running as a Windows Service in the background and is independent from the normal QAC functions.
5. It provides an interface to upgrade the firmware
6. It provides an interface to initialize the controllers.

The DXA display a graphical device tree showing the live status of all devices connected to the QAC.

Schedules

The QAC allows creating and storing an unlimited number of schedules for use in the System. It is can create two types of schedules

1. Recurring events
2. One Time events

Recurring Events

You maintain a schedule for events which occur more than once or multiple times

Onetime Events

One time event option can be used if you want to maintain a schedule for an event which is only going to happen once

Anti-Passback

The QAC has the ability for card readers to be configured with anti-passback. The QAC allows for hard anti-passback, soft anti-passback and timed anti-passback, on a per card reader basis. The anti-passback function must not be limited to readers connected to the same area controller, or readers connected to the same QAC communication server. A true global anti-passback system must be supported.
The QAC allows the creation of areas, with card readers assigned to specific areas for anti-passback control. The QAC supports an unlimited number of areas.
Each area is assignable with an alphanumeric name of up to 40 characters.
The System allows the card reader configuration of the following anti-passback functions:

1. Hard anti-passback
2. Soft anti-passback
3. Timed anti-passback
4. Area Entering
5. Area Exiting
6. Hard Anti-passback

When a card is read at a card reader configured with hard anti-passback, and the result is a valid access, the SMS updates the cardholder record with the area that the card reader is defined as "entering". If the cardholder requests access at the same card reader, or a card reader defined as entering the same area, the access request will be denied, and reported by the SMS as an invalid access – anti-passback. This event is reported to the system operator, and logged in the SMS transaction file.

Soft Anti-passback

When a card is read at a card reader configured with Soft anti---passback, and the result is a valid access, the SMS is updated the cardholder record with the area that the card reader is defined as "entering". If the cardholder requests access at the same card reader, or a card reader defined as entering the same area, the access request is granted, however the transaction is reported by the SMS as a valid access with an anti---passback error. This event will be reported to the system operator, and logged in the SMS transaction file.

Timed Anti-passback

Timed anti-passback shall be a function of a defined Area. The Area configuration shall support the configuration of an anti-passback Timer, which is set to a value in minutes from zero to nine hundred ninety nine (0 to 999). A setting of zero (0) will disable the timed anti-passback function for that area. Any value higher than zero (0) will enable the timed anti-passback function for that area, and will prevent any cardholder using their card again for the duration of the timer setting. Once the time has elapsed the card can be used again at that reader.

Operator Access and Permissions

The QAC shall support the definition of unlimited number of system operators. Operators shall be defined as administrators or general operators. Administrators shall automatically have access permission to all functions of the QAC software.

Each system operator shall be defined with a unique operator name and password. The operator password shall consist of up to 16 alphanumeric characters. A schedule shall be assigned to each operator to further define the times and days that each operator can have access to the QAC.

Each system operator shall be definable with specific access permissions on a per menu or function basis within the QAC software. Operator permissions can be specified as full permission, read-only, or no permission for each of the specific configuration, monitoring, and command functions, as well as specific reports within report generation.

Defined operators shall have the option for an expiration date, causing that operator to be restricted from QAC access when expired.

Access Levels

The cardholder database shall support the use of access levels for defining what doors/portals

the cardholder is authorized to enter. Each access level shall be defined as a list of card reader controlled doors/portals, along with an assigned schedule to designate when the cardholder is authorized to access that door.
Each access level shall be defined with an alphanumeric text name for easy recognition.
The cardholder record shall allow the assignment of multiple access levels to the same cardholder.

Rules Management

The QAC shall support the ability for an event or input to be linked to an event or output. The linked event could cause any of the following linked dependencies

1. Door Momentary
2. Door Unlock
3. Door Lock
4. Door Group Momentary
5. Door Group Unlock
6. Door Group Lock
7. Door Lockdown
8. Door Lockdown Clear
9. Output Momentary
10. Output On
11. Record Video of 5 seconds for any camera in Q-vision
12. Move Camera to Preset Location
13. Show Live Streaming
14. Take a snapshot from specified camera

The QAC shall allow for the ability to alter event system event messages as either a Global setting or on an individual input.

REPORT GENERATION SOFTWARE MODULE

1. The QAC shall include a full featured Report Generation Utility to display or print database information Reports.

The Report Utility should contain the following functionality:

1. Parameter select functions
2. Search between two date/time stamps
3. Search on event time
4. Export to Excel (XLSX)
5. Export to PDF (PDF)
6. Export to Word (DOCX)

Cardholders Management

Managing your card holders' data effectively is one of the fundamental tasks you perform in the application. Cardholder management module allows to register a new card holder and manages the existing card holders' data as well. Physical cards are assigned to the users along with their specific details.

Card holders and access levels

1. You can add a new access level by specifying details
2. Existing access levels can be accessed through access level tab in card holder details panel
3. Elevator access levels can be created by adding a name for the access level, schedule and multiple floors for the associated elevator. Existing access levels can also be modified as per the user requirement.

Adding cardholder details

To add a card holder, specify Card number in decimal format, raw card data in lower case hexadecimal, 4 digit pin and a facility code.
Following information is required:

1. Appropriate reader
2. Validity period [specifying the valid from and valid to dates and time]
3. Status

Enable anti pass back override mechanism if required.
Save card info for the specified cardholder

Database Backup/Restore Module

Database recovery and backup are help in case of accidental loss of information. Database module is used for backup and restore of the application data.

Backup: You need to specify a destination where you want the backup file to be created.

Restore: To restore, select a source from drop down list and provide an associated name.

Elevator Control

QCS supports elevator control through the use of standard card readers and A9188 controller for relay outputs to control the floor selection buttons inside elevator.
A9188 is a peripheral device which can be configured as a stand-alone module and can be used to function elevator system. QCS supports only two A9188 controllers together with one controller.
The elevator control will allow cardholders to be assigned an elevator access level that will allow access to floors designated within the assigned access level. The cardholder will present their card to the elevator reader and the outputs corresponding to authorized floors will be enabled for floor selection.

e-Mustering solution

QCS provides mustering solutions which mainly works with Areas. It provides an interactive interface for monitoring mustered areas and give useful information to security personnel for quick actions in an emergency situation.
At the time of emergency, the mustering dashboard displays people present inside multiple areas. The user can quickly see the missing person's name, and his last recorded location and time. The Mustering dashboard continuously updates with the latest data.

Physical Access Control System

ONVIF Profiles 'A' and 'C' compliance requirement

The growth in interoperability between access control and other devices is key to the end user 'fit for future' philosophy. Access controllers and field devices must be able to function on different software platforms; i.e. the controllers shall not be restricted to one manufacturer software. This is essential to afford end users with choice, both in immediate selection and to ensure the QCS remains fit for purpose over time, as demands and needs change. Access controllers shall demonstrate conformance with ONVIF Profiles A & C.

OSDP compliance

The controllers should be compatible with OSDP (Open Supervised Device Protocol) door readers. The QCS shall also be capable of both 125 KHz and 13.56 MHz Wiegand door reader technology, within a transition path from lower to higher frequency, the timing of which is dictated by the end user.

IP / Networked Controllers

The system shall be an IP based configuration with controllers connected via a dedicated network switch. Only IP controllers which are designed specifically for connection to company or security networks are acceptable.

PoE controller power / lock output

The controllers shall use PoE as the basis for operating power, together with lock output power, managed directly from the controller and configuration menu. Where additional power is required, the bid shall include power enclosures designed as suitable for user lock demand and power/battery back up in the event of a power outage and tested to perform with the nominated QCS controller.

Controller - operational overview

1. The Controllers should be configurable in a 'by the door' design; i.e. capable of location close to doors, thereby reducing the cabling to readers and door furniture (sensors, locks, buttons, etc.). Each controller shall have a housing fit for that purpose, with tamper sensing for cover and base removal. Controllers must offer a scalable growth path to

enable the user to decide, on their timescale, if expansion of the system is required. Which is scalable and can be able to be adapted to a variety of applications. Each controller shall have, as standard, its own administration software for single controller installation. Set-up, alarms, events and a full reporting solution for all events and actions are to be included in the admin software.

2. Controllers should be able to operate without need for a permanently connected server or pc, where necessary and preferred. This is useful where a single controller or smaller installation can function without incurring additional costs of servers / pc's. UI software and configuration programs useful for the set up and commissioning / re-programming of controllers and
    a) Enhanced management of rules across several controllers are of course accepted for that
    b) Purpose.
3. Multiple controllers may be connected in a standalone network, to be administered by any pc, without the need for that pc or server to be connected during normal operational mode (out of configuration). Access to the controller(s) is achieved via a web enabled device and the device's IP address.

Door monitoring contacts

Door monitoring contacts shall be installed to each opening leaf of each door to be monitored to check the door status where this is not achievable through an access control lock or where an access control lock shall not be installed.

Electric locks

All electronically controlled locks to be installed shall meet current building regulations. The type of lock shall take into account the nature, construction and use of the door, the volume of traffic and the level of security required. The Contractor shall confirm in their tender response which locks they propose for each door.

All locks that are fitted shall be of the type that allows monitoring of the lock by the system or a door contact must monitor each door leaf.

Any one and a half and double leaf doors shall have both leaves fitted with a locking device or the contractor shall obtain agreement from the client that the half leaf is to be normally secured shut using alternative mechanical locks.

All locking devices shall have a holding force of at least: 12 kN.

All locking devices shall adhere to the requirements of PAS 24:2012 requirements and will be tested as part of the full door set.

Fail safe/fail secure

All access control doors shall fail safe in the event of a fire alarm.

Emergency break glass units (BGU)

Green emergency break glass units shall be installed adjacent to each access controlled door to allow the door to be released in the case of an emergency.

The BGUs:

Shall either have "EMERGENCY DOOR RELEASE" etched in white or a pictogram of a man exiting. The style shall match that of the red fire BGUs.

Shall match the red fire BGUs in molding

Shall utilize resettable plastic elements.

General Controller Specification Consideration

1. Safety
2. IEC/EN/UL 62368-1
3. Environment
4. IEC/EN 60529 IP20, UL2043 Plenum rated, NEMA 250 Type 1, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27

Warranty

The controller unit shall be backed by a minimum of three years' manufacturer warranty. The manufacturer shall provide the option of extended warranty for the unit. The optional extended warranty shall be available for a total warranty period of maximum five years.

Sustainability

1. The specified unit shall be manufactured in accordance with the environmental standards as defined in ISO 14001.
2. The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).
3. The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).
4. The specified unit shall be PVC-free.
5. The manufacturer shall have signed and support the UN Global Compact initiative as defined by United Nations https://www.unglobalcompact.org/
6. The manufacturer and its sustainability strategy and policy, shall be based on the ten principles outlined by UN Global Compact, relating to;" human rights, labor, environment and anticorruption".

Quality Assurance

1. The manufacturer shall go through documented physical testing to ensure the products' complete functionality for the complete specified operative environments in a worst-case scenario.
2. The specified unit shall be manufactured in accordance with ISO9001.