ENGINEERING AND ARCHITECTURAL SPECIFICATIONS

COMPLETE SOLUTION FOR
WEB ENABLED PHYSICAL ACCESS CONTROL

FEBRUARY 2020

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to outline the specifications, architecture and submission criteria for a Physical Access Control System (PACS), communicating via Broadband Ethernet (BBE) using technologies such as private corporate networks.

SYSTEM DESCRIPTION

ATRIUM, the Ethernet communicating Integrated Access Control and Security System's primary function, is to allow businesses to regroup all of their security system installations into 1 (one) system, no matter what the distance is between each one. Secondly, ATRIUM will allow for management of all the systems from 1 (one) single point. Thanks to ATRIUM's innovative architecture, the cost, time and installation complexities normally related to such a system, are practically eliminated. In addition, the system's architecture reduces initial configuration time and allows for quick and effective future servicing saving time and money.

ATRIUM, the Integrated Access Control and Security System, can be installed in each of the locations necessary which will all be regrouped and relayed to 1 (one) secure central database. Various workstations can be managed and distributed in different buildings (locations) in order to administer and manage various users as well as other parameters in the ATRIUM system.

ATRIUM is comprised of an innovative and distributed architecture which spreads the work load and provides superior performance and response time. This information is exchanged among all modules via TCP/IP. All communications are protected using advanced proprietary protocols and Encryption Algorithms.

The ATRIUM system also features electronically protected and supervised 12V power outputs commonly used to control standard door locking devices such as direct current (DC) door strikes and/or magnetic locks.

KRYPTO
HIGH SECURITY SOLUTION

Say ***"NO"*** to card cloning with ATRIUM's unique KRYPTO high security solution.
Eliminate complex and arduous programming using the ATRIUM A22K controller, CDVI Mifare DesFire EV2 credentials and CDVI K1 readers. Systemwide AES encryption stops card cloning and provides end-to-end security.
Whether you remote in from the internet or connect on your network you can be sure KRYPTO has you covered.

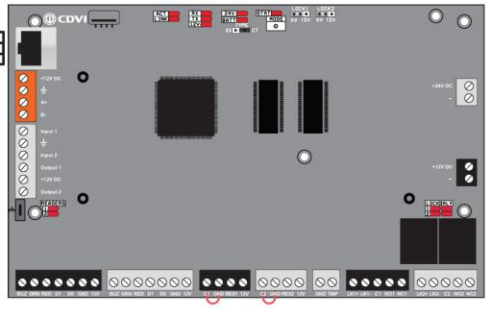
ATRIUM Network Connectivity

IP CONNECTIVITY

Out of the box the A22K is ready for IP connectivity, fifty (50) A22K per account.
If you have more than one A22K controller per account, one must be set as the ***"Master"*** controller to manage the others. These forty (49) others are defined as ***"Sub-Controllers"***.

"MASTER" CONTROLLER

The ***"Master"*** controller manages up to forty nine (49) ***"Sub-Controllers"***.
(100 doors fully IP)

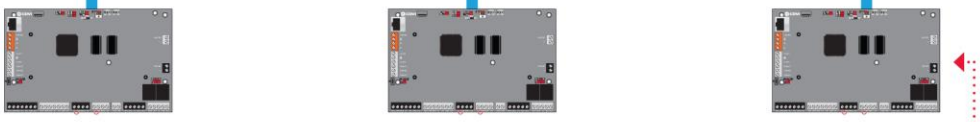


AES256 ENCRYPTION

Communication between the ***"Master"*** controller and its ***"Sub-Controllers"*** is done by TCP / IP **ONLY**.

IP Network
Maximum 300 ft (100 m)

LAN or WAN



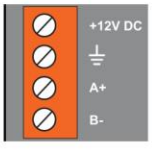
"SUB-CONTROLLERS"

Up to forty nine (49) A22K defined as ***"Sub-Controllers"***.

RS485 CONNECTIVITY

An A22K can be set as an ***"Expander"*** (see below). Up to four (4) can be connected to the RS485 network (orange connector) of the ***"Master"*** or ***"Sub-Controllers"***.

A22K ***"Master"*** or ***"Sub-Controllers"*** RS485 port (orange connector).

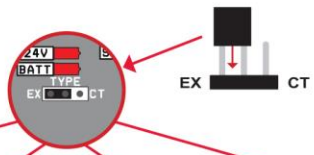


Use twisted pair wiring for RS485 connection (1 pair for ground and 1 pair for A+ B-)

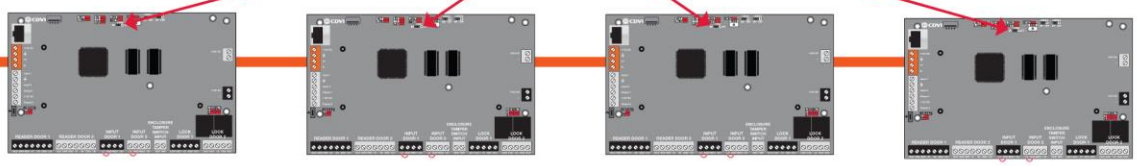
Maximum 4000 ft (1220 m)

How to set an A22K as an "Expander"

On power OFF, move the ***"Module Type"*** jumper setting to the two pins closest to ***"EX"***.



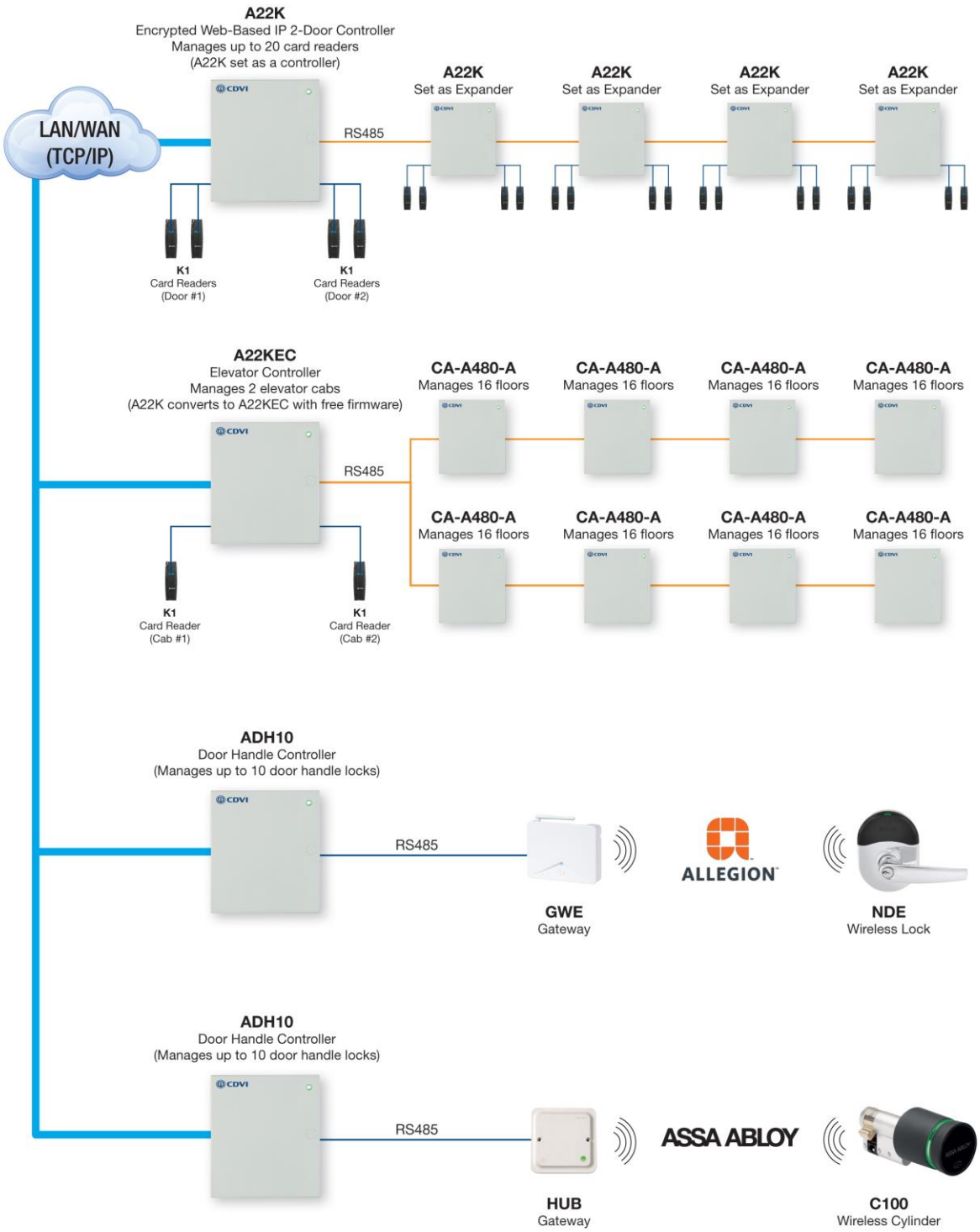
DO NOT use IP connection when A22K is set as ***"Expander"***.



A22K set as ***"Expander"*** | A22K set as ***"Expander"*** | A22K set as ***"Expander"*** | A22K set as ***"Expander"***

The ATRIUM system supports any combination of fifty A22K, A22KEC and/or ADH10 controllers for a maximum of 500 doors.

Below, a reference diagram of ATRIUM - the Integrated Access Control and Security System:



RELEVANT DOCUMENTATION

These documents contain certain portions of the ATRIUM product documents listed below, which may be consulted for more details:

- A22K 2-Door Controller Manual
- A22KPOE+ 2-Door Controller Manual
- A22KEC 256-Floor Elevator Controller Manual
- AIOM 10 Input/Output Module Manual
- ADH10 10-Door Handle Controller Manual
- A10 Software Manual

2 SYSTEM ARCHITECTURE

The following sections provide an overview of ATRIUM's specifications, hardware modules, features and functionalities.

DATABASE SERVER

The central database is conveniently located on a 2-door controller accessible via web-enabled devices such as smart phones, tablets and commonly available computers via their web browsers allowing day-to-day management.

PC (personal computer) software is also used to access the central database and incorporates advanced configuration menus and features.

WEB SERVER

1. An embedded web server is included in each ATRIUM's controller.
2. The embedded web server allows access by various web browsers.
3. ATRIUM has an embedded SDK that exhibits ALL ATRIUM commands.

WEB NAVIGATION ACCESS

1. The ATRIUM Controller (A22K) is accessible by any standard web browser on multiple platforms including, but not limited to, Microsoft Windows®, MacIntosh MAC OS, iPhone iOS, Android and Linux.
2. The ATRIUM Controller (A22K) supports connectivity with a Microsoft Windows® personal computer (PC) using ATRIUM's free software.
3. The basic configuration and consulting functions are offered by using any standard web browser.
4. ATRIUM's PC software allows complete and advanced system configuration.
5. The ATRIUM Controller (A22K) supports up to 10 simultaneous web browser connections and one software connection.

AUTHENTICATION & ENCRYPTION

1. All commands between the web browser and the ATRIUM controller are protected, thus encrypted by various protocols including SSL/TLS, RC4 and MD5.
2. All communications between the ATRIUM Server Software and the ATRIUM system are protected, thus encrypted by AES protocol with a 256-bit key.
3. All network communication between the ATRIUM controller and its peripherals are protected by a proprietary protocol. All network communication between the system and all peripheral ATRIUM will be protected by a proprietary protocol (AES256 encryption) for rapid high performance.
4. All communication between the ATRIUM controller and the web browser must first be authenticated and authorized.
5. All communication between the ATRIUM controller and server software must first be authenticated and authorized.
6. All communication between the ATRIUM controller and its peripherals must first be authenticated and authorized.

NETWORK ACCESS VIA BROADBAND

1. The ATRIUM controller shall communicate via internet or corporate ETHERNET network.
2. The ATRIUM controller must be connected directly to the main control panel via ETHERNET.
3. The main control panel is equipped with an RJ45 connector to allow IP Connectivity.

CENTRAL DATA STORAGE UNITS

1. All client data and all configuration settings of control panels and peripherals will be saved in a centralized database and will be distributed to each of the control panels accordingly if needed during the synchronization of the system upon connection.
2. ATRIUM's PC software will provide a mechanism for local or remote backup to preserve all information in the system. The backup data shall be stored on the PC hard drive or corporate network storage device.

3 SOFTWARE / ATRIUM SERVER

Here is a list of features and a more detailed description of certain key functions.

1. Provides central backup of the ATRIUM system information.
2. Allows for database restore as well as data archiving capabilities.
3. History of all time-stamped system events.
4. Allows for multiple managers to simultaneously manage the system (web server only).
5. Allows the user to perform system configuration to ensure the security of installations and sensitive information.
6. Allows the user to customize schedules in order to manage the installation and the testing of devices.
7. Provides robust communication so that exchanges between all system components are effective, reliable and secure.
8. Allows administrators to define and manage their installations and their various access points.
9. Offers different types of users giving them different access rights within the web server and PC software.
10. Allows supervision of the actions taken by the various users across the whole system.
11. Active management of all the pieces of ID associated with an account, a user or a building.
12. Detailed history of all system activities including attempts to access the system.
13. Provision of a protection system that allows administrators to deny rights of access to certain users.
14. Configuration of email transmission initiated by the occurrence of certain events or situations.
15. Ability to create detailed reports of certain activities such as requests for access denied.
16. Provides the means to integrate IP-based cameras for real-time viewing using a web browser.
17. Integrates with any intrusion detection alarm system control panel via key switch arming input.

CUSTOMIZED SCHEDULES

ATRIUM offers 250 schedules each supporting 100 programmable time periods, modifiable and useable for the automatic unlocking of doors, user access rights, macro commands and sending of emails.

ATRIUM allows for the definition of holiday periods, to override normal time periods used in a schedule. The transactions related to timetables and holiday periods include:

- Creating schedules with programmable periods and repetitiveness
- Repetitive schedules allow for a programmable cycle length from 1 to 100 days before repeating the cycle
- The assignment of these schedules for access levels, schedules for unlocking doors, sending emails and the activation of macro commands
- The addition or withdrawal of schedules to/from an access level
- The addition, deletion and modification of one or more periods of time in a schedule
- The combination of days or holiday periods to one or more schedules
- The ability to configure the start time and date of a holiday period and its duration.
- The addition, deletion and modification of one or more holiday periods
- Holiday periods are defined in duration by the number of days, hours, minutes and seconds
- Support for rule-based (day of the week) and fixed date holidays
- Support for automatic annual holiday recurrence
- Holidays periods are removed from (e.g., statutory holidays) or added to (e.g., an inventory day) a schedule

ACCOUNT MANAGEMENT

ATRIUM will allow account administrators the creation and management of accounts including all their associated equipment, such as control panels, doors, areas and peripherals. The system will allow the following :

- The definition and management of control panel accounts
- The configuration of doors to an account and their associations to control panels
- The activation and deactivation of the supervision of doors left open and the definition of the acceptable length of opening
- Define and edit schedules
- Management of request-to-exit detectors
- The activation and deactivation of individuals to some or all of the access points
- The definition and monitoring of alarm conditions and the definition of possible alarm conditions
- The configuration peripherals to a site and the association of these devices to control panels
- The configuration of the behavior of a device
- Tracking events in history
- The removal of devices
- The definition and the modification of unlocking and/or schedules for a door
- The addition of an area
- The withdrawal of an area
- The definition of an area or an area delimited by doors
- Associating areas to both sides of doors

SOFTWARE USER RIGHTS

ATRIUM will provide 4 levels of software user rights to the administrator to create user subordinates (operators). Each of these users (operators) will have a unique ID and password indicating to ATRIUM everyone's rights for consultation, editing and management of information.

Here are the 4-software user rights levels:

SOFTWARE USER RIGHTS

User Rights	Can do firmware update	Can configure the system	Can add, delete or modify users, cards and PIN	View only
1. Installer	✓	✓	✓	✓
2. Administrator		✓	✓	✓
3. Operator			✓	✓
4. View Only				✓

1. For each of the ATRIUM system's operator rights, the following information must be available:

- Given name
- Family name
- Email address
- Telephone number
- Status
- Login ID
- Password
- Secret question and / or hint
- Secret answer

ADMINISTRATOR AND OPERATOR TRACEABILITY

For security reasons, the ATRIUM system must first validate access to an administrator or operator and preserve the history of all the actions taken. In the event of this occurrence, the software will

- Ask the user to provide a login and a password to gain access to an account, its control panels and the associated database
- Support multiple administrators and operators for each account, each with a login ID and password
- Maintain and view a history of all actions taken by administrators and operators of the software to obtain a permanent trace of such actions.

CREDENTIAL MANAGEMENT

The ATRIUM software and web server will support the management of information such as access cards and PINs (**P**ersonal **I**dentification **N**umbers) associated with a user account and their owners.

Possible software operations include:

- The validation of the uniqueness, format and values of a card number
- The ability to combine multiple pieces of user identities to one user
- The ability to record unique up to 8-digit PIN numbers entered by the user
- The provision of a text field allowing the entry of additional information for a user
- Automatic propagation of identities throughout the ATRIUM system to affected devices without any intervention

USER & ACCESS LEVEL MANAGEMENT

The ATRIUM software provides the ability to configure access rights for users having one or more accounts and to allow the assignment of these users to a group of users determining their rights. The possible operations include:

- The creation of an access level
- The modification of an access level
- The removal of an access level
- The creation of a new user
- The assignment of a user code (up to 8-digit PIN)
- The removal of a user code (PIN)
- The modification of a user code (PIN)
- The addition of a card to a user
- The removal of a card from a user
- A card can only be assigned to one user at a time
- Cards can be withdrawn from a user and issued to another new or existing user
- One user can be issued multiple cards
- Setting an activation date of a user
- Setting a termination date of a user
- The modification of a termination date of a user
- The removal of a termination date of a user
- The assignment of a user to one or multiple access levels
- The removal of a user from one or multiple access levels
- The removal of a user
- The assignment of a schedule to access one or more areas to a user
- The assignment of multiple schedules to access different areas to a user
- An access level is issued to a user, not to a card
- Any card(s) is denied access to all doors at all times unless it has been issued to a user with a valid access level

EVENT HISTORY MANAGEMENT

The ATRIUM software will record all attempts to access various sites associated with an account and maintain this information in a history log accessible by administrators of the account.

Event history recording includes :

- Displaying all events stored in history
- Displaying all events stored in history sorted by user
- Displaying all events stored in history sorted by door
- Displaying all events stored in history sorted by peripheral
- Displaying all events stored in history limiting the number of results
- The possibility to conduct a search of events based on certain criteria such as Users, Peripherals, Doors or Account within a specified time period or for a specific date

4 CONTROL PANEL

The following sections describe the characteristics of the control panel.

SUPPORTED READERS

The control panel support K1 Mifare DESFire proximity card reader and a various card reader technologies including WIEGAND standard and ABA TRACK 2:

- Proximity card reader
- Biometric reader
- WIEGAND reader
- WIEGAND keypad
- ABA TRACK 2 magnetic card reader

POWER REQUIREMENTS

1. The control panel must be powered by a standard AC outlet 120Vac or 240Vac and 50 or 60 Hz
2. The control panel shall be equipped with a backup battery 12Vdc
3. The panel will provide the following status display:
   - The control panel will indicate the source of its power; primary or backup
   - The control panel will transmit a signal to the software indicating the transfer of power from the primary source to the backup battery and vice versa
4. The control panel will tell the software if it's powering up, starting and / or restarting

CONTROL CIRCUITS

Out of the box, the A22K and ADH10 are ready for IP connectivity, maximum fifty (50) of any combination per account. If you have more than one A22K/ADH10 controller per account, one must be set as the **"Master"** controller to manage the others. These forty-nine (49) others are defined as **"Sub-Controllers"**. Also, an A22K can be set as an **"Expander"** by changing is "Module Type" jumper setting (hardware). Up to four (4) can be connected to the RS485 network (orange connector) of the **"Master"** or **"Sub-Controllers"**. The A22K can be converted to an elevator controller by changing is firmware (downloadable from CDVI website for ***FREE***). The ATRIUM ADH10 is an integration controller that can manage up to ten electronically locking door handles from ASSA ABLOY or ALEGION (wired or wireless).

IP connectivity:

- A22K 2-Door / 4-Reader Controller (default setting)
- A22KEC Elevator Controller (by changing A22K firmware for FREE)
- ADH10 10-door handle controller (ASSA ABLOY or ALLEGION)

RS485 Connectivity:

- A22K (by changing the module type jumper setting)
  (maximum 4 per A22K "Master" or "Sub-Controllers")
- AIOM Expansion module 10 inputs / 10 outputs (for a maximum of 1000 zones)

These controllers and modules include the following with their maximum amount:

1. Each A22K (out of the box) will provide the following input and outputs:

- ETHERNET 10/100 Communication port (1)
- ATRIUM RS485 Communication port (3)
- Reader interfaces (2)
- Assignable zone input (6), using zone doubling (12)
- Entry tamper detection (1)
- Smart supply output (fuseless) (2)
- Door lock output (2)
- Auxiliary relay (2)
- Low power output (12)
- Battery backup intput (1)

2. Each A22K, set as **"Expander"** (by changing is module jumper setting), will provide the following inputs and outputs:

- ATRIUM RS485 Communication port (3)
- Reader interfaces (4)
- Assignable zone input (6), using zone doubling (12)
- Entry tamper detection (1)
- Smart supply output (fuseless) (2)
- Door lock output (2)
- Auxiliary relay (2)
- Low power output (12)
- Battery backup intput (1)

3. Each A22K, set as **"Elevator Controller"** (by changing the firmware), will provide the following inputs and outputs:

- ETHERNET 10/100 Communication port (1)
- ATRIUM RS485 Communication port (3)
- Reader interfaces (2)
- Assignable zone input (6), using zone doubling (12)
- Entry tamper detection (1)
- Smart supply output (fuseless) (2)
- Door lock output (2)
- Auxiliary relay (2)
- Low power output (12)
- Battery backup intput (1)

4. Each ADH10 Schlage door handle controller will provide the following input and outputs:
    - ATRIUM RS485 Communication port (1)
    - ETHERNET 10/100 Communication port (1)
    - Entry tamper detection (1)
    - Battery backup intput (1)

5. Each AIOM input and output expansion module offers the following inputs and outputs:
    - ATRIUM RS485 (1) Communication port
    - Assignable zone input (10)
    - Assignable zone output (10)
    - Tamper detection input (1)
    - Programmable 12VDC 100 mA output (10)

ACCESS CONTROL FUNCTIONS

Each control panel:

- Supports the request to exit connection and activate (if necessary) the lock output for the opening of the associated door without generating a door alarm condition
- Supports the connection of an auxiliary input allowing the activation an associated relay
- Offers door relay activation and deactivation
- Notifies when there is a prolonged opening of a door or door left open having a programmable timer
- Notifies the ATRIUM system of a door opening by using a contact connected to an input system
- Notifies the ATRIUM system of a door closing by using a contact connected to an input system
- Advises the system of an automatic unlocking of a door
- Provides a local storage unit to preserve an event history
- Offers configuration for a door unlocking schedule
- Offers configuration of holidays
- Notifies all changes of the control panel and / or its peripherals
- Notifies the system of all unauthorized openings of doors

5 ATRIUM PRODUCT SPECIFICATIONS

GENERAL FEATURES

The ATRIUM system was conceived for multiple door and area applications. The system offers as a base, 2 doors, expandable up to a network of 500 doors and areas, which within themselves can be interlinked.

Here are some additional features of the ATRIUM system:

- Management and centralized control of all access and security privileges via any computer or device with INTERNET connectivity with SSL/TLS encryption
- Compatible with virtually all WIEGAND readers
- Memory unit for the automatic recording of events
- Real time updates of all transactions, modifications, configurations
- Up to 10,000 users per account
- 25,000 events per control panel
- Multilingual software
- Automatic detection and dynamic assignment of inputs / outputs of new modules and devices detected on a RS485 network of a controller

HARDWARE COMPONENTS

The following components are included with ATRIUM A22K controllers:

- Universal plug-in power supply 120/240 Vca - 50/60Hz for each control panel and door expander
- 1 Master and 1 Programming card
- User's manual
- Web access quick guide
- Metal cabinet (box)
- Bag :
  - Resistors
  - Supports for printed circuit boards
  - Diode protection systems for door locks
  - Connection cables for backup battery

RECOMMENDED READERS

ATRIUM supports but is not limited to the following readers and keypads:

- K1 – KRYPTO High Security RS485 Proximity Card Reader (Mifare Classic, DESFire EV1/EV2)
- NANOP – Mini Proximity Reader (CDVI encoding)
- STARP – Multi Technology narrow Proximity Reader
- SOLARP – Multi Technology rectangular Proximity Reader
- KCPROXWLC – Multi Technology keypad and Proximity Reader
- DGLP WLC26 – Multi Technology rectangular Proximity Reader
- DGLP FN WLC26 – Multi Technology narrow Proximity Reader
- DGLI WLC26 – Multi Technology stainless, rectangular Proximity Reader
- DGLI F FLC26 – Multi Technology stainless, narrow Proximity Reader
- DGLP60WLC – Multi Technology long-range Proximity Reader
- DGID/W/US – Digital imprint Biometric Reader
- CABAPROX/W – Mifare® Biometric and Proximity Readers
- Additional readers are also supported, on a customized base

ONLINE ACCOUNT MANAGEMENT

A wide range of functions are available to assist account administrators in the management of their buildings such as:

- Web interface with history of system events
- Multitudes of account managers each with individual passwords
- Time-stamped log of system activities
- Customization of users and areas
- Supports card and PIN confirmation
- Supports card or PIN

SERVICE & SUPPORT

To help visualize, understand and enjoy all the advantages of the ATRIUM system, CDVI Americas offer support in a variety of formats:

- Documentation (also available online)
- Online video tutorials
- Quick Start Guide
- User's Manual
- Installation Manual
- Connection (wiring) diagram
- Technical Support: 8:00a.m. to 8:00p.m. (EST)
- Toll-free support line
- Email support
- Online support via SKYPE
- Five-year system warranty

6 TECHNICAL SPECIFICATIONS

Number of readers:	Up to 1000 per account (2 per door)
RS485 compatible readers:	K1 Mifare DESFire EV1/EV2 (2 per door)
WIEGAND compatible readers:	26-bit, 30-bit, 44-bit and other
ABA TRACK2 compatible readers:	Yes
Compatible keypads:	4-bit, 8-bit
Compatible biometric readers:	BIOSYS, Bioscrypt, L1-Identity 26-bit, 30-bit and 44-bit
Data archiving:	Yes
Input configurations:	Open / Closed / Sabotage / End of line / Doubled
Output relays:	Common, Normally Open, Normally Closed
Required power:	120 Vac / 220 Vac / 50/60 Hz
Backup battery:	1 battery 12 V DC of 4.5 Ah to 28 Ah
Cabinet / Box:	Metal 1.2 mm, Anti-sabotage
ATRIUM network reach RS485:	4000 ft (1220 m) without the need for LDF BIAS resistors
ETHERNET network reach:	Unlimited by router usage / switch
Temperature:	-20°C to +70°C (-4°F to +158°F)
Humidity:	0% to 85% (without condensation)
Memory capacity:	10,000 users
Warranty:	Five-year warranty

Note: The properties described in this document represent the most accurate information at the time of this writing. The data here within, which may change without notice, are supplied as a technical guideline only. The specifications can be confirmed with your local CDVI representative.

This guide of specifications is provided as general information about the ATRIUM system. As manufacturers of access systems, CDVI Americas Limited assumes no liability for errors in the installation defect. The architect, contractor and agent of the owner of the building are required to verify all dimensions, details and design compatibility of conception.

Note : The data here within may change without notice. CDVI Americas Limited is not responsible for errors that may/have occure(d).