**Access Management System (AMS)**

Architect & Engineer Specifications

***NOTES TO POTENTIAL USERS OF THIS DOCUMENT:***

THIS DOCUMENT IS PREPARED AND PROVIDED BY BU SECURITY AS A GENERAL GUIDE TECHNICAL TENDER SPECIFICATIONS FOR THE ACCESS MANAGEMENT SYSTEM AND THE ACCESS MODULAR CONTROLLER (REFERRED THROUGHOUT THIS DOCUMENT AS **ACCESS CONTROL SYSTEM**).

THE INTENT OF THIS DOCUMENT IS TO GUIDE THE SPECIFYING CONSULTANT/ARCHITECT/ENGINEER IN DEVELOPING A TENDER DOCUMENT WITH GENERAL OPERATIONAL & TECHNICAL SPECIFICATIONS.

ALL TEXT IN BLUE IS PROVIDED AS AVAILABLE CONFIGURATION CHOICES THAT MUST BE MADE BY THE AUTHOR OF THE DOCUMENT. SELECT DESIRED OPTION AND DELETE ALTERNATE CHOICES BEFORE ISSUING TO SPECIFIER/CONTRACTOR/SYSTEM INTEGRATOR.

ALL TEXT IN GREEN IS PROVIDED AS SUB-SYSTEM OPTIONS TO THE AUTHOR OF THE SPECIFICATION AND SHOULD BE REMOVED IF NOT REQUIRED BEFORE ISSUING TO THE SPECIFIER/CONTRACTOR/SYSTEM INTEGRATOR.

ALL TEXT IN RED IS PROVIDED TO DENOTE A CRITICAL PIECE OF INFORMATION/REQUIREMENT OR INSTRUCTIONS FOR DOCUMENT USER; THEY CAN HAVE A SIGNIFICANT IMPACT ON SYSTEM CONFIGURATION AND PRICING. OWNER MAY EDIT, CHANGE THE REQUIRMENTS OR DECIDE TO REMOVE IT

WE RECOMMEND THAT SPECIFYING CONSULTANT/ARCHITECT/ENGINEER VERIFY WITH BOSCH LOCAL REPRESENTATIVE THAT YOU HAVE THE MOST CURRENT VERSION OF THIS DOCUMENT.

THIS COPY OF THE ACCESS MANAGEMENT SYSTEM SPECIFICATION WAS ISSUED/UPDATED:

June 2020

IF YOU HAVE QUESTIONS DURING THE USE OF THIS DOCUMENT OR IF SUPPORT IS REQUIRED FOR EDITING THIS DOCUMENT FOR A SPECIFIC PROJECT, PLEASE DO NOT HESITATE TO CONTACT YOUR LOCAL BOSCH SECURITY SYSTEMS REPRESENTATIVE.

# TABLE OF CONTENTS

[TABLE OF CONTENTS 3](#_Toc67302392)

[ABBREVIATIONS 4](#_Toc67302393)

[Access Control System 5](#_Toc67302394)

[Overview 5](#_Toc67302395)

[SCOPE OF WORKS 7](#_Toc67302396)

[Access Control System REQUIREMENTS 9](#_Toc67302397)

[General 9](#_Toc67302398)

[Access Control System Server Structure and System Architecture 11](#_Toc67302399)

[Access Control System Applications Software 13](#_Toc67302400)

[Map Viewer 19](#_Toc67302401)

[Graphical User Interface 23](#_Toc67302402)

[Swipe Ticker 23](#_Toc67302403)

[Access Control System Alarm Handling and Management 24](#_Toc67302404)

[Threat Level Management 25](#_Toc67302405)

[Access Control System Reporting 25](#_Toc67302406)

[Video Integration 25](#_Toc67302407)

[Intrusion Integration 26](#_Toc67302408)

[Mobile Access Integration 26](#_Toc67302409)

[Access Control Hardware 27](#_Toc67302410)

[Specifications for Proximity Card Reader 30](#_Toc67302411)

[Specifications for Contactless Smart Card Reader 31](#_Toc67302412)

[Specifications for Proximity Card 31](#_Toc67302413)

[Specifications for Contactless Smart Card 31](#_Toc67302414)

[Specifications for Finger-print (FP) Biometric Reader & Operations 32](#_Toc67302415)

[4. Change History 34](#_Toc67302416)

# ABBREVIATIONS

ACS Access Control System

AMS Access Management System

IDS Intrusion Detection System

LAC Local Access Controller

MAC Master Access Controller

ROLS Remote Online Locking System

VMS Video Management System

OS Operating System

AS Application Software

GUI Graphical User Interface

LAN Local Area Network

TCP/IP Transmission Control Protocol / Internet Protocol

LDAP Lightweight Directory Access Protocol

CF Compact Flash

FP Fingerprint

# Access Control System

## Overview

* 1. The intent of this document is to outline the minimum requirements for the design, supply, delivery, installation, testing, commissioning and maintenance of the proposed Access Control System
  2. The specifier shall provide the owner with detailed information of the system design architecture to demonstrate that the offered system hardware and software is designed for a truly centralized and integrated environment.
  3. The proposed Access Control System shall offer a highly efficient and automated solution that allows operators to quickly identify an alarm scenario.
  4. The proposed overall system design and operation shall be user friendly and only require minimum training to allow an operator to perform his daily routine with minimum supervision required.
  5. All proposed security field devices installation shall not only to operate functionally, they have also to blend with the interior design of the building. Installer shall liaise directly with the architect and/or interior designer to ensure such requirements are harmonized.
  6. The following sections shall provide a general overview of the operation for each of the systems.
  7. All interfaces within the Access Control System shall be based on TCP/IP network protocol connectivity over the corporate intranet / LAN.
  8. The specifier shall ensure that the Access Control System must be expandable in the following areas:
     1. The system shall be designed to allow foreseeable organizational changes and procedural changes beyond current plans,
     2. Additional hardware units shall easily be added without any modification to the existing hardware, software and network configuration,
     3. All systems shall provide at least **10**% spare capacity for future expansion.
  9. The Access Control System shall be a multi-tasking and multi-users based head end, running on a distributed TCP/IP network.
  10. The system shall be designed to provide alarm gathering, monitoring, handling, reporting, full logging including the performance and activities of the operators within the secured areas of the building. It shall also provide monitoring and control of inputs and outputs both locally and remotely (e.g. in different Buildings).
  11. The system shall be a flexible and user-friendly workstation providing user(s) with a Graphical User Interfaces (GUIs) for alarm monitoring and control of entrances and areas. Such GUIs shall be the core of the entire Access Control System that includes map viewer with alarm list, a swipe ticker for visual door monitoring and command and control of a connected intrusion detection system (IDS).
  12. The system shall be provided to control access into designated security controlled doors only by personnel with a valid access card or Identification-PIN and within valid time schedule. All access cards shall be authenticated against the central and/or local database before granting access.
  13. The system shall support credential enrollment via field readers connected to the LAC or via USB readers.
  14. Up to five cards can be assigned to a person.
  15. Instead of a card a person can use an identification PIN or a biometric credential to request access.
  16. The first card of each person can also be used for the Remote Online Locking System (ROLS).
  17. All designated security controlled doors shall be fitted with a suitable card and/or biometric reader and/or PIN pad.
  18. The included Remote Online Locking System (ROLS) requires special terminals on each remote door.
  19. All door access activities shall be logged in the central database. Any unauthorized attempt or invalid card used shall be reported to the Access Control System, including doors held or forced open.
  20. The system shall also include a feature to display the last access requests from an specified entrance with last name, first name, database picture, timestamp and event type (authorized, card is unknown, card is blocked, etc.)
  21. Reports shall always be readily available and owner shall be able to request for the reports on exactly what information from the report is required.

## SCOPE OF WORKS

* 1. The scope of work for this sub-contract shall include design, procurement, installation and associated services for a fully operational Access Control System as per manufacturer’s guidelines, codes described within this document, that provide central security management, integrated control and remote monitoring of the intended site, including the interfacing of all existing facilities.
  2. All necessary tools, equipment, hardware, software and software user licenses required as describe in this document for the complete installation of the Access Control System shall be supplied and installed under this sub-contract.
  3. All equipment necessary for the Gigabit Ethernet LAN networking installation such as, domain/application servers, PC workstations, fiber optic interfaces, routers, switches, hub, modem, fiber and copper patch cords and the like shall be supplied and installed by the successful specifier under this sub-contract.
  4. All equipment supplied by the successful specifier shall be installed, configured, programmed, tested and commissioned, as specified herein and shown on the sub-contract drawings and the equipment schedules. The Specifier shall supply all materials and services necessary for or incidental to the installation and commissioning of the systems.
  5. The entire Access Control System including all its hardware, peripherals, software and software licenses as specified within this document shall be supplied and provided as part of this sub-contract.
  6. All equipment within the Access Control System shall continue to operate for at least 2 hours in the event of main AC power failure. The specifier shall take in consideration the traffic loads and power consumption at each point of installation when determining the size of the Uninterrupted Power Supply (UPS) as backup power. Provision of the UPS shall be under the scope of this sub-contract.
  7. The extend of the sub-contract works shall include cabling necessary to interconnect the various security systems central equipment, hardware and devices and the like for it to provide the performance as specified in this sub-contract document.
  8. All cable enclosures including conduits, cable trays, ducts, wall boxes, termination panels and the like that are required to facilitate and complete the installation shall be supplied and installed as part of this sub-contract.
  9. The successful specifier shall liaise directly with the owner, main contractor; architect; civil engineer, interior designer; and other sub-contractors at site in coordination of the installation work.
  10. All installations carried out by the successful specifier shall conform to the national standards and code of practices.
  11. The successful specifier shall cooperate and work closely with the appointed site safety officer to ensure safe working environment at all times.
  12. The Specifier shall upon completion of the installation provide complete training with documentations on the configuration, operation and maintenance of the systems to the required operators assigned by the owner. At least two (2) training sessions covering system operations shall be planned and provided to operators and two (2) sessions covering system administration and management for system administrators.
  13. The Specifier shall supply all training materials, operational manuals, as-built drawings, diagram, negatives, printed materials, magnetic and optical storage disk as specific in the sub contract document.
  14. All equipment, systems and materials furnished and installed in this sub contract shall be in accordance with the applicable National and Local standards.
  15. All components, parts, and assemblies supplied and installed by the Specifier shall be warranted against defects in material and workmanship for a period of at least 24 months which include parts and labor.

### Access Control System REQUIREMENTS

### General

1. The Access Control System shall be of open-architecture, PC-based system based on latest and most secure Windows Operating Systems, such as Windows 10 and Windows Server 2016
2. The Access Control System shall comply with all locally binding legal regulations regarding physical and data security-
3. The main function of the Access Control System shall be to control and monitor all designated access to the selected doors, areas or buildings.
4. The Access Control System shall provide and require a single security license key for system operation. Without or removing of such key shall disable the operation of the system upon detection.
5. The Access Control System shall be of modular design providing the flexibility to allow the user to add or remove any components and/or controlled functions or in the event when operating requirements change or as system expands.
6. The Access Control System provided shall contain all the features and requirements specified, but not limited to, in this document. The specifier shall highlight and update the owner of any new or special functionality that are useful and relevant to the user’s application but not found in any part of this document.
7. The Access Control System shall provide the functions and specifications described in this document. In particular, the proposed access controller shall be equipped with all common interfaces such as Ethernet and RS-485 for connection to the Access Control System.
8. The Access Control System shall allow control of door entry access both by a proximity card reader and from the Access Control System workstation.
9. The proximity card readers shall also provide a keypad for authorization by Card and/or PIN.
10. The Access Control System shall support up to eight (8) different Wiegand card formats simultaneously. The number of formats supported shall be unlimited.
11. A locally mounted door REX (request for exit) button shall be provided for purpose of exiting at selected doors, as defined by the owner or as indicated on the drawings.
12. For highly secure areas as further specified or indicated on the drawings, exit card readers shall be provided to allow monitoring of persons leaving and entering the controlled area.
13. All access doors shall have an emergency break-glass door release installed to unlock the door for exit in the event of emergency. In addition, all dedicated doors along the escape route shall be opened automatically during fire alarms.
14. The Access Control System shall also provide control of elevators and vehicle boom-barriers.
15. The specifier shall supply, install and configure the Access Control System management software.
16. The Access Control System shall monitor and record in a logbook all access events at each control point.
17. The Access Control System shall provide configuration and programming of access groups, where each access group contains a list of control points or access doors for which a card holder has authorization.
18. The Access Control System shall provide configurable time zones to govern periods of restricted and unrestricted access. These time zones can restrict access to different access groups.
19. The time zones shall be subject to a configurable calendar that tracks public holidays and user-definable special holidays. All time zones shall be definable by day, hours and minutes.
20. The Access Control System shall be designed such that local failures do not entail the failure of the whole system. Local access controllers shall continue to operate even if the network connection to the management software fails.
21. The Access Control System management software shall allow card personalization. That is, it shall include a tool for designing badges that supports the importing of bitmaps, text and database fields, such as name or badge number for creating of corporate badge designs printable on a standard card printer that come with a Windows compliant printer driver.
22. The Specifier shall ensure that the system must be expandable and by adding new component to the existing system will not affect its normal operation.

### Access Control System Server Structure and System Architecture

1. The Access Control System server shall be provided and structured based on centralized server architecture.
2. The CPU provided for the Access Control System server shall be reliable and robust in construction to perform all the necessary functions as described in this document relative to the management of all sub-systems.
3. The CPU shall be micro-processor based, completed with adequate storage to service the total system requirements and shall be of an industrial standard type, having proven record in similar applications.
4. Database for Access Control System shall reside within the same server hardware or on a separate server hardware.
5. The Access Control System can be shared with up to 400 tenants (divisions). Every tenant has access to only his own data.
6. All alarms processing, logging, operator’s response, data entry/input, graphical user interface and other system operations and management functions shall be performed at the Access Control System workstations connected to the Access Control System network. The operating system shall be a current version of Windows 10 or Windows Server 2016.
7. All Access Control System servers and workstations shall be connected using a standard IP network over the corporate Intranet or dedicated LAN/WAN.
8. Access Control System hardware requirements:
   * + Standard Windows PC for both server and client
     + Intel i5 or higher (server with min. 4 cores)
     + Min. 8 GB RAM (recommended 16 GB for client, 32 GB for server)
     + Server: 200 GB free disk space (SSD recommended)
     + Client: 20 GB free disk space
     + 1 Gbit/s Ethernet card for server and client
     + Graphical adapter with 256 MB RAM and 32k colors
     + Resolution of 1920 x 1080
     + Free USB port or network share for installation files
     + USB Keyboard and Mouse
9. The Access Control System shall have a multi-level priority interrupt structure proven in multi-tasking and multi-client real time applications. Simultaneous alarms/events monitoring by multiple users, system supervision and history archiving shall be possible without degradation of any functionality specified for system or operation.
10. The Access Control System shall allow the configuration of different operator profiles with varying levels of permission for managing personnel data, for instance:
    * + read only
      + read, write, change, and delete
      + change the current location of persons
      + change the access authorizations of persons
11. The Access Control System shall allow the configuration of different operator profiles with varying levels of permission for managing event data, for instance:
    * + view own messages
      + view all messages without personal data
      + view all messages
12. The Access Control System shall allow the configuration of different operator profiles with varying levels of permission for managing the configuration dialogs.
13. The Access Control System shall allow the configuration of different operator profiles with varying levels of permission for managing doors and entrances.
14. The Access Control System server shall act as the source that provides time synchronization across all sub-systems.
15. The Access Control System shall be designed such that failure of any sub-system shall not affect all the other sub-systems. This shall also apply to any loss of power or network communications. In any case, each sub-system shall remain fully operational.
16. The Access Control System shall have a modular structure that allow for future system expansion with minimum cost and disruption to the existing operational system.
17. The Access Control System shall be expandable to support a limited number of 80 concurrently operating workstations.

### Access Control System Applications Software

1. The Access Control System Applications Software (AS) proposed shall be proven to be robust and reliable prior to being supplied, installed, tested and commissioned. It shall be user friendly and provide prompting to assist operators who are not familiar with the system.
2. The Access Control System AS proposed shall provide English descriptions and messages using both text based menus and graphical icon displays. Other languages shall also be supported in the standard version. These are German, French, Dutch, Hungarian, Polish, Russian, Spanish, Portuguese (BR), Turkish, Arabic, Simplified Chinese (CN), Traditional Chinese (TW).
3. The Access Control System AS shall be capable to support to the following:

* Number of active cardholders – 200,000
* Number of readers – 10,000
* Number of access groups – 255
* Number of time schedules – 255
* 4 – 8 digits programmable (Personal Identification Number) PIN codes
* Remote Online Locks – 1,000
* Map viewer floor plans – 1,000

1. The software shall also allow the programming of individual operator’s permissions.

* Permission regarding personal data shall be configurable to the following:
  + read only
  + read, write, change and delete
  + change the current location of persons
  + change the access authorizations of persons
* Permission regarding event log messages shall be configurable to the following:
  + view own messages
  + view all messages without personal data
  + view all messages
* Special permission for the configuration dialog.
* Special permission for door management.

1. The Access Control System AS shall provide a simple way for the system administrator to configure entrances selecting from a list of pre-defined door models. The following list of door models shall be provided by the system:

* Door with entry and exit reader
* Door with entry reader and request to exit button
* Door with entry or exit reader
* Door with time & attendance readers
* Door with reversible turnstile for entrance or exit
* Parking Lot for entrance or exit
* Elevator with floor control
* Vehicle boom barrier and rolling gate
* Mantrap
* Door with IDS arming/disarming
* Independent output signals

1. Selecting a pre-defined door model shall automatically assign the corresponding reader.
2. Cardholder Enrollment:

* The Access Control System AS shall provide an easy way of entering cardholders into the database. In addition to basic data, such as first name, last name, badge number and access authorizations, the following information shall be possible, but not limited to:
* 3 PIN codes (IDS, Access, Identification)
* Validity period
* Membership
* Status fields, such as employee, visitor, guard
* Address fields
* Personal data
* Individual fields can be added, deleted or edited by administrator
* Individual fields can be edited to different data types like text, number, date, time, check-box and combo-box
* Individual text fields can contain up to 2000 characters
* Individual fields can be tagged as “unique” and “required”
* Individual fields can have editable labels with up to 20 characters

Enrollment of electronic credentials like cards, tags and fobs shall be possible through an access control reader connected to the LAC.

Enrollment of biometric templates (like from fingerprints and palm vein images) shall be fully integrated into Access Control System without the need of third party software.

1. Cardholder Images:

* It shall be a standard feature provided in the Access Control System management software for taking photos, scanning or importing cardholder images into the cardholder database. Such that stored cardholder’s image can be displayed automatically on the Access Control System workstation during access monitoring or for video verification purposes.

1. Import and Export of Cardholder Master Records

* The Access Control System AS shall provide a web based import and export interface to import cardholder master records from a separate database during installation, or to export the master records for further use by another application.
* The interface shall support at least commonly used comma-separated and fixed-field-length file formats for easy adaptation by applications when import or export.
* The interface shall support LDAP for importing cardholder data from Microsoft Active Directory servers

1. Cards
   * A person can have up to five cards at a time. Every card has the same access authorizations and limits (validity limitations, locks, etc.).
   * An identification PIN can be configured for use instead of a card.
2. Area-Time Authorizations:

* The Access Control System shall allow the linking of access authorizations with time models. The assigned time models govern the periods where an access authorization is active at an entrance or entrance group.

1. Time Models, Day Models, and Special Days:

* The Access Control System AS provided shall allow for the creation of time models for any specific day within the day models. Configuration for Special days, such as local public holidays, shall also be supported. Time models provide a simple way of defining periodically recurring day models. The time model can activate and deactivate access authorizations at entrances and entrance groups.

1. Defining Areas of control:

* The Access Control System shall provide the ability to define and manage arbitrary logical areas within the premises. These could be single rooms, groups of rooms, entire floors or parking areas.

1. Access Sequence checking:

* There shall be an access sequence check provided, allowing authorized cardholders to enter an area only when they have swiped their card at the neighboring area.

1. Dual or Multiple Authorized Access:

* The Access Control System AS shall provide the possibility to permit access only when two or more authorized cardholders present their badges consecutively at the card reader.

1. PIN Codes:

* The Access Control System AS shall support the input of three kinds of PIN codes for each cardholder. The length of the PIN code (4 to 8 digits) is defined once in the system. The definition of validity periods for the PINs must be supported.
* Verification PIN – This will be requested after presentation of card at an entrance, as an additional security measure.
* Identification PIN - This Identification-PIN can be typed at keyboard readers instead of presenting a card. As this PIN functions virtually as a card number it also carries with it all authorizations assigned to that card number.
* Arming PIN - to arm the alarm system.
* A fourth variety of PIN, the Door-PIN, can be assigned separately to individual doors. This code must be known to anyone using the door.

1. Duress Code Alarm:

* A duress code alarm message shall be generated at the Access Control System and display on the monitoring workstation if a cardholder enters their PIN in reverse order, or in some other predefined way.

1. Blocking Cardholders:

* The Access Control System AS shall allow the blocking of cardholders, for example after a defined validity period.

1. Visitor Management:

* Visitor Management shall be web-based and compatible to modern browsers, minimum: Microsoft Edge (Chromium based), Google Chrome, Mozilla Firefox
* Different views for reception desk, host and visitor self-registration (“kiosk mode”) shall be available
* Document scanners and signature scanners shall be supported to digitally collect personal information and signatures
* Visitor registration page shall be fully customizable to meet local data privacy regulations
* Administration of visitors shall be provided by the Access Control System management software in the same database.
* Pre-registration of visitors shall be possible by the host or by receptionist
* A visitor dashboard is available with most needed information on one screen: expected visits today, number of visitors on premise, credentials in use, credentials still to be collected
* Expiration dates for visitor profiles and their attachments to meet local data privacy regulations
* The following information shall be assignable to a visitor:
* Identification number
* Access authorizations
* credential

3.3.21 Car Park Management:

* Display vehicle count and available space per zone in carparks
* Available space can be managed flexibly; multiple spaces can be assigned for trucks and larger vehicles
* Space can be given to external persons via vouchers for multiple entries

3.3.22 Guard Tour Management and Patrols:

* Up to 200 guard tours can be planed and scheduled in advance
* Up to 8 simultaneous patrols can be monitored and tracked

3.3.23 Route Enforcement

* A Route (or Tour) is a predefined sequence of readers that can be prescribed for persons to direct their movements within the premises, regardless of the person’s authorizations.
* Typical uses are to enforce strict access sequences in industrial clean environments, hygienically controlled, or high-security areas.
  + 1. Random Screening of cardholders (process)
  1. A cardholder presents their card at a reader configured for random screening.
  2. If the randomizer selects this cardholder for extra security checks. The person is blocked (prevented from using credentials) throughout the whole system, until the block is manually removed.
     + The event is recorded in the system event log.
     + The Blocking dialog receives an entry of unlimited duration marked Random screening.
     + The status bar of the personnel data dialogs indicates the current status of the cardholder within the system.

3. The randomly selected person is diverted to a separate booth for additional security checks.

4. After carrying out these checks the security guard resets the block in the access control software.

5. The randomly screened person can now use their card again at all readers for which they are authorized.

### Map Viewer

* + 1. The system shall contain a map viewer. This map viewer shall provide a graphical presentation of the premises by means of floor plans, pictures or any desired graphical representation.
    2. Map Viewer shall have two basic modes: one for viewing and one for editing

1. The map structure is shown in a map tree at the left side of the active map. The tree allows jumping multiple layers by selecting the target map in the tree directly.
2. The map viewer shall have navigation buttons, a refresh button and a home button.
3. On the maps entrances and devices like MAC, AMC, readers and digital input/outputs can be positioned as a dynamic icons. These graphical icons will display the location of the device in the map and the actual status of the device. Every icon can be displayed in several sizes, angle and color and background color. Clicking any of the devices automatically shows the commands available for controlling the respective device. Control commands are automatically linked based on device type.
4. An operator can be assigned one or multiple authorizations for parts of the map viewer, such as door commands, reader commands, controller commands, system commands, special door commands, digital output commands, alarm list commands, swipe ticker commands.
5. Map view operators can only edit and view the scenes of the Divisions for which they are authorized.
6. Depending on their authorization, operators can cold start or warm start master controllers (MAC) or local controllers (AMC), enable and disable different access modes, grant access, block or unblock doors and readers, set and clear digital outputs.
7. An application menu shall offer icons to show a device tree, an area overview or an alarm list.
8. The device tree shall be able to show server, MAC, AMC, entrances, readers, turnstiles, assembly points (muster points), parking areas, boom barriers, elevators, remote online locks and digital inputs and outputs.
9. An area overview shall be able to show name, type (e.g. parking), current count, maximum count and state (e.g. empty, full).
10. The alarm list shall coordinate multiple operators working concurrently, ensuring for instance that the handling of an alarm is reserved for the operator who first accepts it.
11. In case of alarms, the map will automatically focus on the alarm location. The device that triggered the alarm will show alarm status on the map, and play a sound that can be configured for individual event groups.
12. The alarm shall appear in the alarm list dialog as an alarm event. Alarm events in the alarm list require an acknowledgement by the operator before they can be handled (including deletion).
    * 1. Remote Online Locking System (ROLS)
    * The Access Control System allows the integration of wireless connected ROLS devices.
    * The personnel data will be managed by the online Access Control System.
    * Persons can use the cards they have for the Online System
    * There are special access authorizations regarding to the ROLS.
    * There are special time models regarding to the ROLS.
    * There are separate validation limits regarding to the ROLS.
      1. Man Trap:

* A mantrap function shall be provided to allow management of two or more interlocking doors controlled by two pairs or more of readers (in/out), or entrance readers and request to exit buttons. Only one door can open at a time. As long as one door is opened, the other shall be remain closed.
  + 1. Elevator Control:
* The Access Control System AS shall allow the definition of floor access authorizations at designated lift, and assign them to card holders. If a cardholder presents his card at the elevator reader, the system shall activate the elevator floor buttons the cardholder has authorized access.
  + 1. Random Screening:
* The Access Control System AS shall be able to perform an additional security check by the officer on duty at the site/building exits. The readers at such exits are easily set to that mode by checking a checkbox and setting the frequency. At Random, the selected door should not opened, but an event shall be triggered at the Access Control System monitoring workstation. Upon receiving the message, shall remind the operator/guard to check the cardholder and his pockets/bags. After which, he can decide to open the door manually by clicking on the door icon inside the location map, release the card reading with a special configured reader, or delete the locking via dialog
  + 1. Time and Attendance Data:
* Access control readers shall be allowed to be configured additional as time and attendance readers. The booking events are stored in a separate file to export them for use in other applications.
  + 1. Access Control Management Alarms and Events

The Access Control System AS shall provide a wide range of standard events. The following events, but not limited to, shall be supported:

* Card unknown
* Card not authorized
* Card outside time profile
* Card anti-passback
* Access timeout
* Door open time exceeded
* Door opened unauthorized
* Door blocked
* Tamper alarm controller
* Tamper alarm reader
* PIN code error
* Duress alarm code
* Access denied
* Wrong card version
* Card blocked
* Card blacklisted
* Card out route
* Guard tour alarms
* Random screening
* Other individual alarm extensions like intrusion alarms and video alarms (e.g. motion)
  + 1. All events are pre-configured in 4 alarm groups “hold-up”, “alarm”, “warning”, “maintenance”, but can be re-configured quickly.
    2. All alarm/events have to be logged in the central Access Control System event log files together with all assigned alarm documents for a complete reporting.
    3. The Access Control System AS provided shall have support for central alarm monitoring and management. It shall provide a graphical user interface (GUI).
    4. The Access Control System AS shall provide practicable the central configuration platform or tool from where everything concerning system behavior, such as access control cardholder settings, display features, and authorizations are set up.
    5. The Access Control System AS shall securely log all events, alarm activations and operator’s actions/responses into the alarm/event log files, so to prevent after-the-fact changes, and to protect data from any manipulation.
    6. The events log files shall include an advanced filter functions such that archive can be kept small and precise. If required, only desired information shall be archived.
    7. A device tree and the device names shall be provided for in the GUI.
    8. The Access Control System AS shall support any standard laser or inkjet printer that comes with a Windows-compliant printer driver for use as an alarm printer.

### Graphical User Interface

* + 1. The Access Control System GUI shall support single or multi-screen displays having multiple dialogs separately over a maximum of two (2) monitors per workstation by using a corresponding video graphics card.
    2. The Access Control System shall provide a default GUI that is adequate and ready for used in normal system operation. It shall support at least the following standard resolution 1280x1024 for 1-monitor operation).
    3. The Access Control System GUI shall enable operators to find a specific detector, door, or reader for fast control, such as open door manually, show camera live image, and so on.
    4. In the event of alarm activation, the alarm message shall be displayed at the destined Access Control System operator workstation together with a configurable sound via PC internal speaker.
    5. For the alarm sound generated from the PC internal speaker, a standard format such as WAV shall be supported and selectable for assigning to individual event groups of events during system configuration.

### Swipe Ticker

* + 1. An application can be configured within the Map view that displays the last 10 minutes of access events in a dynamic scrolling list. The number of events can be limited (e.g. 50) and events older than 10 minutes are automatically dropped from the list. The operator can monitor all readers in the system, or select a subset. The operator can easily pause and resume the display.
    2. Each record in the list contains details of the event and the credential used, for example:
* The name of the cardholder and their stored photo, for visual confirmation of identity.
* A time stamp.
* Company and/or department name
* The entrance and the reader at which the credential was used
* An event category with a colored label, for example:
  + Green: A completed access with a valid credential
  + Yellow: An incomplete access with a valid credential, for example, the cardholder cycled the lock but did not open the door
  + Red: A failed attempt to access with an invalid credential. The type of invalidity is shown, for example, the credential is blacklisted, unknown or expired

### Access Control System Alarm Handling and Management

1. The Access Control System shall provide the operator a simple and efficient way to handle any incoming alarms.
2. Only authorized operator with the valid login username and password shall be able to access and operate the system. Once successfully login, the operator shall only see all the alarm and event messages destined to him for monitoring and processing based on his user login access profile.
3. The operator shall be able at the Access Control System workstation acknowledge/accept, response to incoming alarm or event messages. The location of the alarm shall be displayed by animation on a graphical representation of the premises.
4. All incoming alarms at the Access Control System GUI workstation shall contain a comprehensive alarm message.
5. The incoming alarm or event message shall provide, but not limited to, the following information:

* Alarm date and time
* Alarm status
* Alarm location

1. The operator shall be able to silence the audible alarm sound or buzzer, while he is busy processing earlier alarms.
2. The operator shall be allowed to switch between all alarms or events messages.
3. The Access Control System operator shall also be able to send remote commands or activate controls manually from the workstation when requested such as, unlocking and re-locking of access controlled door/s, or resetting of detectors.
4. The operator shall be allowed based on his login access profile generate alarm and event reports from his operating workstation.

### Threat Level Management

* + 1. At least 15 different threat levels can be pre-configured for instant activation in case of emergency.
    2. A threat level is activated by a threat alert. A threat alert can be triggered in one of the following ways:
* By a command in the software user interface
* By an input signal defined on a local access controller, for instance from a push button or a fire panel.
* By swiping an Alert card at a reader

Threat alerts can be cancelled by the UI command or hardware signal, but not by alert card.

### Access Control System Reporting

* + 1. A minimum of 15 predefined reports are available for master data, authorizations and system data.

### Video Integration

* + 1. Access Control System can be integrated with minimum 2 different video management systems, e.g. Bosch VMS and Milestone XProtect to achieve as minimum the following functions:
       - 1. Live Video Verification

A person with valid card is displayed with database picture and camera live stream on the video management system, so the operator can decide after image comparison whether to grant or deny access.

* + - * 1. Forensic Person Tracking

A person can be searched in a database for all entrance actions so that the recorded videos of this person are shown quickly. A door can be searched for all persons getting through the entrance for quick video investigation.

* + - * 1. Generic command & control for video management systems  
           A connected video management system (e.g. Bosch VMS or Milestone XProtect) can trigger door commands (block, normal, permanent open), reader commands (grant access) and digital outputs (open, close).   
           Access Control System can send reader events (access denied, access granted, access requested, person did not enter, authorized but selected for random screening), door events (unauthorized open, door opened too long), door contact states (opened, closed), door states (unlocked, locked, secured), duress events and digital IO events (closed, opened) for further processing to the video management system.

### Intrusion Integration

* 1. Access Control System can be integrated with intrusion control panels:
     + - 1. For User Management

Up to 50 panels are supported for central user management. Up to 2000 panel users can be managed centrally in the access control system. Users can be assigned name, user group, passcode, access card, key fob (up to 1000), language, authorization profile and level.

* + - * 1. For Command & Control

Intrusion areas can be drawn as polygons on the map viewer. Intrusion areas show the current states (unarmed, ready to arm, armed, alarm) on the map viewer and in a table view.

Intrusion areas can be armed (if ready to arm) and disarmed (if armed).

Intrusion alarms can be clearly seen per area and per detector on the map and in the alarm list.

Up to 25 alarm panels with up to 599 points and 32 areas each are supported for central command & control.

Up to 600 intrusion events per second are supported and up to 300 alarms per second can be processed.

### Mobile Access Integration

* 1. Access Control System can be integrated with at least 2 different system for mobile access control

Access authorizations are assigned to mobile credentials similar to physical credentials, e.g. cards. Credentials can be read on reads via NFC (Near Field Communication) or BLE (Bluetooth Low Energy)

### Access Control Hardware

1. The Access Control Hardware provided shall conform, but not limited to the following requirements and directives:

* CE
* EN 50130-4:1995
* EN 61000-3-2
* EN 61000-4-2
* EN 61000-4-4
* EN 61000-4-6
* EN 55022:1998
* EN 60950:2000
* EN 61000-3-3
* EN 61000-4-3
* EN 61000-4-5
* EN 61000-4-11
* EN 50131-1
* IEC/EN 60839-11
* C-Tick

1. The Access Control Hardware provided shall be of modular design with a download software built-in so that the application program can be easily changed and downloaded without the physically touching the controller itself.
2. The Access Control Hardware design shall be of standard 19” rack mountable and also rail mountable for installation in a weather-proofed enclosure suitable for used in outdoor.
3. The connection from the Access Control Hardware to the Access Control System server running the management software shall preferably by Ethernet 100BaseT or RS-485.
4. The Access Control Hardware shall have a 16-characters liquid crystal display (LCD), and a button provided for selecting the display to show all its network parameters and actual status like:

* IP address of the controller
* MAC address of the controller
* DHCP on/off
* Status of all the inputs connected to it
* Status of all the outputs connected to it
* Online and Offline status of the controller
* Firmware version
* Date and Time:   
  A real time clock (RTC) that will adjust itself to leap year computations automatically.

1. The Access Control Hardware shall support and include a standard Compact flash (CF) memory card for storing cardholder data and access events. The CF memory card must be formatted with a standard FAT file system, to allow reading them using a standard card reader connected to a computer, if the Access Control Hardware fails.
2. The Access Control Hardware memory shall under no circumstance lose a single transaction, not even the last transaction when power fails.
3. The Access Control Hardware and all devices connected to it shall continue to operate and control access in off-line mode, even if the computer network fails.
4. The Access Control Hardware memory shall store database that has a capacity with a minimum of 200,000 cardholders, each having a programmable 4 – 8 digits (Personal Identification Number) PIN codes
5. The cardholder database shall be upgradeable by exchanging the CF card. The system shall automatically detect the size of the CF-card.
6. The Access Control Hardware provided shall support the connectivity of up to maximum of 4 standard Wiegand interface readers or 8 serial interface readers operating on RS485 bus technology.
7. The Access Control Hardware provided shall support multiple card formats:
8. The Access Control Hardware shall provide minimum eight programmable I/Os on board, and shall be expandable to 32 each, using I/O extensions.
9. All inputs provided shall be configurable to provide 2- or 4- status selectable, via End-Of-Line (EOL) resistors, namely:

* Input Closed
* Input Opened
* Input Shorted (provided in 4- status mode)
* Input Tamper (Cable cut, provided in 4- status mode)

1. EOL resistor’s values shall be flexibly selectable in the Access Control System management software during configuration.
2. The Access Control Hardware and all devices connected to it shall continue to operate and control access in off-line mode, if there is a failure with the computer network.
3. The Access Control Hardware shall support standard CF flash memory card for storing cardholder data and access events. The CF memory card must be formatted with a standard FAT file system, to allow reading them using a standard card reader connected to a computer, if the Access Control Hardware fails.
4. The Access Control HardwareFirmware is updateable through the Host System via download
5. The Access Control Hardware memory shall under no circumstance lose a single transaction, not even the last transaction when power fails.
6. UPS shall be provided to continually supply power to the Access Control Hardware and readers for a minimum of 2-hours, in the event of power failure.
7. The Access Control Hardware shall generate a transaction record and save them in its memory for every alarm, they include –

* Time/date of occurrence and restoration
* Location of alarm sensors

### Specifications for Proximity Card Reader

1. The proximity card reader provided shall be of ruggedized design, sealed in weatherized polycarbonate enclosure to withstand harsh environments for both indoor/outdoor used and provide a high degree of vandal resistance.
2. Power requirement: 10 – 16Vdc.
3. Transmit frequency: 125 kHz
4. The proximity card readers shall have a read range of at least 3”.
5. The response time to unlock the door after a card is presented to the card reader shall not exceed 1.0 second +/- 0.5 second.
6. The card reader unit shall have an integral keypad with beeper, multi-color LEDs.
7. The keypad shall have back-light to allow easy viewing, in case of power blackout. It shall lights automatically upon pressing any key or when a card is presented to the reader.
8. The overall thickness of the card reader unit shall not exceed 30 mm.

### Specifications for Contactless Smart Card Reader

* + 1. The Smart card reader provided shall be of ruggedized design, sealed in weatherized polycarbonate enclosure to withstand harsh environments for both indoor/outdoor used and provide a high degree of vandal resistance.
    2. The smart card reader shall be based on contactless smart card 13.56MHz technology for connection to the Access Control Hardware with Wiegand interface.
    3. The contactless smart card reader provided shall be capable of reading MIFARE serial number in 32-bit format in accordance with ISO standard 14443A.
    4. The data transfer between the contactless smart card reader and smart card shall be encrypted.
    5. Power requirement: 10 – 16Vdc.
    6. The contactless smart card readers shall have a read range of at least 2.4”.
    7. The response time to unlock the door after a card is presented to the card reader shall not exceed 1.0 second +/- 0.5 second.
    8. The card reader unit shall have an integral keypad with beeper, multi-color LEDs.
    9. The keypad shall have back-light to allow easy viewing, in case of power blackout. It shall lights automatically upon pressing any key or when a card is presented to the reader.
    10. The overall thickness of the card reader unit shall not exceed 30 mm.

### Specifications for Proximity Card

* + 1. The proximity cards shall be similar in size and thickness to standard credit cards or bank ATM cards.
    2. The proximity cards shall operate on 125 kHz.
    3. The cards shall have CE/UL Approvals

### Specifications for Contactless Smart Card

1. The offered contactless smart cards shall be similar in size and thickness as standard credit cards or bank ATM cards.
2. The offered smart cards shall be of contactless technology operating on 13.56 MHz and shall be compliance to ISO standard 14443A.
3. CE/UL Approvals are required.

### Specifications for Finger-print (FP) Biometric Reader & Operations

1. The Finger-print (FP) biometric reader provided shall be of ruggedized design, having weatherized polycarbonate enclosure or similar protection to withstand harsh environments for both indoor/outdoor used and provides a high degree of vandal resistance.
2. The FP biometric reader shall provide two-factor authentication with the combination of a proximity [/contactless smart] card and a fingerprint biometrics.
3. The FP biometric reader together with the proximity [/contactless smart] card shall support operation with 1:1 verification mode or 1:N, identification mode.
4. The FP biometric reader shall continue to operate to control access in off-line mode. When the network connection restored, the reader shall automatically upload and synchronize its database with the server.
5. The FP biometric reader shall include a FP scanner that uses capacitive verification techniques for the live finger recognition and resistance of the human skin.
6. The FP biometric reader provided shall have a read tolerance of at least +/-30 degree and a displacement of about +/- 5mm from the FP scanner.
7. The same FP biometric reader provided shall be able to be used for both access control and as an enrollment station.
8. The specifier shall supply and install the necessary software to manage the FP enrollment for all users and configuration of the FP access control operations. The software provided shall be integrated to the Access Control System for access control and monitoring.
9. During enrollment process, the FP biometric reader and software used for capturing the finger-print shall provide, but not limited to the following:
10. The FP image shall have a minimum size of 256 x 360 pixels
11. Provide full visibility of the ridge details including texture, continuity, edges and pores.
12. Allow for real-time on-screen preview of the FP image while performing the FP capture.
13. FP captured shall have resolution of at least 500dpi.
14. Minutiae file size of at least 256 bytes.
15. The FP enrollment process shall support a percentage estimation of the image quality such that the operator can accept or reject the enrolled FP.
16. Up to a maximum of 10 FP templates shall be allowed to be assigned to a single user.
17. The enrolled FP templates shall be stored in the Access Control System centralized database or in the reader’s memory storage.
18. The FP templates stored shall incorporate a date stamp and shall record the number and/or name of the finger taken.
19. The real FP images captured shall not be stored for highest data privacy.

# Change History

Change history:

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author / Editor** |
| 0.1 | 13-Aug-19 | Initial Version (derived from APE A&E Specs) | H. Maier |
| 0.2 | 13-Sep-19 | Draft for verification | H. Maier |
| 0.3 | 25-Sep-19 | Re-formatting and review | P. Brittain, H. Maier |
| 3.0 | 19-Jun-20 | Update for AMS 3.0 | H. Maier |
| 3.0.1 | 22-Mar-21 | Update for AMS 3.0.1 | H. Maier |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |