Access Professional Edition (Version 3.0)
Architect & Engineer Specifications

NOTES TO POTENTIAL USER OF THIS DOCUMENT:

THIS DOCUMENT IS PREPARED AND PROVIDED BY BU ACCESS AS A GENERAL
GUIDE TECHNICAL TENDER SPECIFICATIONS FOR THE ACCESS PROFESSIONAL
EDITION 3.0 AND THE ACCESS MODULAR CONTROLLER (REFERRED
THROUGHOUT THIS DOCUMENT AS ACCESS CONTROL SYSTEM).

THE INTEND 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 REQUIREMENTS 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 PROFESSIONAL EDITION 3.0 SPECIFICATION WAS
ISSUED/UPDATED:

Apr 2015 VERSION 1.0.0.07

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>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>ABBREVIATIONS</td>
<td>4</td>
</tr>
<tr>
<td>ACCESS CONTROL SYSTEM</td>
<td>5</td>
</tr>
<tr>
<td>1. OVERVIEW</td>
<td>5</td>
</tr>
<tr>
<td>2. SCOPE OF WORKS</td>
<td>7</td>
</tr>
<tr>
<td>3. ACCESS CONTROL SYSTEM REQUIREMENTS</td>
<td>9</td>
</tr>
<tr>
<td>3.1 General</td>
<td>9</td>
</tr>
<tr>
<td>3.2 Access Control System Server Structure and System Architecture</td>
<td>11</td>
</tr>
<tr>
<td>3.3 Access Control System Application Software</td>
<td>14</td>
</tr>
<tr>
<td>3.4 MAPVIEWER</td>
<td>18</td>
</tr>
<tr>
<td>3.5 Graphical User Interface</td>
<td>22</td>
</tr>
<tr>
<td>3.6 Access Control System Alarm Handling and Management</td>
<td>23</td>
</tr>
<tr>
<td>3.7 Access Control Hardware</td>
<td>24</td>
</tr>
<tr>
<td>3.8 Specifications for Proximity Card Reader</td>
<td>27</td>
</tr>
<tr>
<td>3.9 Specifications for Contactless Smart Card Reader</td>
<td>28</td>
</tr>
<tr>
<td>3.10 Specifications for Proximity Card</td>
<td>28</td>
</tr>
<tr>
<td>3.11 Specifications for Contactless Smart Card</td>
<td>28</td>
</tr>
<tr>
<td>3.12 Specifications for Finger-print (FP) Biometric Reader &amp; Operations</td>
<td>29</td>
</tr>
<tr>
<td>4. CHANGE HISTORY</td>
<td>31</td>
</tr>
</tbody>
</table>
ABBREVIATIONs

Access PE  Access Professional Edition
CCTV     CCTV surveillance and Recording System
OLS      Offline Locking System
OS       Operating System
AS       Application Software
GUI      Graphical User Interface
LAN      Local Area Network
WAN      Wide Area Network
TCP/IP   Transmission Control Protocol / Internet Protocol
IE       Internet Explorer (Microsoft)
OLE      Object Linking and Embedding (Microsoft)
OPC      OLE for Process Control
HTML     Hyper Text Mark-up Language
LDAP     Lightweight Directory Access Protocol
CPU      Central Processing Unit
CF       Compact Flash
AMC      Access Modular Controller
FP       Finger-Print
EOL      End Of Line resistor
Access Control System

1. OVERVIEW

1.1 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.

1.2 The specifier shall provide the owner with detailed system design architecture information to demonstrate that the offered system hardware and software is designed for a truly centralized and integrated environment.

1.3 The proposed Access Control System shall offer a highly efficient and automated solution that allows operators to quickly identify an alarm scenario.

1.4 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.

1.5 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.

1.6 The following sections shall provide a general overview of the operation for each of the systems.

1.7 All interfaces within the Access Control System shall be based on TCP/IP network protocol connectivity over the corporate intranet/internet/LAN/WAN.

1.8 The specifier shall ensure that the Access Control System must be expandable in the following areas:

   1.8.1. The system shall be designed to allow foreseeable organizational changes and procedural changes beyond current plans,

   1.8.2. Additional hardware units shall easily be added without any modification to the existing hardware, software and network configuration,

   1.8.3. All systems shall provide at least 10% spare for future expansion and connection.

1.9 The Access Control System shall be a multi-tasking and multi-users based head end running on a distributed TCP/IP network.

1.10 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).

1.11 The system shall be a flexible and user-friendly workstation providing user(s) with a Graphical User Interfaces (GUIs) for alarm monitoring and control. Such GUIs shall be the core of the entire Access Control System that includes
mapviewer with alarm list and a Video Verification module for surveillance and recording video streams.

1.12 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.

1.13 The system shall support credential enrollment via field readers connected to the LAC.

1.14 Up to three cards can be assigned to a person.

1.15 Instead of a card a person can use an Identification-PIN for access request.

1.16 The first card of each person can be used for the Offline Locking System (OLS), too.

1.17 All designated security controlled doors shall be fitted with a suitable card reader and/or pin pad.

1.18 The included Offline Locking System (OLS) requires special terminals on each door of the OLS.

1.19 All door access activities shall be logged into the central database. Any unauthorized attempt or invalid card used shall be reported to the ACCESS CONTROL SYSTEM, including door held and forced opened alarm as priority alarm transactions.

1.20 With the Video Verification module, live images from the camera installed at the door location shall be displayed at Access Control System GUI during door alarm activation and access request. It shall also be possible to select live view of the camera to view the person’s face before activating (manually unlocking the door via icon control on the GUI) and granting during door access request.

1.21 The system shall also include a feature to display the last 5 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.)

1.22 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 with the use of event filters.
2. SCOPE OF WORKS

2.1. 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.

2.2. 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.

2.3. 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.

2.4. 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.

2.7. 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.

2.8. 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.

2.9. 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.

2.10. 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.

2.11. 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.
2.12. All installations carried out by the successful specifier shall conform to the national standards and code of practices.

2.13. The successful specifier shall cooperate and work closely with the appointed site safety officer to ensure safe working environment at all times.

2.14. 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.

2.15. 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.

2.16. All equipments, systems and materials furnished and installed in this sub contract shall be in accordance with the applicable National and Local standards.

2.17. 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 labour.
3. Access Control System REQUIREMENTS

3.1 General

3.1.1 The Access Control System shall be of open-architecture, PC-based system based on Windows Operating Systems, such as Windows XP, Windows 7 (32 and 64 bit, Enterprise), Windows Server 2008 (R2).

3.1.2 The Access Control System shall comply to the strict regulation and adapting state-of-the-art security technologies, the highest level of reliability, and integrate to networking infrastructures such as the Intranet, Internet, LAN/WAN.

3.1.3 The main function of the Access Control System shall be to control and monitor all designated access to the selected doors, areas or buildings.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 The proposed 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 server running the management software.

3.1.8 The Access Control System shall allow control of door entry access both by a proximity card reader and from the Access Control System workstation.

3.1.9 The proximity card reader shall also incorporate a numeric keypad to be used if Card and/or Pin number access configuration is desired.

3.1.10 The Access Control System shall support up to four (4) different Wiegand card formats simultaneously. The number of each format supported shall be unlimited.

3.1.11 A locally mounted door release push button shall be provided for purpose of exiting at selected doors as defined by the owner or as indicated on the drawings.

3.1.12 For highly secured areas as further specified or indicated on the drawings, exit card reader shall be provided to allow an exact tracking of people going in & out the predefined area.
3.1.13 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 automatically open during fire alarm activation.

3.1.14 The Access Control System shall also be provided to designated lift access and car barrier systems.

3.1.15 The specifier shall supply, install and configure the Access Control System management software.

3.1.16 The Access Control System shall monitor and record in a logbook all movements and activities at each control point.

3.1.17 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 to which a card holder has authorized access.

3.1.18 The Access Control System shall provide configurable time schedules to have the flexibility for programming automatic locking and unlocking of any access controlled doors, as well as activating and de-activating of card holder settings for restricting any access groups from entering certain areas with the pre-programmed time model.

3.1.19 The time schedule shall include holiday facilities to allow user programming for public holidays and user definable special holidays. All schedules shall be definable by day, hours and minutes.

3.1.20 The Access Control System shall be designed such that any point of failure within the system shall not affect the normal operation of the other sub-systems. It shall continue to operate even if the connection with the management software is not present.

3.1.21 The Access Control System management software provided 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.

3.1.22 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.
3.2 **Access Control System Server Structure and System Architecture**

3.2.1 The Access Control System server shall be provided and structured based on centralized server architecture.

3.2.2 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 subsystems.

3.2.3 The CPU shall be micro-processor based, completed with adequate disk storage to service the total system requirements and shall be of an industrial standard type, having proven record in similar applications.

3.2.4 Database for Access Control System shall reside within the same server hardware.

3.2.5 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 preferably be Windows 7 (32, 64 Bit) Enterprise, Windows Server 2008 (32, 64 bit), Windows XP.

3.2.6 All Access Control System servers and workstations shall be connected using a standard IP network over the corporate Intranet or dedicated Internet/ LAN/WAN.

3.2.7 Access Control System PC hardware requirements:

- Standard Windows PC for both server and client
- 4GHz CPU
- at least 4GB RAM
- Server: 20GB free disk space
- Client: 1 GB free disk space
- 100 Ethernet NIC (PCI)
- Graphical adapter with 1280 x 1024, 32 k colors
- Resolution Support:
  i. 1024 by 768
  ii. 1280 by 1024
  iii. 2048 by 768
  iv. 2560 by 1024
- CD/DVD ROM.
- I/O Expansion Option
- USB Keyboard and Mouse
3.2.8 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 system or operation.

3.2.9 The Access Control System shall allow the configuration for information access permissions, that is, user/operator profile for the access on the master records, the permissions shall restrict to:

- read only
- read, write, change, and delete
- change the current location of persons
- change the access authorizations of persons

3.2.10 The Access Control System shall allow the configuration for information access permissions, that is, user/operator profile for the access on event data, the permissions shall restrict to:

- view own messages
- view all messages without personal data
- view all messages

3.2.11 The Access Control System shall allow the configuration for information access permissions, that is, user/operator profile for the access to the Configuration dialog.

3.2.12 The Access Control System shall allow the configuration for information access permissions, that is, user/operator profile for door management.

3.2.13 The Access Control System shall allow the configuration for information access permissions, that is, user/operator profile for the access on video applications and devices, the permissions shall restrict to:

- Persons
- can use alarm verification
- can use video verification
- video devices
- can use the specified group(s) of cameras
- video functions
- can use live video
- can use the archive of video streams
- can record and export video streams

3.2.14 The Access Control System server shall act as the source that provides time synchronization to all sub-systems.
3.2.15 The Access Control System shall be designed such that any failure of any sub-systems shall not affect all the other sub-systems. This shall also apply to any loss of power supply or suffer a loss in communications due to a break in the communication loop. In any case, each sub-system shall continue to function in a fully operational state with no loss of functionality.

3.2.16 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. Such upgrade shall not make use of or compromise the spare requirement specified or utilizing or sharing any of its functions.

3.2.17 The Access Control System shall be expandable to support a limited number of 16 integrated operator workstations.
3.3 Access Control System Application Software

3.3.1 The Access Control System Application 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 flexible enough to provide interactive operator prompting to assist operator who are not familiar with the system terminologies, operating system or menu structures, to be able to operate the system with ease and minimal training.

3.3.2 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, Dutch, Russian, Spanish, Portuguese (Brazil), Polish, Chinese (PRC).

3.3.3 The Access Control System AS shall be capable to support to the following:
   - Number of active cardholders – 10,000
   - Number of readers – 128
   - Number of access groups – 255
   - Number of time schedules – 255
   - 4 – 8 digits programmable (Personal Identification Number) PIN codes
   - Video channels – 128
   - Offline Locks – 128
   - Mapviewer floor plans - 128
   - Map links – 64 per map
   - Devices – 64 per map
   - Hierarchal levels between maps – 3
   - If these limits were reached, an upgrade to an Enterprise solution is possible without changing any of the installed hardware.”

3.3.4 Operator Rights
   - 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.
  - Permission regarding video application and devices shall be configurable to the following
    - can use alarm verification
    - can use video verification
    - can use the specified group(s) of cameras
    - can use live video
    - can use the archive of video streams
    - can record and export video streams

3.3.5 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
- Elevator with floor control
- Mantrap
- Door with combined arm/disarm IDS function

3.3.6 Selecting a pre-defined door model shall automatically assign the corresponding reader.

3.3.7 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 editable by administrator

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

3.3.8 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.

3.3.9 Import and Export of Cardholder Master Records
- The Access Control System AS shall provide an 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.

3.3.10 Cards
- A person can have up to three cards at a time. Every card has the same access authorizations and limits (validity limitations, locks, etc.).
- Additional the Identification PIN can be used like a card.

3.3.11 Access Authorizations:
- Grouping of entrances that consist of one or more readers shall be possible, where one entrance can exist in several groups. A cardholder shall be assignable directly to any of the Access Authorization groups.

3.3.12 Area-Time Authorizations:
- The Access Control System shall allow incorporating of access authorizations with time models. The assigned time model defines the time when an access authorization is active at an entrance or entrance group.

3.3.13 Time Models, Day Models, and Special Days:
- The Access Control System AS provided shall allow the creation of time models for any specific day within the day models. Configuration for Special days, such as public holidays shall also be supported. The definition of time models provides a simple way of defining periodically recurring day models, which have a specific order. The time model can be used together with the access authorization at any entrance or entrance groups to control access.

3.3.14 Defining the Area of Control:
- The Access Control System AS shall provide the ability for defining of logical areas, which could be single room, groups of rooms, entire floors where access control points/entrances could be assigned to.

3.3.15 Access Sequence Check:
There shall be an access sequence check provided, allowing an authorized cardholder to enter a door or group of doors belonging to a pre-defined area only when he has already passed another dedicated door.

3.3.16 Dual or Multiple Authorized Access:

- The Access Control System AS shall provide the possibility to configure and allow access to an access controlled door only when at least two authorized cardholders present their badges at the card reader. The number of cardholders for that kind of access check in front of an entrance should be limited by 6 persons.

3.3.17 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 input of a validity period has to be supported.
  - Verification PIN – it 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.

3.3.18 Duress Code Alarm:

- A duress code alarm message shall be generated at the Access Control System and display on the monitoring workstation when cardholders keyed in their PIN codes in another defined way.

3.3.19 Blocking Cardholders:

- The Access Control System AS shall allow the blocking of cardholders, for example by validity period.

3.3.20 Visitor Management:

- Administration of visitors shall be provided by the Access Control System management software in the same database.
- The visitor management shall allow the printing of a visitor badge from this data.
- The following information should be assignable to a visitor:
  - Identification number
  - Access authorizations
3.4 MAPVIEWER

3.4.1 The system shall contain a map viewer. This map viewer shall provide a graphical presentation of the premises or object by means of floor plans, object pictures or any desired graphical representation.

3.4.2 Navigation links allow navigating from one map to the next. It should be possible to navigate maps horizontally on the same level enabling to cover a larger area with multiple maps next to each other, or vertically up to three levels in which navigation to the next map brings the underlying map e.g. navigate into the room details from the map showing the floor details.

3.4.3 The map structure is given in a map tree at the left side of the active map. The tree allows jumping multiple layers or bypassing multiple correlated links by selecting the target map in the tree directly.

3.4.4 Back and forward buttons in the top of the map viewer allow navigation between the maps by viewed sequence.

3.4.5 On the maps entrances and cameras can be positioned as a graphical icon. These graphical icons will display the location of the device in the map and the actual status of the device. Clicking any of the devices automatically shows the controlling commands available for the respective device. Control commands are automatically linked based on device type.

3.4.6 Access events at the door are automatically recorded by one or more mapped cameras for a predefined recording time window. The time window for recording can be programmed.

3.4.7 Recordings will be part of the logged event and can be accessed by clicking on the camera symbol in the stored event line.

3.4.8 Alarm management:

3.4.9 The system shall offer alarm management. The alarm management builds on the map view functionality extended with an alarm list.

3.4.10 The alarm list shall support multi handling ensuring when multiple operators are logged in at the same time the event can only be treated by one operator, the operator that treats the event first.

3.4.11 In case of alarm the map with the alarm location will automatically get dialog focus and will be displayed accordingly. The device that triggered the alarm will show alarm status on the map by means of a .gif format animated icon to attract attention together with a beeping tone.

3.4.12 The alarm shall appear in the alarm list dialog as alarm event. The alarms in the alarm list queue require a manual alarm acceptance from the operator.

3.4.13 Alarm events in the alarm list require a written comment entry by the operator before it is possible for the alarm to be accepted. The comments are logged. Accepted alarms are removed from the alarm list.

3.4.14 In case the operator navigates through maps while an unaccepted alarm exists, maps with a direct navigation link to the map with the alarming device, shall display any hyperlink to that map with an animated red blinking notification. This
animated signalling navigation link indicates that behind this navigation link a map exists with an unaccepted alarm.

3.4.15 The system shall offer alarm video verification as part of the alarm management. The alarm video verification builds on the alarm management functionality extended with video streaming and recording of alarm events.

3.4.16 It shall be possible to map system devices on the map to one or more cameras for alarm video verification. If the respective device reaches the state of alarm the corresponding cameras will automatically start recording the event and show the camera live streams to the operator.

3.4.17 Video Verification Access:
- There shall be possibility by combining with existing video devices to configure dedicated readers for video verification access mode.
- Instead of opening the door immediately when an authorized card is presented, the reader/controller shall generate an event at the ACCESS CONTROL SYSTEM. A corresponding alarm dialog displays the stored image of the cardholder along with a live video image from the corresponding door. The operator shall determine if both images match, he can decide to open the door or to deny the access.
- It shall be possible to link up to 5 camera’s per door to ensure video verification with optimal situational awareness at the door.

3.4.19 Offline Locking System (OLS)
- The Access Control System allows the integration of OLS devices.
- The personal data will be managed by the Access Control System Online System.
- Persons can use the cards they have for the Online System - but only the first one.
- There are special access authorizations regarding to the OLS.
- There are special time models regarding to the OLS.
- There are separate validation limits regarding to the OLS.

3.4.20 Mantrap:
- 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 rest shall be blocked for access.

3.4.21 Elevator Control:
- The Access Control System AS provided 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.
3.4.22 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 be opened, but an event shall be triggered at the Access Control System monitoring workstation. Upon receiving the message, the operator/guard shall be reminded 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.

3.4.23 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.

3.4.24 Access Control Management Alarms and Events

The Access Control System AS shall provide a wide range of standard alarm and event states. The following alarms/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
- Random screening
- Other individual alarm extensions
3.4.25 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.

3.4.26 The Access Control System AS provided shall have support for central alarm monitoring and management. It shall provide a graphical user interface (GUI).

3.4.27 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.

3.4.28 The Access Control System AS shall securely logged 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.

3.4.29 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.

3.4.30 A device tree and the device names shall be provided for in the GUI.

3.4.31 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. The printers shall be connectable directly to a workstation or to the network.
3.5 **Graphical User Interface**

3.5.1 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.

3.5.2 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 resolutions: 1024x768, 1280x1024 (1-monitor operation), 2048x768 and 2560x1024 (2-monitor operation).

3.5.3 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.

3.5.4 In the event of alarm activation, the alarm message shall be displayed at the destined Access Control System operator workstation together with an external audible siren or via PC internal speaker.

3.5.5 For the alarm sound generated from the PC internal speaker, standard formats such as WAV, MP3 or WMA shall be supported and selectable for assigning to individual alarm/event or groups of alarms/events during system configuration.
3.6 **Access Control System Alarm Handling and Management**

3.6.1 The Access Control System shall provide the operator a simple and efficient way to handle any incoming alarms.

3.6.2 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.

3.6.3 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.

3.6.4 All incoming alarms at the Access Control System GUI workstation shall contain a comprehensive alarm message.

3.6.5 The incoming alarm or event message shall provide, but not limited to, the following information:

- Alarm date and time
- Alarm status
- Current alarm condition
- Alarm location

3.6.6 The operator shall be able to silence the audible alarm sound or buzzer, while he is busy processing earlier alarms.

3.6.7 The alarm message shall also show live video images from the Video Verification camera installed at the alarm location such that, the operator can have first time view of the site situation if required.

3.6.8 The operator shall be allowed to revert or toggle between all alarms or events messages.

3.6.9 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.

3.6.10 The operator shall be allowed based on his login access profile generate alarm and event reports from his operating workstation.
3.7 **Access Control Hardware**

3.7.1 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
- C-Tick

3.7.2 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.

3.7.3 The Access Control Hardware design shall be of standard 19\(^\circ\) rack mountable and also rail mountable for installation in an weather-proofed enclosure suitable for used in outdoor.

3.7.4 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.

3.7.5 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.

3.7.6 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.

3.7.7 The Access Control Hardware memory shall under no circumstance loose a single, not even the last transaction when power fails.

3.7.8 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.

3.7.9 The Access Control Hardware memory shall store database that has a capacity with a minimum of 80,000 cardholders (upgradeable to 400,000), each having a programmable 4 – 8 digits (Personal Identification Number) PIN codes.

3.7.10 The cardholder database shall be upgradeable by exchanging the CF card. The system shall automatically detect the size of the CF-card.

3.7.11 The Access Control Hardware provided shall support the connectivity of up to a maximum of 4 standard Wiegand interface readers or 8 serial interface readers operating on RS485 bus technology.

3.7.12 The Access Control Hardware provided shall support multiple, but not limited to the following card formats:
  - Wiegand 26 Bit
  - Wiegand 35 Bit (HID Corporate 1000)
  - Wiegand 37 Bit (HID iClass)
  - Mifare 32 Bit CSN

3.7.13 The Access Control Hardware shall provide minimum eight programmable I/Os on board, and shall be expandable to 32 each, using I/O extensions.

3.7.14 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)

3.7.15 EOL resistor’s values shall be flexibly selectable in the Access Control System management software during configuration.
3.7.16 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.

3.7.17 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.

3.7.18 The Access Control Hardware Firmware is updateable through the Host System via download

3.7.19 The Access Control Hardware memory shall under no circumstance loose a single, not even the last transaction when power fails.

3.7.20 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.

3.7.21 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
3.8 Specifications for Proximity Card Reader

3.8.1 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.

3.8.2 Power requirement: 10 – 16Vdc.

3.8.3 Transmit frequency: 125 kHz

3.8.4 The proximity card readers shall have a read range of at least 3”.

3.8.5 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.

3.8.6 The card reader unit shall have an integral keypad with beeper, multi-color LEDs.

3.8.7 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.

3.8.8 The overall thickness of the card reader unit shall not exceed 30 mm.
3.9 Specifications for Contactless Smart Card Reader

3.9.1 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.

3.9.2 The smart card reader shall be based on contactless smart card 13.56MHz technology for connection to the Access Control Hardware with Wiegand interface.

3.9.3 The contactless smart card reader provided shall be capable of reading MIFARE serial number in 32-bit format in accordance with ISO standard 14443A.

3.9.4 The data transfer between the contactless smart card reader and smart card shall be encrypted.

3.9.5 Power requirement: 10 – 16Vdc.

3.9.6 The contactless smart card readers shall have a read range of at least 2.4".

3.9.7 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.

3.9.8 The card reader unit shall have an integral keypad with beeper, multi-color LEDs.

3.9.9 The keypad shall have backlight 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.

3.9.10 The overall thickness of the card reader unit shall not exceed 30 mm.

3.10 Specifications for Proximity Card

3.10.1 The offered proximity cards shall be similar in size and thickness as standard credit cards or bank ATM cards.

3.10.2 The proximity cards shall operate on 125 kHz.

3.10.3 CE/UL Approvals

3.11 Specifications for Contactless Smart Card

3.11.1 The offered contactless smart cards shall be similar in size and thickness as standard credit cards or bank ATM cards.

3.11.2 The offered smart cards shall be of contactless technology operating on 13.56 MHz and shall be compliance to ISO standard 14443A.

3.11.3 CE/UL Approvals
3.12 **Specifications for Finger-print (FP) Biometric Reader & Operations**

3.12.1 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.

3.12.2 The FP biometric reader shall provide two-factor authentication with the combination of a proximity [contactless smart] card and a fingerprint biometrics.

3.12.3 The FP biometric reader together with the proximity [contactless smart] card shall support operation with 1:1 verification mode or 1:N, identification mode.

3.12.4 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.

3.12.5 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.

3.12.6 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.

3.12.7 The same FP biometric reader provided shall be able to be used for both access control and as an enrollment station.

3.12.8 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.

3.12.9 During enrollment process, the FP biometric reader and software used for capturing the finger-print shall provide, but not limited to the following:

3.12.10 The FP image shall have a minimum size of 256 x 360 pixels

3.12.11 Provide full visibility of the ridge details including texture, continuity, edges and pores.

3.12.12 Allow for real-time on-screen preview of the FP image while performing the FP capture.

3.12.13 FP captured shall have resolution of at least 500dpi.

3.12.14 Minutiae file size of at least 256 bytes.

3.12.15 The FP enrollment process shall support a percentage estimation of the image quality such that the operator can accept or reject the enrolled FP.

3.12.16 Up to a maximum of 10 FP templates shall be allowed to be assigned to a single user.

3.12.17 The enrolled FP templates shall be stored in the Access Control System centralized database as well as within the reader’s memory storage.

3.12.18 The FP templates stored shall incorporate a date stamp and shall record the number and/or name of the finger taken.
3.12.19 The FP images captured shall be stored in an open format such as jpeg or bmp for the purpose to export for further use by another application when required.
## 4. Change History

Change history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author / Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>01-Mar-08</td>
<td>Initial Version (derived from SSG A&amp;E Specs)</td>
<td>Kolberg</td>
</tr>
<tr>
<td>0.02</td>
<td>20-Apr-09</td>
<td>Review by Harald Gilleßen</td>
<td>Gilleßen</td>
</tr>
<tr>
<td>0.03</td>
<td>23-Apr-09</td>
<td>Review and comments by Daniel Queck</td>
<td>D. Queck</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>27-Apr-09</td>
<td>First Release</td>
<td>Gilleßen</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>29-Apr-09</td>
<td>Review A. Squarize</td>
<td>A. Squarize</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>01-June-11</td>
<td>Review M.Wings</td>
<td>M.Wings</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>27-June-11</td>
<td>Review M.Wings</td>
<td>M.Wings</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>01-Nov-11</td>
<td>Review M.Wings</td>
<td>M.Wings</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>06-Feb-12</td>
<td>Review M.Wings</td>
<td>M.Wings</td>
</tr>
<tr>
<td>1.0.0.0</td>
<td>06-Feb-14</td>
<td>Update M.Wings (APE3.0)</td>
<td>M.Wings</td>
</tr>
</tbody>
</table>