Access Easy Controller 2.1

(Architect and Engineer Specification)

THIS DOCUMENT IS PROVIDED AS A GENERAL GUIDE TECHNICAL TENDER SPECIFICATIONS FOR ACCESS EASY CONTROLLER 2.1 (REFERRED THROUGHOUT THIS DOCUMENT AS AEC2.1).

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 TENDERER/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 TENDERER/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 AEC2.1 SPECIFICATION WAS ISSUED/UPDATED:

August 2010 VERSION 1.0.3

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

TABLE OF CONTENTS

1.0 Overview

1.1 Web-Based Access Control

The proposed system shall fulfill the functions and specifications described in this document. In particular, the access control system shall be an IP web based access control system whereby any computer can be used to operate the controller (or control panel) directly using a standard web browser program available freely. The controller shall be a black-box design with embedded software built-in, including a web server program. The basic functions are:

- Card access control
- Alarm monitoring and handling procedures
- Time attendance data capture and post processing
- Video verification and video surveillance

1.2 System Architecture and Specifications

The proposed PC shall be based on the latest version of Intel or AMD based computers.

1.2.1 The controller used shall be based on minimum 32-bit embedded microprocessor chip, and communicate with the central PC via Ethernet network directly at speed of 100 Base-T.

1.2.2 The controller, input-output interfaces and card readers shall be able to work in off-line mode even if there is a failure with the computer network.

1.3 Main Hardware Components for the proposed system

The overall system shall consist of the following major equipments:

1.3.1 A standard desktop PC to be used for cards assignment to users and monitoring of alarms in the whole system.

1.3.2 A controller (control panel) used for access control and alarm monitoring and control functions. This controller shall be able to support a maximum of 32 doors and monitor 64 alarm sensors. It shall also be able to control xx units of siren boxes and control an alarm communicator box to send alarms to a central alarm monitoring station. The controller shall be able to connect to an external GSM communicator to send out alarm messages via the standard GSM telecommunication network.

1.3.3 Card readers for access control, attendance data capture, intrusion alarm arming/disarming.

- Provide for XX units of entry card readers for access control
- Provide for XX units of exit card readers for access control
- Provide for XX units of arming/disarming card readers
- Provide for XX units of card readers for time attendance
- Provide for XX units of PIR sensors as intrusion alarm sensors
- Provide for XX units of magnetic door contacts as intrusion alarm sensors
- Provide for XX units of dual PIR + motion sensors as intrusion alarm sensors
- Provide for XX units of siren box with strobe light
- Provide for connection to a GSM communicator to send alarm text messages to hand phones

1.3.4 Provide an UPS for the central computer lasting minimum of 2 hours of uninterrupted power during power failure.

1.3.5 Power supplies with back-up batteries for all other access control equipments and electric locking devices, providing minimum 4 hours of uninterrupted power during power failure shall be provided.

1.3.6 Provide a PC with following minimum specifications:

- Latest version of Intel Pentium IV with the fastest speed
- Microsoft Windows 2000 SP4 or later
- 1 GB RAM (2GB for Vista and later)
- Hard disk: 80 GB

- CD-ROM drive
- 15" color LCD monitor
- Ethernet network port: 10/100 Base-T
- DirectX 9.0c
- Video card that supports DirectX 9.0c
- Microsoft.NET Framework 3.0
- Printer Port: Parallel port (LPT-1)
- DirectX
- Keyboard
- Printer

1.4 Technical Specifications of the Controller

The controller shall be a generic unit that is designed with a common firmware running all embedded software. It shall be able to perform multiple tasks concurrently.

1.4.1 Minimum specs for the embedded controller shall be:

- At least a 32-bits CPU
- Have a minimum speed of 500 MHZ
- Support a communication port for remote dial-in via modem
- Support standard RS 232 port
- Support a Ethernet 100 Base-T port
- Minimum of 512 Megabytes of Flash memory, upgradeable to 2 Gigabytes
- Minimum of 512 Megabytes of RAM

1.4.2 Support up to 64 digital input monitoring channels for alarm monitoring. Each monitoring channel shall employ end-of-line sensing devices to detect against alarm and cable fault. Each input shall provide selection choice of 2-state or 4-state alarm monitoring. For 4-state monitoring, it shall be possible to detect cable short circuit or open circuit.

1.4.3 Supports up to 64 channels of voltage-free relays for alarm signaling and on/off controls using form-C type of relays.

1.4.4 Each controller shall consist of at least one CPU board, one or two card readers' controller board, and/or one 8 channels input and output board, AC Line Filter, one regulated power supply unit with an optional on-line battery charger charging a single 12V 7AH maintenance-free backup battery.

1.4.5 Each card reader's controller board shall support atleast 4 industry standard wiegand compatible reader interface ports. Each board shall also provide digital input interfaces to egress switches and door status sensors, and form-C relay output interfaces to door strikes, magnetic or electronic locks. All output relay shall be rated 24VDC @ 1 ampere with at least 2 spare relay circuits.

1.4.6 The 8 channels Input and Output board shall provide 8 digital input channels to be connected to intrusion alarm sensors. The 2 form-C relay output channels shall be provided for alarm devices control.

1.4.7 Additional Extension Unit shall be provided if additional doors or inputs/outputs are required.

1.4.8 A modem port shall be provided for PSTN/dial-up or lease line operation. Dial-up operation shall use standard PPP protocols. Upon successful log-in, the accessing computer shall only require a standard web browser program to operate, monitor or control it.

1.4.9 The controller memory buffer shall be able to hold 100,000 transactions when the controller is operating in a standalone mode (off-line mode)

1.5 Technical Parameters of the Controller

1.5.1 Card Parameters:

The controller database shall have a memory capacity for a minimum of 20,480 cardholders, each having a programmable 4 - 7 digits (Personal Identification Number) PIN codes

1.5.1.1 The PIN for each card number in the database shall be unique. The capacity of the card numbers in the database shall not be decreased due to the use of PIN for each card.

1.5.1.2 Each cardholder shall be able to change his/her own PIN on the card reader itself without the needs of having it done by the system

administrator at the central PC. Change of any cardholder's PIN code shall not affect the rest of the user's PIN codes

1.5.1.3 The card reader-controller shall be able to select 2 modes of operations, between "Card" only or "Card + PIN". It shall also be possible to program up to 8 sets of schedules (different start time and end time periods) per person everyday to be used for automatic activation of the PIN requirements as described earlier. To further enhance the security level, this mode shall be able to work differently during weekends or holidays by utilizing another set of schedules (time zones.)

1.5.1.4 It shall be possible to allow a cardholder to carry only one card, where that card can function as a normal access card, or as an arm/disarm card, or as a time attendance card, or a combination of any of these functions. All cards shall be generic in nature and the controller shall be able to reassign the function(s) of each card.

1.5.1.5 Every card shall have a start and expiration date parameter, so that the card is valid on 'start date' and becomes void on the 'expired date'. This function allows a card to be issued to contract employees or contractors in advance.

1.5.1.6 It shall be possible to assign a cardholder to a 2-person rule (alternatively known as dual-card group) and operate with the following security access control requirement:

- Any normal access cards may be assigned to a dual-card grouping. There shall be at least 255 dual-card groupings.
- Card readers shall grant access based on dual-card rule for important access doors.
- Card readers shall be able to change operational behavior automatically, from dual-card rule to single access rule; and then reverting back to dual-card rule; or remains at dual-card rule at all time.

1.5.2 System Parameters

1.5.2.1 Access Groups

Each controller shall have at least 254 programmable Access Groups. Each Access Group defines access for a particular group of doors associated with its own set of schedules (time zone groups) where a person can enter.

Each cardholder shall be assigned a minimum of 2 access groups.

1.5.2.2 Schedules (Time Zones)

Each controller shall have at least 255 weekly schedule (time zone) groups for all operations. Each schedule consists of at least 4 different start and stop time zone periods.

These schedules (time zones) shall be usable for any or all of these applications:

- activating different card access operation modes
- automatic locking/unlocking of doors
- automatic arming/disarming of an alarm point
- automatic arming/disarming of the intrusion monitoring modes
- automatically control electrical equipments on and off
- sending Email/SMS

1.5.2.3 It shall be possible to pre-program up to 32 regular holiday dates and 32 special holiday dates so that its operations will change automatically. It shall also adjust itself to leap year computations automatically and also GMT date/time reference.

1.5.2.4 The controller shall provide anti-passback feature for a single reader or a group of readers as a standard feature.

1.5.2.5 True anti-passback shall be implemented with selectable forgiveness or non-forgiveness modes. In forgiveness mode, a cardholder shall be able to get out of the controlled area even if he/she forgets to use his/her card at the entry reader and instead followed someone in.

1.5.3 Door Parameters:

1.5.3.1 When a card reader reads a valid card, the controller shall unlock the door for 3 seconds (shall be programmable from 3-255 seconds). For each handicap person, it shall be possible to provide extended door unlocking timings to facilitate their slower movement.

1.5.3.2 A door ajar (partially open) alarm shall be generated if the door is held open longer (example 1 minute, but programmable from 60 seconds to 255 seconds) than the allowed preprogrammed time. This alarm shall automatically be reset when the door is closed back.

1.5.3.3 It shall be possible to control the locking/unlocking of doors automatically up to four time zone periods per day based on schedule (time zone) control. The card reader shall emit a beeping warning signal if the door is not closed at the end of the time where the door is supposed to be re-locked.

1.5.3.4 It shall be possible to set the video verification camera and the surveillance camera.

1.5.4 Alarm Messaging Via Built-in Email:

1.5.4.1 It shall be possible to select and send specific events, transaction(s) or alarms via integrated built-in email function. The email messaging shall be deployed using industry standard SMTP protocols.

1.5.4.2 Each email subject text message and body text message shall be user programmable in alphanumeric, just like normal email.

1.5.4.3 It shall be possible to send any event or alarms generated throughout the systems and the following minimum events and alarms transactions shall be provided:

- any selectable events with location, date, time and the cardholder name such as access denied, invalid schedule and wrong PIN code used
- any alarms indicating the location, date and time of occurrence
- duress alarm, date and time of occurrence
- illegal log-in attempts via modem, date and time of occurrence
- power failure and restore, date and time of occurrence
- alarm points being armed/disarmed, date and time of occurrence
- controller being tampered, date and time of occurrence
- door being forced opened or left opened, date and time of occurrence

1.5.5 Video Parameters:

1.5.5.1 Each card reader shall support up to three cameras.

1.5.5.2 It shall be possible to view ‘Live’ and ‘Playback’ video. It shall be possible to compare the ‘Live’ and ‘Playback’ video using the compare option.

1.5.5.3 The surveillance window shall pop up when an event is triggered in the configured location.

1.5.5.4 When a card is presented to the reader the video verification function shall enable the live video display of the access point for comparison with the cardholder’s photo for the operator to grant or deny door access.

1.5.5.5 The system shall auto detect the available cameras and shall add the selected cameras to the system

2.0 Access control system -- Computer and software requirements:

2.1 It shall be possible to use an Intel based PC as the central monitoring computers to operate the system.

2.2 All software provided shall reside within the controller. There shall be no need to install any software in the PC. When user logs in to the controller via a standard web browser software with .NET Framework 3.0 (Microsoft Internet Explorer 7.0 and above) User shall be able to operate the entire system, whether to view transaction activities, make changes to system operating behavior, add or delete cards.

2.3 Up to 25 users shall be able to operate, monitor and control the entire system, each with a unique ID and password. All user ids and password are encryption protected and case sensitive. The system shall support up to a maximum of 8 concurrent users. The system shall allow multiple users to log in and monitor activities, view alarms or administrate different database for different purposes, whether access control or alarm monitoring.

3.0 Access Control and alarm monitoring -- Software Functions:

The following software functions shall be provided:

- Administrators or users access rights setup
- Password assign to all users and administrators
- Centralized access control and alarm transactions monitoring

- Remote control functions for access control, arming/disarming of alarm points and on/off controls
- Alarm monitoring and alarm handling procedures
- Card database administration
- Global card formats setup
- View ‘Live’ or ‘Playback’ video
- Compare ‘Live’ and ‘Playback’ video
- Grant/Deny access based on video verification feature
- Auto detect the available cameras
- Report generation of transactions

3.1 Database Access Rights & Setup:

3.1.1 It shall be possible to select a language from the Multilanguage webpage provided for the GUI interface

3.1.2 It shall be possible to setup different access rights for each administrator and users to allow them access to different database.

3.1.3 The controller shall have different web pages for parameters setup, monitoring or control purposes.

3.1.4 Any administrators shall have their own access rights to view the card database only or include rights to add or delete cards.

3.1.5 Any system administrators shall have their own access rights to monitor transactions and alarms only, or include alarm handling.

3.1.6 Any system administrators shall have their own access rights to remotely unlock doors via web browser.

3.1.7 Any system administrators shall have its own access rights to view alarm monitoring status only or include rights to arm/disarm a point or group of points via web browser.

3.1.8 Any system administrators shall have its own access rights to control any relays on/off, where such relays are used to control any electrical devices or equipments via web browser.

3.2 Transaction Activity Viewing Functions:

The transaction activity viewing webpage shall display the photo of the cardholders when the user moves along the card number column.

The transaction activity page shall provide the reset APB option.

The system shall provide multiple choices of View Modes:

3.2.1 All Transactions View

The All transactions view shall display each and every transaction as it occurs in the system, consisting of normal as well as alarm transactions. For card access events, the transactions shall consist of the date and time of occurrence, door location, cardholders name and his or her card number.

3.2.2 Alarm View

The Alarm view shall only display the alarm transactions.

- For card access events, it shall consist of the date and time of occurrence, door location, person's name, his or her card number and the type of alarm.
- For alarm monitoring function, it shall consist the date and time of occurrence, intrusion location and the type of alarm.

3.2.3 Alarm & Restore View

The Alarm & Restore view shall display the alarm condition has been restored to normal state.

3.2.3 APB View

The APB view shall display the cardholders name currently in the selected APB zone or all the zones.

3.2.4 Time Attendance View

The Time attendance view shall display the date and time details when the cardholder accessed the system.

3.2.5 Online Swipe View

The online swipe view shall display the latest three cardholders with photo, who accessed the system. It shall also display the cardholder's photo and cardholder details that accessed the system in the selected location.

It shall allow the authorized users to reset APB for the APB violating users.

3.2.6 Surveillance View

When an alarm event is triggered the surveillance window shall automatically display the 'Live' event video of the location. It shall allow the user to toggle between the 'Live' and 'Playback' event video.

The compare option shall compare the 'Live' video and the event video playback clip simultaneously. In the surveillance playback view the user shall download the event clip or capture a snapshot from the even video.

3.2.7 Camera Monitoring View

The camera monitoring view shall display the 'Live' and 'Playback' video for a selected date. The user shall view the 'Live' or 'Playback' video of any configured camera.

This view is used to monitor the cameras.

3.2.8 Video Verification View

The video verification view shall display the live video of the access point for comparison with the cardholder's photo. This allows the door operator to grant or deny access to the cardholder via webpage manually. In event that there is no action and the timeout occurs, the access is granted automatically based on the settings of the video verification feature.

Video verification feature shall be enabled or disabled based on schedules. This view shows the 'Live' video of all the cameras configured to the reader.

3.3 Remote control Functions:

All remote control actions shall be executed via specific web pages. Each control action shall be designed for minimum mouse clicks. Web pages shall show the current state of the devices and the state after a control action has been executed.

3.3.1 Locking & Unlocking of Doors

- User(s) shall be able to unlock and re-lock a door from web page directly. A door can be momentarily or permanently unlocked and re-locked.
- The controller shall generate a transaction indicating who has unlocked a door and the date and time of his or her action.
- All doors shall show its status on web pages, whether it's locked or unlocked.
- It shall also be possible to execute this function without any limitation via modem dial-in remotely.

3.3.2 Arming & Disarming of Alarm Functions

- Users shall be able to arm/disarm the alarm monitoring functions via the card readers or web pages
- Users shall be restricted to arm/disarm alarm zone(s) within their access rights only.
- Transaction shall show who has armed or disarmed a specific alarm zone(s) and the date and time of action.
- It shall also be possible to execute this function without any limitation via modem dial-in.

3.3.3 Output Control Functions

- Users shall be able to turn on or off electrical equipments or devices, such as lightings, air-conditioning units, motors etc., via web pages.
- It shall also be possible to execute this function without any limitation via modem dial-in.

3.3.4 Advance IO Functions

- It shall allow unique programming options for input and output linking based on logic programming.

- It shall allow pre defined logic programming such as Guard Tour, Feed Through, OR Logic, AND Logic, XOR Logic, NAND Logic, Interlock, Up-Down Counter, Exit door, One shot and Intrusion.

- It shall integrate a 3rd party intrusion system using standard input/output from the system.

3.4 Alarm Handling Procedures

3.4.1 All alarm transactions shall be acknowledged individually.

3.4.2 When an alarm transaction is received, the computer shall generate an alarm tone to alert the operator. This audio alarm shall sound continuously until the alarm has been turned off by the operator.

3.4.3 The controller shall generate a transaction record in its memory for every alarm and restore conditions, which include –

- Date and time of occurrence and restoration

- Location of alarm sensors

- Date and time of user's acknowledgement

3.5 Card Database Administration

3.5.1 It shall be possible to add or delete cards and define all other card related parameters for the controller.

3.6 Report Generation

3.6.1 It shall be possible to generate any reports within the controller. All reports generations shall also be executed via web page command.

3.6.2 System Reports

- Reports generated shall include normal transactions, alarm transactions, system parameters set up and the controllers' parameters set up.

3.6.3 It shall be possible to view the reports on computer screen first prior to printing.

3.6.4 Activity reports

The reporting program shall allow report filter selection by:

- Activities (transaction types)
- Card Number
- Cardholder name
- Department
- Location
- Date range selection
- APB zone

3.6.5 Card reports

The reporting program shall allow report filter selection by:

- Card Number
- Access group

3.6.6 Device reports:

The reporting programs shall be able to generate the following reports

- Reader
- Input point
- Output point
- IO Function blocks
- Camera description
- Video device

3.6.7 Configuration reports:

The reporting programs shall be able to generate the following reports

- Criteria

- Schedules
- Regular holiday
- Special holiday

3.6.8 Audit Log Reports

Audit log reports shall be available to provide the following minimum information:

All operators' log-in and log-out date and time stamp

The date and time stamp of each operator whenever the operator made a change in any of the database, including the exact changes made.

3.7 Card Formats Setup

3.7.1 The controller shall be able to program and set up to 16 different card formats. Each card format template shall be programmable and only require the card number field, facility code (site code) field and parity bit pattern/location data fields to be entered.

4.0 Attendance Data Capture

4.1 It shall be possible to setup card readers for the purpose of capturing of attendance data for 'date and time clock-in' and 'date and time clock-out' for staff or guards. Standard card readers with keypad similar to those configured for access control shall be able to perform these functions.

4.2 A separate web page shall be dedicated for this function and be able to view the date and time the transactions occurred.

4.3 It shall be possible to export transaction file in comma separated value file format (CSV or XLS file format) that is readable by Microsoft Excel programs for further processing.

5.0 Configuration

5.1 The user can upgrade the firmware in a separate dedicated webpage

5.2 It shall be possible to set a daily auto backup to the compact flash or a manual backup of the system database

5.3 It shall be possible to upload the customer logo to the webpage. The uploaded customer logo is seen on all the WebPages and in the reports generated and printed

6.0 Approvals

6.1 The offered controller shall be FCC or CE and UL approved.