ENTRYPASS

EntryPass
Technical Specification

SPECIFICATION FOR ARCHITECTS, CONSULTANTS AND ENGINEERS (PHASE1 – V1.02)

Access Control System (ACS) overview

The card access control system is to control and secure access to the restricted area. In a complete access control system solution, both software and hardware play a very important role in managing the whole security network. The software is referring to the server where all the captured transaction on the door controller will be polled back to the server for real time transaction monitoring purposes and other application such as time attendance and etc.

1 Software

This section specifies the overall software feature which shall form part of this contract. The function of the software system is to provide a user interface for the user to enter the data or setting and also to produce various types of reports for reference. It shall provide a local database file to keep all the setting and transaction logs. It shall download all the setting or control function performed by the user to the controller.

1.1 Server and client type

This software shall be able to support server and client architecture whereby server is referring at the central/main system that manage the entire system include of user database, controller database, transaction storing, report viewing and etc.

Client is refer as a client software that install in another PC and with the help of the client software, user can now directly login from other computer with a dedicated password and username to monitor and maintain the system. The client software shall be able to communicate with the server software via LAN based on TCP/IP protocol. If the client software implementation is involve in a remote site via WAN environment, a proper network and router configuration are needed to be done before the client software can connect to the server.

1.2 Password authentication

The software shall require the user to enter the password in order to access. Each user shall be assigned a menu control access privilege to control their accessibility to the menu command in the software. This password authentication is required in both server and client software for security purposes. The software shall allow user to change their password upon login.

1.3 Communication

The software shall be able to communicate with the controller via LAN based on TCP/IP protocol and serial communication type via RS485 or RS232.

1.4 Comport

The software shall allow a maximum of 8 comport to be connected to the software working concurrently. Therefore it shall support up to 128 controllers for serial type.

1.5 OnlineTransaction

This software online transaction shall prove the capacity to provide real-time processing of normal transactions and also any events occurred. The online transaction shall be able to provide a 'Pause' button for user to pause the incoming transaction and a 'Show Detail' button for user to view additional information of the selected card holder and also the card holder photo if available. The online transaction shall able to provide user the ability to select the desire column to be present at the online transaction list. Below are the lists of item that can be selected by user:

- Date (hard-code)
- Time (hard-code)
- Controller
- Door
- Staff No.
- Name
- Department
- Job
- Shift
- Card No.
- Transaction
- IO Board
- Zone
- Point

1.6 Alarm Events

The software shall be capable of categorizing each alarm events in priority level form where each priority levels are categories as below:

- Highest Priority
- Higher Priority
- Normal Priority
- Lower Priority
- Lowest Priority

Different priority level is differentiate by colour indicator and each assigned alarm event occur in the software will display according to the colour.

The software shall be capable of allowing user to change each alarm event sound (wav format)

When alarm event occurs in the system, the system shall at least perform the following functions:

- An alarm list will be pop-up even when the software is minimized on the window taskbar
- Sound the PC buzzer or speaker
- An indicator will keep on flashing/blinking to draw user attention

The software shall only allow login user to clear the alarm event from the alarm list by acknowledging the viewed alarm.

The software shall allow login user to write a comment on the viewed alarm event before acknowledging it and this comment can be viewed in report form.

1.6.1 SMS Notification

The software shall be able to send out SMS notification to dedicated recipient upon any alarm event received. The software shall allow user to configure up to 5 recipients at minimum.

1.6.2 Email Notification

The software shall be able to send out Email notification to dedicated recipient upon any alarm event received. The software shall allow user to configure up to 5 recipients at minimum.

1.7 Device List

This software device list shall be capable of displaying the entire controller status that connect to the system in one list form and this device list shall also provide the door status whether the door is in lock/secure condition or unlock/unsecure. Apart from monitoring the controller and door status, the software shall also allow user to monitor the controller power status whether is running on AC power or battery power.

The software device list shall be able to provide certain door command in-case of emergency situation where user needs to release all the doors or inhibit certain door from accessing. Below are the door commands that can be performed by user:

- Security Off
- Security On
- Pulse Door Open
- Inhibit Door
- Uninhibit Door

1.8 Interactive Floor Plan

The software shall have floor plan database and the capacity of the floor plan is not less than 100 floor plan maps. Each door is represented by an icon placed on the floor plan for much user-friendly interface and to resemble the actual door installed on the area.

The software floor plan shall provide an easy step on positioning the door icons on the floor plan by means of drag and drop method.

The software floor plan shall be able to select the floor plan mode either in manual mode or automatic mode where the floor plan map will be automatic change to the next map according to the selected time interval.

The software floor plan shall have the online real-time floor plan display whereby the icon that represent the door shall change colour whenever unwanted alarm event such as door force open occurs at the door. The floor plan shall be automatically display and switch to the floor plan map containing the door icon.

The software floor plan shall support the following types of picture format:

- BMP (Bitmap)
- JPEG (Joint Photographic Experts Group)
- GIF(Graphic Interchange Format)

1.9 Wizard

The software shall be able to provide wizard assistance where this wizard function shall guide the user to install the active network controller into the software database by following the easy steps provided. If any of the active network controllers is detected by the software, the wizard form shall automatically pop up from the screen to notify user that there is a new controller reporting in for service.

1.10 Active Engine

The software shall be able to provide an Active Engine module which serves as a messenger between the software and active network controller. This Active Engine module shall be able to detach from the core software when large scale installation is implemented. Depending on the PC server specification, when necessary, Active Engine module can be setup on additional PC to balance the server process loads. Hence this will maintain the PC server efficiency. The software shall be able to support up to 10 Active Engine modules at minimum.

1.11 Transaction Server

The software shall be able support transaction server in Extensible Markup Laguage format (XML). The software shall be able to integrate with third party software by transmitting the transaction data in XML format to the software that require those transactions data for other function. The software shall allow user to configure the port and the destination IP before the software can begin to transfer the transaction to the third party software upon transaction received from the controller.

1.12 Guard Tour

The software shall provide a real-time monitoring of guards activities, reporting if a guard

arrives early or late at designated tour stations, missing a guard tour point or taking too long to finish a tour.

The guard tour check points are defined as any of the access readers in the Access Control System, either dedicated for the guard tour system or shared with the door access system. The guard tour shall support up to 255 guard tour route with each route consisting of guard tour checkpoint which depend on how many controller that connected to the software. The software shall generate guard tour reports as a subset to the standard reports.

When programming the routes, it shall be possible to easily add, delete or move checkpoints within the route. For each route that is programmed, the user shall be able to enter a Guard ID which is equivalent to the security guard's card number, the first tour position and the time allowance to reach the first position. If this data is not entered it shall not be possible to start the tour. A late arrive or early arrive notification event transaction will be listed on the guard tour transaction list if the respective guard did not reach the check point on time.

The software shall provide the following feature when there is an emergency occur:

- If there is an emergency case, the guard can flash 3 times on the reader to trigger the Guard Tour Duress Alarm that will appear on the Online Transaction screen and also alarm list to notify other on duty guards to take immediate action.

1.13 Lift

The software shall also provide a lift control system at low-level to provide lift access control for lift cars as identified on the tender drawings. The control will allow authorised persons to traverse to authorise floors only.

To achieve this, a reader will be required within the lift car. When a person with a valid card enters the lift they shall present the card to the reader, cardholder will then be allowed to select from a floor button or the floor buttons corresponding to the floor level or floor levels he/she is authorized to gain access to. Once a floor level is selected, the lift car will carry the cardholder to the selected floor level. An unauthorized person will not be presented with any floor button for selection.

The software shall be capable of capturing the transaction of the cardholder upon flash and the transaction shall be kept in the software database, which can be retrieved for review if required.

The software shall allow user to create lift access level where lift access level is defines as the lift car access right of a cardholder when using the lift. Each lift controller is designed to cater up to a maximum of 255 lift access level only. Each lift controller shall be capable of controlling up to 64 floors per lift car.

1.14 Alarm Monitoring

The software shall be capable of providing alarm monitoring for input and output monitoring status. The software shall allow user to send alarm command on the provided I/O list. The software shall provide the following alarm command on the I/O list at a minimum:

- Arm
- Disarm
- Reset

1.14.1 Input

The software shall allow user to configure 16 digital inputs for 1 HIO board and each digital input of the HIO board can be configure as ‘Close Trigger’ mode or ‘Open Trigger’ mode.

Users are allow to select either 1 digital input only or more than 1 digital input in a zone and the mode can be ‘AND’ gate or ‘OR’ gate selection. When in AND gate selection, all of the configured digital inputs must triggered in order for the selected output to activate whereas for the OR gate selection, any of the digital input is triggered within the same zone will activate the selected output.

1.14.2 Output

The software shall allow user to configure the output as toggle mode. When in toggle mode, the output relay will trigger according to the input. The software shall also allow user to configure the output base on duration mode and the duration of the output shall up to 99 seconds.

And the software shall allow user to select more than 1 output in 1 zone. For instant, user can connect output 1 to to strobe light and output 2 to siren. Upon input triggered, these 2 devices shall activate to notify user that the particular input is triggered.

The software shall allow the zone to be configured base on time zone control and when the zone is triggered, the HIO board will send a signal and transmitted back to the software to notify user that the zone is triggered. In addition, an audible alarm shall sound and it shall be logged as transaction data which will be kept on the software database for reference. The software shall also provide user a transaction report for alarm monitoring purposes where user shall be able to view back the alarm triggered history, or to print it out directly.

1.15 Database Engine

The software database engine shall be running in Firebird SQL database. The supported version for the software database engine is firebird version v2.1 and above.

1.16 Database Download

The software shall be able to download all the setting required for door accessing to the controller via the communication link. The software shall keep all the setting in the database file. The software shall automatically prompt user of immediate downloading whenever there is a modification of setting is performed earlier.

If the software does not successfully download the setting to the controller, a 'Fail to send' notification form shall pop-up to notify user which downloading setting process is failed to send.

The software shall also provide a menu command for the user to perform the downloading setting to controller manually.

1.17 Database Upload

The software shall be able to upload back all the setting in the controller to the software for viewing and inspection purposes. This is to ensure the setting in controller is correct and at the same time is to reduce the need to check at the controller whenever problem occurs. The database upload from controller to software however does not overwrite or interrupt the software database.

1.18 Transaction Upload

The software shall be able to automatically upload the transaction record from the controller whenever the controller is detected in the communication port or upon the software start-up. The software shall automatically resume the uploading of the transaction in the controller whenever the controller is detected on the communication port. The software shall activate the PC speaker/buzzer whenever an alarm event is received during the uploading process

1.19 Controller Database

The software shall have the user interface for the user to view, enter or modify the controller setting into the database. It shall support all types of controller model even if the previous controller model selection is different from the current selection.

1.20 Door Database

The software shall have the user interface for the user to view, enter or modify the door setting into the database. Each of the doors shall be able to be represented by a logical name.

The software door database shall have the user interface to allow the user to enter or modify the door setting including but not limited to:

- Lock release time
- Open time
- Reader Type
- Card Plus Pin Time Zone

- Card Plus Pin Lockout Count
- Automatic Lock Release Time Zone
- Exit Requesting Button Time Zone
- Antipassback Time Zone
- Antipassback Lockout
- Buddy Mode Time Zone
- Access Limit
- Door Pin 1
- Door Pin 2
- Door Pin 3
- Door Pin 1 Time Zone
- Door Pin 2 Time Zone
- Door Pin 3 Time Zone
- Door Open Pin Lockout
- Check Card Expiry Date
- Fire Release Group
- Roll Call Group

1.21 Staff Database

The software staff database shall have the user interface to allow the user to enter or modify the staff setting including but not limited to:

- Staff No.
- Name
- IC No.
- Gender
- Date Of Birth
- Date Of Join
- Department
- Job
- Shift Type
- Resign
- Date Of Resign
- Card Number
- Card Type
- Pin No
- Start Date
- End Date
- Access Level
- Buddy Mode
- Buddy Mode No
- Antipassback
- Activate

- User Defined Field 1
- User Defined Field 2
- User Defined Field 3
- User Defined Field 4
- User Defined Field 5
- User Defined Field 6
- User Defined Field 7
- User Defined Field 8
- User Defined Field 9
- User Defined Field 10

The software staff database shall be able to allow user to create a maximum of six different cards for 1 staff with each of the card can have a different access level and card data configuration.

The software staff database shall provide a filtering list option in the user interface to ease the staff database viewing. The software shall allow the user to choose the filtering by:

- Name
- Card No,
- Access Level
- Job
- Department
- Shift

The software staff database shall be able to specific search for a staff in the staff database and user can select 3 methods to perform searching process:

- Staff No.
- Card No.
- Name

1.22 Time Set

The software shall support up to 255 time sets. Each of the time set shall consist of 3 time intervals.

1.23 Time Zone

The software shall support up to 255 time zones. Each of the time zones shall consist of 8 time sets to cater for a weekly basis and holiday.

1.24 Access Level

The software shall support up to 255 access level. The access level assigned on the card will decide which door can be access with a specific time zone.

1.25 Holiday

The software shall provide the Holidays to facilitate the changing of control strategies based on different holidays dates in a year. The software shall support up to 365 holidays. A holiday shall define with the following identification and configuration parameters:

- Alphanumeric name
- Date and month
- Holiday type – Yearly selection or Not Yearly selection

1.26 Audit Trails

The software shall maintain an audit trail file of all login user and system activities, and provide the ability to generate a report by user, time and date, and type of activity. The software shall allow the user to direct the audit trail report to, screen, printer or file (Portable Document Format). The audit trail feature shall record the following system events as a minimum:

- Staff added, deleted or changed.
- Controller database added, deleted or changed.
- Door database added, deleted or changed.
- Time Set added, deleted or changed.
- Time Zone added, deleted or changed.
- Access Level added, deleted or changed.
- Holiday added, deleted or changed.
- Working shift added, deleted or changed.
- Field device/points added, deleted or changed.

1.27 Location Keep Track

The software shall allow user to keep track on every staff location. The software shall make use of the existing door reader to keep track on staffs location when they flashes the card either on entry side or exit side provided with a time, date, door name, controller name, status as a minimum details to be displayed out.

1.28 Roll Call

The software shall allow user to monitor the staff that have not flash card on exit reader in a particular area. By having this roll call feature, the system shall provide user the advantages to check/count the staff number that is still occupying that area.

1.29 Fire Release

The software shall be able to allow user to configure the fire release point in a selected controller. With the point being created, the software shall also allow user to assign the selected controllers to the fire release group according to the layout of the building where the system may be implemented on multi building design. When the software received a fire input point triggered event from the controller, all the doors that under the fire release group will be automatically release.

1.30 Online Help System

The software shall provide text sensitive online help which shall be available at anytime and from any screen with a specific button press to call out the online help. The online help shall allow user to print out as a hardcopy reference

1.31 Working Shift

The software shall allow user to create and configure the working hour shift and to apply it into the staff for attendance report calculation purposes.

The software working shift shall support 2 various type of working shift as listed below:

1.31.1 Normal Shift

This section allow user to create shift setting for the company. Each staff can have different working hour as long as it is predefined. By comparing the transaction from the reader, software can automate the calculation process for total working hours, total overtime worked etc. The normal shift shall be able to allow user to configure:

- Break time period
- Minimum working hour per day
- OT claims
- OT out grace (min)

1.31.2 Roster Shift

This section allow user to create individual shift setting to be applied to roster schedule. Daily shift defines all the planned daily working hour which to be applied to yearly roster schedule. This is particularly flexible when a working changes his/her shift in a daily, weekly or monthly basic

1.32 Time Attendance & Time Attendance Report

The software shall be able to provide user a built-in time attendance module for time attendance report viewing. Before a time attendance report can be viewed, transactions collected from the controllers must be pre-processed according to the predefined normal shift or roster setting.

The software shall be able to process the transaction records based on the ‘First In Last Out’ policy and it shall allow user to configure the including but not limited to:

- Time attendance reader selection
- OT alignment
- Offset for working time and break time
- Grace time for working time and break time

The software shall be able to produce daily attendance report showing the detail of the staff attendance for the particular day. The software shall also be able to produce the monthly attendance summary report by combining the daily details to provide a statistical monthly summary for the management to review it.

The software shall be able to allow user to authorize the staff attendance working time and also assigning the reason. This action shall not interfere with the transaction database.

The software shall be able to allow user to apply leave and when the time attendance report show up, the software will not listed the applicant as absent.

The software shall be able to produce the following predefined attendance report as a minimum:

- General Report
- Early In Report
- Early Out Report
- Late In Report
- Late Out Report
- Break Early In Report
- Break Early Out Report
- Break Late In Report
- Break Late Out Report
- Absentee Report
- Incomplete Report
- Overtime Report
- Reason Report
- Not Working Report
- Time Card Report

1.33 Report

The software report shall be able to provide user the print out report as a hardcopy reference and the report shall be able to have the flexibility to convert it into Portable Document Format (.pdf)

The software report shall be able to produce the predefined report and the report shall include the following at a minimum:

- System report – Which consist most of the system information report such as connection, router, time set, time zone, controller setting, door setting, input point, IO board, alarm zone, access level, map and many more.

- Company report – Which consist most of the company information report such as user login, menu access, staff, card, department, job, holiday, leave, normal shift, shift roster, and many more.
- Guard Tour Report – Which consist most of the guard tour information report such as schedule, route, point, guard tour card, and guard tour transaction
- Daily Event Report - Which provide user the transaction report with the ability to filter by any one or more of the following parameters:
    - Start Date and End Date
    - Start Time and End Time
    - Controller
    - Door
    - Card Holder
    - Event Type (Ex: Valid Card Entry, Door Is Forced Open, Valid Pin Entry, Card Expired, Wrong Time Zone and etc)
    - Department
    - Job Position
- Daily Alarm Report – Which provide user the alarm report with the ability to filter by any one or more of the following parameters:
    - Start Date and End Date
    - Start Time and End Time
    - Controller
    - Door
    - Card Holder
    - Event Type (Ex: Controller Down, Door Is Forced Open, Door Is Left Open, Harddisk Full, I/O Board Down, Duress Alarm Is Triggered, Fire Alarm Is Triggered and etc)
    - Department
    - Job Position
- User Audit Trail Report – Which provide user the audit trail report with the ability to filter by any one or more of the following parameters:
    - Start Date and End Date
    - Start Time and End Time
    - Login User
    - Action Taken
    - Table
- Roll Call Report – Which consist most of the roll call information report such as roll call transactions and real time roll call

1.34 Export

The software shall provide user the export module to allow user to export data to be process by other application or other usage. The software export shall at least support the following types of export:

1.34.1 Export Transaction

The software shall provide user the export module to allow user to export transaction data. The export format can be at least Text format, MS Excel format, and CSV format. The export transaction shall allow user to select the output file as a single file or multiple file with. The export transaction shall also allow user to define which field to be selected as first column and so on according to the user requirement. The software export transaction must at least allow user to select the date format and time format of the exported content.

1.34.2 Export Time Attendance

The software shall provide user the export module to allow user to export time attendance data. The export format can be at least Text format and MS Excel format. The export time attendance shall allow user to select the output file as a single file or multiple file with. The export time attendance shall also allow user to define which field to be selected as first column and so on according to the user requirement. The software export time attendance must at least allow user to select the date format of the exported content

1.34.3 Export Staff

The software shall provide user the export module to allow user to export staff data. The export format can be at least Text format, MS Excel format and CSV format. The export staff shall also allow user to define which field to be selected as first column and so on according to the user requirement. The software export staff shall allow user to filter the exported content by staff, department, job and shift.

1.35 Backup

The software shall be able to allow user to perform backup operation. The software shall allow user to select the software database, transaction database, audit trail, photo files, map file and wave files at a minimum for backup purposes.

1.36 Restore

The software shall be able to allow user to perform restore operation. The supported file format must be in backup file format (.bck)

1.37 Client Status

The software shall be able to provide user an interface of client login status. This client status shall be able to show which login user is currently login into the server and at the same time shall display out the PC name, IP address, Login Type and Login Time at a minimum.

2 Integration with third party system

This section specifies the software integration that can be done with the third party software system for a one stop solution that can be offer to fulfil the need of the tender specification

2.1 Visitor Management System (VMS)

The software shall be able to integrate with the visitor management system whereby the VMS is designed to keep track of visitor coming and going out of the premises. The VMS shall allow user to enrol the visitor by utilising the existing identification card to gather some personal information such as name. Once the visitor information is gathered, the software shall be able to retrieve the information from the VMS via network where the card adding into the system database will be executed by the software. Once completed, the software shall download this visitor card to controllers and the person in charge shall issue the installed card to the visitor as a visitor access card. The access level for the visitor group shall be created on the software and this will be pre-defined in the VMS software.

3 Hardware

This section specifies the controller specification that can be offered to fulfil the need of the tender specification for project implementation purposes. The control panel specification may categorize in few section as listed below:

- Active Network: Integrated Reader come with LCD and keypad controller
- Active Network: Active Network Control Panel
- Serial Contol Panel
- Elevator Control Panel
- Hybrid Input Output (HIO) Control Panel

3.1 Active Network Controller

Integrated Reader come with LCD and Keypad Control Panel

3.1.1 Connectivity

The active network control panel shall be able to connect to the software via TCP/IP network obeying standard network protocol.

3.1.2 ActiveTransmit

The active network control panel shall be able to support active transmit. Rather than keeping the transaction event data in the memory awaiting for software to poll, active controller actively transmits the current transaction event data back to the software as it happens, meaning transaction events gets delivered and can be act upon faster. Previous generation of network controller or serial controller only support networked/RS 485 multi-drop polling architecture whereby the transactions from the controller memory depend on the software to be polled. If the implementation involve a lot of doors, the software efficiency will be reduce due to the software polling engine architecture that need to polled back the transaction one controller at a time for each bus line.

3.1.3 ActivePush Card Downloading

The active network control panel shall be able to support active push card downloading capability whereby to download a large amount of cards (10000 cards) to the control panel would only take about less than 1 minutes to complete sending.

3.1.4 ActiveCard Searching

The active network control panel shall be able to provide an optimized card searching algorithm. With this improve optimized card searching algorithm, the card authentication only takes a fraction of a second (0.3 sec) even when the controller memory is full.

3.1.5 ActiveResponse

The active network control panel shall be able to provide active response on the controller. Upon a card is presented over the reader, a response message will be return via the LCD display. Other process executions shall return the related message which will enlighten the user for knowing every event occurred in the controller.

3.1.6 ActiveDiagnose

The active network control panel shall be able to perform active diagnose on the built-in LCD. When error detected, the controller will prompts user via the built-in LCD display by displaying the error message. Not only that the control panel shall be able to display the helpline information which can be pre-loaded from the software to ease user work when he/she has difficulties on who to call for help when the system breaks down.

3.1.7 Built-In Web Server

The active network control panel shall be able to provide built-in web server. This feature shall provide an alternative IP configuration tool that allows user to configure the IP settings via standard web browser such as Firefox or Internet Explorer.

3.1.8 Upgradable Firmware via Built-In Web Server

The active network control panel shall be able to allow user to perform firmware upgrade via built-in web server in order to create flexibility to user when come to firmware upgrade where previous controller design required user to bring back the control panel for factory programming.

3.1.9 Wizard Based Configuration

The active network control panel shall be able to support wizard based configuration whereby upon the initial “report for service” signal is transmitted to the software, the wizard engine shall prompt user for a guided configuration process. This process will guide user all the way until the controller is successfully added into the software database.

3.1.10 Capacity

The active network control panel shall be able to support at least 10000 cards and 20000 transaction events. The controller shall support 255 access levels, 255 time zone, 255 time set and 365 holidays where each time set shall have a minimum of 3 time intervals.

3.1.11 Upgradable Card and Transaction Capability

The active network control panel shall be able to expand the card and transaction database up to 50000 cards and 100000 transaction events with the existing memory size that allow the controller to expand to this limit.

3.1.12 Standard IP Configuration

The active network control panel shall be able to comply with the standard TCP/IP configuration like a PC. Thus, if user can configure a PC to a network, definitely user can also configure the controller easily.

3.1.13 Adaptive Reader Location

The active network control panel shall allow user to configure the control panel unit location as IN or OUT reader as he/she wish, hence this enhance the flexibility for installation.

3.1.14 Relay Mirror Capability

The active network control panel shall support relay mirror capability in order to reduce the chances of relay aging. The control panel shall allow system administrator to configure the on-board second relay to react exactly as the first relay, this is particularly useful for double-leaf door implementation.

3.1.15 Anti Unit Swapping Capability

The active network control panel shall be able to provide 8-bits security dipswitch to prevent unit-swapping on the reader keypad display unit, without knowing the dipswitch value on the controller that mount on the secure area together with the power supply, the unit-swapping hack will no longer work.

3.1.16 Distributed Processing

The active network control panel shall be design according to the distributed processing architecture whereby the operation of the control panel shall not depend on any of the software when operating any function. The control panel shall able to possess adequate local intelligence such as reasonable CPU processing speed and RAM to operate independently without being connected to the software.

3.1.17 Watchdog

The active network control panel shall be equipped with a watchdog feature to prevent the control panel heartbeat from becoming faulty or malfunctioning by triggering the controller processor. Hence this will reduce the chances of creating controller hang issue.

3.1.18 Onboard Battery

The active network control panel shall be equipped with an onboard battery to preserve continuous running of the real time clock (RTC) during power failure. The onboard battery shall be able to preserve RTC operation for at least 30 days without power supply.

3.1.19 Onboard Memory

The active network control panel shall have a minimum of 32K Bytes of onboard memory and 256K Bytes flash memory which is to retain the database, setting and transaction events in the controller. The data in the onboard memory will still preserved even if the onboard battery fail.

3.1.20 Onboard Buzzer

The active network control panel shall be able provide an onboard buzzer to alert user when unwanted event happened.

3.1.21 Onboard Relay and Input

The active network control panel shall be able to provide 2 Relay Output and 2 Digital Input

3.1.22 Protection

The active network control panel shall be able to provide a surge protection and a reverse polarity protection from the incoming power source.

3.1.23 Antipassback

The active network control panel shall be able to support antipassback feature to prevent unauthorized person from entering the protected area by using access card from other cardholder who had already entered the area (prevent tailgating). Once the antipassback feature has been activated, card holder has to present their card on the reader everytime when they entering or exiting the area. The control panel shall be able to perform antipassback lockout by blocking the access on the cardholder if antipassback violation occurs.

3.1.24 Peer To Peer Antipassback

The active network control panel shall be able to achieve global antipassback without relying on the software. This peer to peer antipassback function resides in the controller constantly monitor each card location status change as it happens and updates accordingly to the member controllers in the antipassback group. (up to 16 controllers per antipassback group)

3.1.25 Buddy Mode

The active network control panel shall be able to support buddy mode feature whereby to enter to the protected areas, a dual cards that under the same buddy number group must be presented at the reader before entering the protected area. This is also applying when exiting from the protected area.

3.1.26 Card + Pin

The active network control panel shall be able to support card + pin feature to provide user a 2 layer authentication for a better security. With the card presented on the reader alone shall not be able to enter the protected area where user needs to enter the personal pin code as well after presenting their card. The control panel shall be able to perform a lockout on the particular user if he/she had performed number of pin trial. This is to prevent unauthorized person to use other cardholder access card but without knowing the pin, the unauthorized persons shall not be able to enter the protected area. **(For certain model only)**

3.1.27 Duress Alarm

The active network control panel shall be able to support duress alarm code when the card + pin feature is activated. When entering the specific sequence of pins, the duress alarm event shall be triggered by the controller and it will sent back to the software to notify the security guard/person in-charge at that moment to take immediate action. **(For certain model only)**

3.1.28 Reader Technologies

The active network control panel shall be able to support various types of reader technologies as follow:

- Wiegand

- HID iClass
- HID Prox
- MIFARE

3.1.29 Card Number Format

The active network control panel shall be able to support 10 digits card number format in order to reduce the chances of duplication card number issue.

3.1.30 Access Mode

The active network control panel shall be able to provide at least 3 access operation mode. The access mode can be Pin, Card and Card + Pin.
(For certain model only)

3.1.31 Door Open Time

The active network controller shall be able to provide user a maximum of 99 seconds for door open time.

3.1.32 Door Release Time

The active network control panel shall be able to provide user a maximum of 99 seconds for door release time

3.1.33 Door Open Pin

The active network control panel shall be able to support 3 sets of door open pin whereby user can access to the protected areas by entering the door open pin.

3.1.34 Exit Requesting Button

The active network control panel shall be able to provide user the exit requesting button control by time zone in a way that user can configure what time to activate or deactivate the exit requesting button.

3.1.35 Auto Lock Release

The active network control panel shall be able to support automatic lock release control by time zone in a way that user can configure what time to energize or de-energize back the lock according to the given time zone assigned to the controller.

3.1.36 Card Expiring Checking

The active network control panel shall be able to support card expiring checking where each card shall be assigned a validity period for each individual. The control panel shall perform a validity period checking when this option is enabled when validating the access of the cardholder. Card expiring checking shall not require software to be connected each time the control panel perform card validity period checking.

3.1.37 Inhibit Mode

The active network control panel shall be able to support door inhibit mode. The access operation of the door can be inhibited through software or controller that comes with

integrated reader, keypad and LCD display. Once door inhibit mode is activated, the controller shall not accept any card or pin presented by the user even though the card or pin presented is valid. User may activate this inhibit mode to certain doors in an area in case of emergency where user need to temporarily disable the area from accessing.

3.1.38 Master Card

The active network control panel shall be able to assign the card as master card type. By assigning the card into master card type, several feature that been activated such as antipassback, card + pin, and buddy mode shall be bypass/disregard where cardholder shall not require to follow the rule set by the feature.

3.1.39 Guard Tour

The active network control panel shall be able to support guard tour feature whereby user can implement this door reader as a guard tour point as well.

3.1.40 Fire Release

The active network control panel shall be able to provide a fire point input which will be connected to the fire panel. Upon fire input point is triggered and received by the software, all the controllers that have enabled the fire release feature will be automatically lock release/security off for safety purposes.

3.1.41 Time Attendance

The active network control panel shall be able to provide time attendance record to user where user can utilize the existing door access reader as a time attendance reader as well. All the time attendance record, report viewing shall be viewed and monitored from the software.

3.2 Active Network Controller

Active Network Contol Panel Board

3.2.1 Connectivity

The active network control panel shall be able to connect to the software via TCP/IP network obeying standard network protocol.

3.2.2 ActiveTransmit

The active network control panel shall be able to support active transmit. Rather than keeping the transaction event data in the memory awaiting for software to poll, active controller actively transmits the current transaction event data back to the software as it happens, meaning transaction events gets delivered and can be act upon faster. Previous generation of network control panel or serial control panel only support networked/RS 485 multi-drop polling architecture whereby the transactions from the controller memory depend on the software to be polled. If the implementation involve a

lot of doors, the software efficiency will be reduce due to the software polling engine architecture that need to polled back the transaction one controller at a time for each bus line.

3.2.3 ActivePush Card Downloading

The active network control panel shall be able to support active push card downloading capability whereby to download a large amount of cards (30000 cards) to the controller would only take about less than 5 minutes to complete sending.

3.2.4 ActiveCard Searching

The active network control panel shall be able to provide an optimized card searching algorithm. With this improve optimized card searching algorithm, the card authentication only takes a fraction of a second (0.3 sec) even when the controller memory is full.

3.2.5 Built-In Web Server

The active network control panel shall be able to provide built-in web server. This feature shall provide an alternative IP configuration tool that allows user to configure the IP settings via standard web browser such as Firefox or Internet Explorer.

3.2.6 Upgradable Firmware via Built-In Web Server and Software

The active network control panel shall be able to allow user to perform firmware upgrade via built-in web server or in the software. This is to create flexibility to user when come to firmware upgrade where previous control panel design required user to bring back the control panel for factory programming.

3.2.7 Wizard Based Configuration

The active network control panel shall be able to support wizard based configuration whereby upon the initial “report for service” signal is transmitted to the software, the wizard engine shall prompt user for a guided configuration process. This process will guide user all the way until the controller is successfully added into the software database.

3.2.8 Capacity

The active network control panel shall be able to support at least 30000 cards and 80000 transaction events.
(For certain model only)

3.2.9 Time Set, Time Zone and Access Level (Access Group)

The active network control panel shall be able to support unlimited time set, time zone and access level in the system
(For certain model only)

3.2.10 Wiegand Format

The active network control panel shall be able to support multiple wiegand bit (default) inclusive of:

- 26 bit
- 32 bit
- 34 bit
- 35 bit
- 37 bit

3.2.11 Wiegand Group

The active network control panel shall be able to allow user to create custom wiegand format in the software. The control panel shall support the reading bit from 0 to 64 bit. This feature is suitable for special card formart such as HID corporate 1000 cards whereby some end-user do not wish to expose their card reading format to third party.

3.2.12 Dynamic Storage Allocation

The active network control panel shall be able to allow user to modify the factory preset card holder (30,000 cards) and event (80,000 transaction events) storage database whenever necessary. Result of this modification leads more personalized usage of control panel whenever needed. Ex: User can modify the card holder to 10,000 cards and transaction event to 100,000 events.

(For certain model only)

3.2.13 Door Interlocking

The active network control panel shall be able to support single-board interlocking and cross-board interlocking:

- Single-board Interlocking – 2 in doors interlocking within the control panel, no external wiring is needed.
- Cross-board Interlocking – Cross-board interlocking is achievable by checking the interlocking signal coming from second control panel befare granting the accessibility to the local control panel.

(For certain model only)

3.2.14 Advance Encryption Standard – (AES 128 bits)

The active network control panel shall be able to support AES 128 bits. AES 128 is an encryption algorithm for data securing purposes. Once the AES 128 feature has been activated in both software and active network control panel, if happen that the server has been cloned by unauthorized person. All the connected control panel will halt transmitting the transaction event back to the software in order prevent data sniffing.

3.2.15 Event Based Relay Trigger

The active network control panel shall be able to support event based relay trigger. This feature allow user to trigger or un-trigger a relay whenever a specific event occurs. It can support up to 10 sets of events. User can freely assign any specific event to trigger or un-trigger any onboard relay output.
(For certain model only)

3.2.16 HID AGK (keypad reader)

The active network control panel shall be able to support HID AGK keypad reader as followed:

- AGK 00
- AGK 09
- AGK 10
- AGK 11
- AGK 14
- AGK 19
- AGK 20

(Note: This feature is only applicable for HID keypad reader)

3.2.17 Standard IP Configuration

The active network control panel shall be able to comply with the standard TCP/IP configuration like a PC. Thus, if user can configure a PC to a network, definitely user can also configure the controller easily.

3.2.18 Distributed Processing

The active network control panel shall be design according to the distributed processing architecture whereby the operation of the control panel shall not depend on any of the software when operating any function. The control panel shall able to possess adequate local intelligence such as reasonable CPU processing speed and RAM to operate independently without being connected to the software.

3.2.19 Watchdog

The active network control panel shall be equipped with a watchdog feature to prevent the control panel heartbeat from becoming faulty or malfunctioning by triggering the control panel processor. Hence this will reduce the chances of creating control panel hang issue.

3.2.20 Onboard Battery

The active network controller shall be equipped with an onboard battery to preserve continuous running of the real time clock (RTC) during power failure. The onboard battery shall be able to preserve RTC operation for at least 30 days without power supply.

3.2.21 Onboard Memory

The active network controller shall have a minimum of 32K Bytes of onboard memory and 256K Bytes flash memory which is to retain the database, setting and transaction events in the controller. The data in the onboard memory will still preserved even if the onboard battery fail.

3.2.22 Onboard Buzzer

The active network control panel shall be able provide an onboard buzzer to alert user when unwanted event happened.

3.2.23 Onboard Relay and Input

The active network control panel shall be able to provide 4 Relay Output and 8 Configurable Input whether analog or digital.

3.2.24 Reader Input

The active network control panel shall be able to provide up to 2 Reader Input for any third party reader in wiegand format

3.2.25 Reader Tampered Monitoring

The active network control panel shall be able to monitor each reader status whether the reader is being tampered by unauthorized person by sending an event notification back to the software to alert the person incharge

(Note: This feature is only applicable for third party reader that have tamper output)

3.2.26 Reader LED and Buzzer Input

The active network control panel shall be able to provide third party reader to connect the LED and Buzzer output to control panel in order to control the reader LED and Buzzer upon certain events. Example: when the door is forced open by unauthorized person, the control panel onboard buzzer and the reader buzzer shall be activated.

(Note: This feature is only applicable for third party reader that have LED and Buzzer output)

3.2.27 AC Fail Monitoring

The active network control panel shall be able to notify the software when AC power fail.

3.2.28 Backup Battery Monitoring

The active network control panel shall be able to notify the software on the controller backup battery status right after AC power fail.

3.2.29 Protection

The active network control panel shall be able to provide a surge protection and a

reverse polarity protection from the incoming power source and the surge protection from reader input.

3.2.30 Antipassback

The active network control panel shall be able to support antipassback feature to prevent unauthorized person from entering the protected area by using access card from other cardholder who had already entered the area (prevent tailgating). Once the antipassback feature has been activated, card holder has to present their card on the reader everytime when they entering or exiting the area. The control panel shall be able to perform antipassback lockout by blocking the access on the cardholder if antipassback violation occurs.

3.2.31 Peer To Peer Antipassback

The active network control panel shall be able to achieve global antipassback without relying on the software. This peer to peer antipassback function resides in the controller constantly monitor each card location status change as it happens and updates accordingly to the member controllers in the antipassback group. (up to 16 controllers per antipassback group)

3.2.32 Buddy Mode

The active network control panel shall be able to support buddy mode feature whereby to enter to the protected areas, a dual cards that under the same buddy number group must be presented at the reader before entering the protected area. This is also applying when exiting from the protected area.

3.2.33 Card + Pin

The active network control panel shall be able to support card + pin feature to provide user a 2 layer authentication for a better security. With the card presented on the reader alone shall not be able to enter the protected area where user needs to enter the personal pin code as well after presenting their card. The controller shall be able to perform a lockout on the particular user if he/she had performed number of pin trial. This is to prevent unauthorized person to use other cardholder access card but without knowing the pin, the unauthorized persons shall not be able to enter the protected area.
(Note: This feature is only applicable for keypad reader)

3.2.34 Keyed Card + Pin

The active network control panel shall be able to support keyed card + pin feature. Upon activated, user will be able to key in the card serial number together with the personal pin number to access to the area even without presenting the valid card.
(Note: This feature is only applicable for keypad reader)

3.2.35 Access Limit

The active network control panel shall be able to provide access limit feature. Upon

activated, the cardholder shall not able to access to the area when the access limit is full.

3.2.36 Duress Alarm

The active network control panel shall be able to support duress alarm code when the card + pin feature is activated. When entering the specific sequence of pins, the duress alarm event shall be triggered by the controller and it will sent back to the software to notify the security guard/person in-charge at that moment to take immediate action.

3.2.37 Operation Mode

The active network control panel shall be able to support several mode of profile which depends on the usage. The mode of profile shall include but not limited to:

- 2 Doors
- IN and OUT Reader
- IN and OUT Barrier
- 2 Turnstiles
- IN and OUT Turnstile
- 4 Doors
- 2x IN and OUT Reader
- 2x IN and OUT Barrier
- 4 Turnstiles
- 2x IN and OUT Turnstile

(For certain model only)

3.2.38 Reader Technologies

The active network control panel shall be able to support various types of reader technologies as follow:

- Wiegand
- HID iClass
- HID Prox
- MIFARE
- SUPREMA biometric

3.2.39 Card Number Format

The active network control panel shall be able to support 10 digits card number format in order to reduce the chances of duplication card number issue.

3.2.40 Door Open Time

The active network control panel shall be able to provide user a maximum of 99 seconds for door open time.

3.2.41 Door Release Time

The active network control panel shall be able to provide user a maximum of 99 seconds for door release time

3.2.42 Door Open Pin

The active network control panel shall be able to support 3 sets of door open pin whereby user can access to the protected areas by entering the door open pin.

3.2.43 Exit Requesting Button

The active network control panel shall be able to provide user the exit requesting button control by time zone in a way that user can configure what time to activate or deactivate the exit requesting button.

3.2.44 Auto Lock Release

The active network control panel shall be able to support automatic lock release control by time zone in a way that user can configure what time to energize or de-energize back the lock according to the given time zone assigned to the controller.

3.2.45 Card Expiring Checking

The active network control panel shall be able to support card expiring checking where each card shall be assigned a validity period for each individual. The control panel shall perform a validity period checking when this option is enabled when validating the access of the cardholder. Card expiring checking shall not require software to be connected each time the control panel perform card validity period checking.

3.2.46 Inhibit Mode

The active network control panel shall be able to support door inhibit mode. The access operation of the door can be inhibited through software or controller that comes with integrated reader, keypad and LCD display. Once door inhibit mode is activated, the controller shall not accept any card or pin presented by the user even though the card or pin presented is valid. User may activate this inhibit mode to certain doors in an area in case of emergency where user need to temporarily disable the area from accessing.

3.2.47 Master Card

The active network control panel shall be able to assign the card as master card type. By assigning the card into master card type, several feature that been activated such as antipassback, card + pin, and buddy mode shall be bypass/disregard where cardholder shall not require to follow the rule set by the feature.

3.2.48 Maintenance Card

The active network control panel shall be able to assign the card as maintenance card type. This card is mainly for reader maintenance purpose. Especially when the reader is being tampered, the person incharge need to present the maintenance card on the reader to stop the reader buzzer and control panel onboard buzzer from activating while

checking the reader condition. Upon maintenance card presented on the reader, an event notification will be updated in the software as well.

3.2.49 Guard Tour

The active network control panel shall be able to support guard tour feature whereby user can implement this door reader as a guard tour point as well.

3.2.50 Fire Release

The active network control panel shall be able to provide a fire point input which will be connected to the fire panel. Upon fire input point is triggered and received by the software, all the control panel that have enabled the fire release feature will be automatically lock release/security off for safety purposes. The fire release feature can be categorized in group.

3.2.51 Time Attendance

The active network control panel shall be able to provide time attendance record to user where user can utilize the existing door access reader as a time attendance reader as well. All the time attendance record, report viewing shall be viewed and monitored from the software.

3.3 Serial Control Panel

3.3.1 Connectivity

The serial control panel shall be able to connect to the software via RS 485 (2 wire) or RS 232. The wiring topology for serial controller shall be connected in daisy chain looping.

3.3.2 Distributed Processing

The serial control panel shall be design according to the distributed processing architecture whereby the operation of the control panel shall not depend on any of the software when operating any function. The control panel shall able to possess adequate local intelligence such as reasonable CPU processing speed and RAM to operate independently without being connected to the software.

3.3.3 Upgradable Firmware via Software

The serial control panel shall be able to allow user to perform firmware upgrade via software. This is to create flexibility to user when come to firmware upgrade where previous control panel design required user to bring back the control panel for factory programming.

3.3.4 Capacity

The serial control panel shall be able to support at least 30000 cards and 80000 transaction events.

(For certain model only)

3.3.5 Time Set, Time Zone and Access Level (Access Group)

The serial control panel panel shall be able to support unlimited time set, time zone and access level in the system

(For certain model only)

3.3.6 Wiegand Format

The serial control panel shall be able to support multiple wiegand bit (default) inclusive of:

- 26 bit
- 32 bit
- 34 bit
- 35 bit
- 37 bit

3.3.7 Wiegand Group

The serial control panel shall be able to allow user to create custom wiegand format in the software. The control panel shall support the reading bit from 0 to 64 bit. This feature is suitable for special card formart such as HID corporate 1000 cards whereby some end-user do not wish to expose their card reading format to third party.

3.3.8 Dynamic Storage Allocation

The serial control panel shall be able to allow user to modify the factory preset card holder (30,000 cards) and event (80,000 transaction events) storage database whenever necessary. Result of this modification leads more personalized usage of control panel whenever needed. Ex: User can modify the card holder to 10,000 cards and transaction event to 100,000 events.

(For certain model only)

3.3.9 Door Interlocking

The serial control panel shall be able to support single-board interlocking and cross-board interlocking:

- Single-board Interlocking – 2 in doors interlocking within the control panel, no external wiring is needed.
- Cross-board Interlocking – Cross-board interlocking is achievable by checking the interlocking signal coming from second control panel befare granting the accessibility to the local control panel.

(For certain model only)

3.3.10 Event Based Relay Trigger

The serial control panel shall be able to support event based relay trigger. This feature allow user to trigger or un-trigger a relay whenever a specific event occurs. It can support up to 10 sets of events. User can freely assign any specific event to trigger or un-trigger any onboard relay output.

(For certain model only)

3.3.11 HID AGK (keypad reader)

The serial control panel shall be able to support HID AGK keypad reader as followed:

- AGK 00
- AGK 09
- AGK 10
- AGK 11
- AGK 14
- AGK 19
- AGK 20

(Note: This feature is only applicable for HID keypad reader)

3.3.12 Watchdog

The serial control panel shall be equipped with a watchdog feature to prevent the control panel heartbeat from becoming faulty or malfunctioning by triggering the control panel processor. Hence this will reduce the chances of creating control panel hang issue.

3.3.13 Onboard Battery

The serial control panel shall be equipped with an onboard battery to preserve continuous running of the real time clock (RTC) during power failure. The onboard battery shall be able to preserve RTC operation for at least 30 days without power supply.

3.3.14 Onboard Memory

The serial control panel shall have a minimum of 32K Bytes of onboard memory and 256K Bytes flash memory which is to retain the database, setting and transaction events in the controller. The data in the onboard memory will still preserved even if the onboard battery fail.

3.3.15 Onboard Buzzer

The serial control panel shall be able provide an onboard buzzer to alert user when unwanted event happened.

3.3.16 Reader Input

The serial control panel shall be able to provide up to 2 Reader Input for any third party reader in wiegand format

3.3.17 Reader Tampered Monitoring

The serial control panel shall be able to monitor each reader status whether the reader is being tampered by unauthorized person by sending an event notification back to the software to alert the person incharge

(Note: This feature is only applicable for third party reader that have tamper output)

3.3.18 Reader LED and Buzzer Input

The serial control panel shall be able to provide third party reader to connect the LED and Buzzer output to control panel in order to control the reader LED and Buzzer upon certain events. Example: when the door is forced open by unauthorized person, the control panel onboard buzzer and the reader buzzer shall be activated.

(Note: This feature is only applicable for third party reader that have LED and Buzzer output)

3.3.19 AC Fail Monitoring

The serial control panel shall be able to notify the software when AC power fail.

3.3.20 Backup Battery Monitoring

The serial control panel shall be able to notify the software on the controller backup battery status right after AC power fail.

3.3.21 Protection

The serial control panel shall be able to provide a surge protection and a reverse polarity protection from the incoming power source and the surge protection from reader input.

3.3.22 Antipassback

The serial control panel shall be able to support antipassback feature to prevent unauthorized person from entering the protected area by using access card from other cardholder who had already entered the area (prevent tailgating). Once the antipassback feature has been activated, card holder has to present their card on the reader everytime when they entering or exiting the area. The controller shall be able to perform antipassback lockout by blocking the access on the cardholder if antipassback violation occurs.. This antipassback feature shall not be limited to one door. Instead, this feature shall be applicable to doors globally across the whole system with the software support.

3.3.23 Buddy Mode

The serial control panel shall be able to support buddy mode feature whereby to enter to the protected areas, a dual cards that under the same buddy number group must be

presented at the reader before entering the protected area. This is also applying when exiting from the protected area.

3.3.24 Card + Pin

The serial control panel shall be able to support card + pin feature to provide user a 2 layer authentication for a better security. With the card presented on the reader alone shall not be able to enter the protected area where user needs to enter the personal pin code as well after presenting their card. The controller shall be able to perform a lockout on the particular user if he/she had performed number of pin trial. This is to prevent unauthorized person to use other cardholder access card but without knowing the pin, the unauthorized persons shall not be able to enter the protected area.

(Note: This feature is only applicable for keypad reader)

3.3.25 Keyed Card + Pin

The serial control panel shall be able to support keyed card + pin feature. Upon activated, user will be able to key in the card serial number together with the personal pin number to access to the area even without presenting the valid card.

(Note: This feature is only applicable for keypad reader)

3.3.26 Access Limit

The serial control panel shall be able to provide access limit feature. Upon activated, the cardholder shall not able to access to the area when the access limit is full.

3.3.27 Duress Alarm

The serial control panel shall be able to support duress alarm code when the card + pin feature is activated. When entering the specific sequence of pins, the duress alarm event shall be triggered by the controller and it will sent back to the software to notify the security guard/person in-charge at that moment to take immediate action.

3.3.28 Operation Mode

The serial control panel shall be able to support several mode of profile which depends on the usage. The mode of profile shall include but not limited to:

- 2 Doors
- IN and OUT Reader
- IN and OUT Barrier
- 2 Turnstiles
- IN and OUT Turnstile
- 4 Doors
- 2x IN and OUT Reader
- 2x IN and OUT Barrier
- 4 Turnstiles
- 2x IN and OUT Turnstile

(For certain model only)

3.3.29 Reader Technologies

The serial control panel shall be able to support various types of reader technologies as follow:

- Wiegand
- HID iClass
- HID Prox
- MIFARE
- SUPREMA biometric

3.3.30 Card Number Format

The serial control panel shall be able to support 10 digits card number format in order to reduce the chances of duplication card number issue.

3.3.31 Door Open Time

The serial control panel shall be able to provide user a maximum of 99 seconds for door open time.

3.3.32 Door Release Time

The serial control panel shall be able to provide user a maximum of 99 seconds for door release time

3.3.33 Door Open Pin

The serial control panel shall be able to support 3 sets of door open pin whereby user can access to the protected areas by entering the door open pin.

3.3.34 Exit Requesting Button

The serial control panel shall be able to provide user the exit requesting button control by time zone in a way that user can configure what time to activate or deactivate the exit requesting button.

3.3.35 Auto Lock Release

The serial control panel shall be able to support automatic lock release control by time zone in a way that user can configure what time to energize or de-energize back the lock according to the given time zone assigned to the controller.

3.3.36 Card Expiring Checking

The serial control panel shall be able to support card expiring checking where each card shall be assigned a validity period for each individual. The control panel shall perform a validity period checking when this option is enabled when validating the access of the cardholder. Card expiring checking shall not require software to be connected each time the control panel perform card validity period checking.

3.3.37 Inhibit Mode

The serial control panel shall be able to support door inhibit mode. The access operation of the door can be inhibited through software or controller that comes with integrated reader, keypad and LCD display. Once door inhibit mode is activated, the controller shall not accept any card or pin presented by the user even though the card or pin presented is valid. User may activate this inhibit mode to certain doors in an area in case of emergency where user need to temporarily disable the area from accessing.

3.3.38 Master Card

The serial control panel shall be able to assign the card as master card type. By assigning the card into master card type, several feature that been activated such as antipassback, card + pin, and buddy mode shall be bypass/disregard where cardholder shall not require to follow the rule set by the feature.

3.3.39 Maintenance Card

The serial control panel shall be able to assign the card as maintenance card type. This card is mainly for reader maintenance purpose. Especially when the reader is being tampered, the person incharge need to present the maintenance card on the reader to stop the reader buzzer and control panel onboard buzzer from activating while checking the reader condition. Upon maintenance card presented on the reader, an event notification will be updated in the software as well.

3.3.40 Guard Tour

The serial control panel shall be able to support guard tour feature whereby user can implement this door reader as a guard tour point as well.

3.3.41 Fire Release

The serial control panel shall be able to provide a fire point input which will be connected to the fire panel. Upon fire input point is triggered and received by the software, all the control panel that have enabled the fire release feature will be automatically lock release/security off for safety purposes. The fire release feature can be categorized in group.

3.3.42 Time Attendance

The serial control panel shall be able to provide time attendance record to user where user can utilize the existing door access reader as a time attendance reader as well. All the time attendance record, report viewing shall be viewed and monitored from the software.

3.4 Elevator Control Panel

3.4.1 Connectivity

The elevator control panel shall be able to provide 2 RS 485 (2wire) communication as below:

- First communication is from elevator control panel to software
- Second communication is from elevator control panel to Hybrid Input Output Control Panel (HIO)

3.4.2 Supported Floor

The elevator control panel shall be able to support 8 floors (onboard) and a maximum of 136 floors with the help of HIO control panel

3.4.3 Supported HIO

The elevator control panel shall be able to communicate with up to 8 HIO control panel where each of the HIO control panel provide 8 digital outputs or 16 digital outputs with the add-in expansion board

3.4.4 Time Set, Time Zone, Floor Access Level and Lift Access Level

The elevator control panel shall be able to support up to 255 sets of time set, time zone, floor access level and lift access level.

3.4.5 Individual Floor Bypass Control

The elevator control panel shall be able to support individual floor bypass base on time zone control.

3.4.6 Emergency Bypass

The elevator control panel shall be able to support emergency bypass by key switch or by software when the control panel is not working.

3.4.7 Capacity

The elevator control panel shall be able to support at least 30000 cards and 80000 transaction events.

3.4.8 Output

The elevator control panel shall be able to provide NO (normally open) and NC (normally close) contact.

3.4.9 Floor Button Turn On Control

The elevator control panel shall be able to provide user a maximum of 99 seconds for button turn on time.

3.4.10 Distributed Processing

The elevator control panel shall be design according to the distributed processing architecture whereby the operation of the control panel shall not depend on any of the software when operating any function. The control panel shall able to possess adequate local intelligence such as reasonable CPU processing speed and RAM to operate independently without being connected to the software.

3.4.11 Upgradable Firmware via Software

The elevator control panel shall be able to allow user to perform firmware upgrade via software. This is to create flexibility to user when come to firmware upgrade where previous control panel design required user to bring back the control panel for factory programming.

3.4.12 Wiegand Format

The elevator control panel shall be able to support multiple wiegand bit (default) inclusive of:

- 26 bit
- 32 bit
- 34 bit
- 35 bit
- 37 bit

3.4.13 Wiegand Group

The elevator control panel shall be able to allow user to create custom wiegand format in the software. The control panel shall support the reading bit from 0 to 64 bit. This feature is suitable for special card formart such as HID corporate 1000 cards whereby some end-user do not wish to expose their card reading format to third party.

3.4.14 Watchdog

The elevator control panel shall be equipped with a watchdog feature to prevent the control panel heartbeat from becoming faulty or malfunctioning by triggering the control panel processor. Hence this will reduce the chances of creating control panel hang issue.

3.4.15 Onboard Battery

The elevator control panel shall be equipped with an onboard battery to preserve continuous running of the real time clock (RTC) during power failure. The onboard battery shall be able to preserve RTC operation for at least 30 days without power supply.

3.4.16 Onboard Memory

The elevator control panel shall have a minimum of 32K Bytes of onboard memory and 256K Bytes flash memory which is to retain the database, setting and transaction events

in the controller. The data in the onboard memory will still preserved even if the onboard battery fail.

3.4.17 Onboard Buzzer

The elevator control panel shall be able provide an onboard buzzer.

3.4.18 Reader Input

The elevator control panel shall be able to provide up to 4 Reader Input for any third party reader in wiegand format

3.4.19 Reader LED and Buzzer Input

The elevator control panel shall be able to provide third party reader to connect the LED and Buzzer output to control panel in order to control the reader LED and Buzzer.

3.4.20 AC Fail Monitoring

The elevator control panel shall be able to notify the software when AC power fail.

3.4.21 Backup Battery Monitoring

The elevator control panel shall be able to notify the software on the controller backup battery status right after AC power fail.

3.4.22 Protection

The elevator control panel shall be able to provide a surge protection and a reverse polarity protection from the incoming power source and the surge protection from reader input.

3.4.23 Reader Technologies

The elevator control panel shall be able to support various types of reader technologies as follow:

- Wiegand
- HID iClass
- HID Prox
- MIFARE
- SUPREMA biometric

3.4.24 Card Number Format

The elevator control panel shall be able to support 10 digits card number format in order to reduce the chances of duplication card number issue.

3.4.25 Card Expiring Checking

The elevator control panel shall be able to support card expiring checking where each card shall be assigned a validity period for each individual. The control panel shall perform a validity period checking when this option is enabled when validating the

access of the cardholder. Card expiring checking shall not require software to be connected each time the control panel perform card validity period checking.

3.5 Hybrid Input Output (HIO) Control Panel

3.5.1 Connectivity

The HIO control panel shall be able to connect to the software via RS 485 (2 wire) or TCP/IP network.

3.5.2 Distributed Processing

The HIO control panel shall be design according to the distributed processing architecture whereby the operation of the HIO shall not depend on any of the software when operating any function. The HIO shall able to possess adequate local intelligence such as reasonable CPU processing speed and RAM to operate independently without being connected to the software.

3.5.3 Watchdog

The HIO control panel shall be equipped with a watchdog feature to prevent the HIO heartbeat from becoming faulty or malfunctioning by triggering the HIO processor. Hence this will reduce the chances of creating HIO controller hang issue.

3.5.4 Onboard Battery

The HIO control panel shall be equipped with an onboard battery to preserve continuous running of the real time clock (RTC) during power failure. The onboard battery shall be able to preserve the memory and RTC operation for at least 30 days without power supply.

3.5.5 Onboard Memory

The HIO control panel shall have a minimum of 32K Bytes of onboard memory and 256K Bytes flash memory which is to retain the setting and transaction events in the controller.

3.5.6 Protection

The HIO control panel shall be able to provide a surge protection and a reverse polarity protection from the incoming power source.

3.5.7 Communication Protocol

The HIO control panel shall support MODBUS serial or MODBUS TCP.

3.5.8 MODBUS Mode

The HIO control panel shall support Serial Slave or TCP slave or TCP active communication mode with the software

3.5.9 ActiveTransmit

The HIO control panel shall be able to support active transmit when running in TCP active communication. Rather than keeping the transaction event data in the memory awaiting for software to poll, HIO actively transmits the current transaction event data back to the software as it happens, meaning transaction events gets delivered and can be act upon faster.

3.5.10 Built-In Web Server

The HIO control panel shall be able to provide built-in web server. This feature shall provide an alternative IP configuration tool that allows user to configure the IP settings. The HIO control panel shall also able to allow user to configure serial setting such as baud rate, data bits, flow control, parity and stop bits via standard web browser such as Firefox or Internet Explorer.

3.5.11 Upgradable Firmware via Built-In Web Server

The HIO control panel shall be able to allow user to perform firmware upgrade via built-in web server in order to create flexibility to user when come to firmware upgrade where previous design required user to bring back for factory programming.

3.5.12 Capacity

The HIO control panel shall be able to support at least 20000 transaction events.

3.5.13 Time set & Time zone

The HIO control panel shall be able to support 255 time zone and 255 time set where each time set shall have a minimum of 3 time intervals.

3.5.14 Arm and Disarm

The HIO control panel shall be able to allow the time zone and time set to arm or disarm each configured zone by user preference. Not only that, the arm or disarm can also be manually performed.

3.5.15 Standard IP Configuration

The HIO control panel shall be able to comply with the standard TCP/IP configuration like a PC. Thus, if user can configure a PC to a network, definitely user can also configure the HIO easily.

3.5.16 Unit Address

The HIO control panel shall be able to support 1 to 31 units addressing during modbus communication. The HIO control panel shall be able to continuously update new unit address for every 3 second without resetting the controller.

3.5.17 Input

The HIO control panel shall be able to provide a total of 8 sets digital input for user configuration and it can be expandable to 16 sets of digital input when daughter board is

connected. The HIO control panel shall also be able to provide input LED indicator whereby the indicator will be functional when setting is applied and the LED indicator will turn ON when the input is triggered.

3.5.18 Input Mode

The HIO control panel shall be able to allow user to select the input either in 'Open Trigger' or 'Close Trigger' mode.

3.5.19 AND or OR selection

The HIO control panel shall be able to allow user to configure the input to 'either point triggered' or 'all point triggered' combination across difference zone.

3.5.20 Output

The HIO control panel shall be able to provide a total of 8 sets digital output for user configuration and it can be expandable to 16 sets of digital output when daughter board is connected. The HIO control panel shall also be able to provide output relay LED indicators and each relay is provided with normally close (NC) and normally open (NO) output relay selection.

3.5.21 Output Trigger Selection

The HIO control panel shall be able to provide 2 types of trigger function:

- Toggle Mode trigger function. If the input trigger, the output will follow trigger as well.
- Alarm Mode trigger function. Once the input trigger, the output will trigger ON and OFF with duration.

3.5.22 Output Relay Duration

The HIO control panel output relay with duration is 99 seconds maximum or without duration which is 0 second to indicate permanent ON/Trigger.

3.5.23 Onboard Coldstart and Factory Default

The HIO control panel shall allow user to perform coldstart and factory default on the board itself without relying on other device to perform the following process.

4 Overall System Hardware Components

This section specifies the overall system hardware components needed when come to implementation as listed below:

4.1 For Door Access System

- Access Control System Software that dedicated for the centralized security management.
- Door Access Controller to control and monitor the door access activity
- Card Reader for entry side and exit side (optional) depending on the reader technology that user required and the reader can also come with keypad or display type if user require pin as well to access.
- Electromagnetic Lock to secure the door. User will require 2 Electromagnetic lock when the door is double leaf type.
- Magnetic Contacts to provide the door status either in door open status or door close status
- Exit Requesting Button

4.2 For Car Park Access System

- Access Control System Software that dedicated for the centralized security management.
- Car Park Controller to control and monitor the car park barrier.
- Card Reader for entry lane and exit lane depending on the reader technology that user required.
- Barrier gate
- Vehicle loop detector
- Exit Requesting Button

4.3 For Lift Access System

- Access Control System Software that dedicated for the centralized security management.
- Lift Access Controller to control the floor access activity
- HIO controller depending on how many floor buttons to be controlled.
- Card Reader depending on the reader technology that user required

4.4 For Alarm Monitoring System

- Access Control System Software that dedicated for the centralized security management.
- HIO controller depending on how many alarm point to be monitored.

- Magnetic contact, strobe light, siren, passive infrared sensor and etc are all optional components depending on the user requirement.

5 Computer Requirement

This section specifies the computer requirement that needed to fulfil the software requirement. The computer specification may categorize in 2 sections as listed below:

5.1 High range requirement (Server machine)

- Processor: Single Quad-Core Intel Xeon Processor 5400 series at up to 3.33GHz OR equivalent
- Minimum Memory: 4GB
- Hard Disk Space: 500GB
- Operating System:
  - Windows XP Professional
  - Windows 2000 Workstation
  - Windows 2000 Server
  - Windows 2003 Standard Server
  - Windows 2003 Advanced Server
  - Windows 2008 Server
  - Windows Vista Home Premium
  - Windows Vista Business
  - Windows Vista Ultimate
  - Windows Vista Home Basic
  - Windows 7
- Optimum Screen Resolution: 1024 x 768
- Graphic adapter: 32MB
- Media Device: 48x DVD/CD-ROM Drive
- Network Device: 10/100 Base T Network Adapter

Optional Peripherals:

- A sound card to play alerts when an alarm event occurred
- A printer to print reports

5.2 Medium range requirement

- Processor: Pentium intel core i5 or i7
- Hard Disk Space: 200GB
- Operating System:
  - Windows XP Professional

  - Windows 2000 Workstation
  - Windows 2000 Server
  - Windows 2003 Standard Server
  - Windows 2003 Advanced Server
  - Windows Vista Home Premium
  - Windows Vista Business
  - Windows Vista Ultimate
  - Windows Vista Home Basic
  - Windows 7
- Optimum Screen Resolution: 1024 x 768
- Graphic adapter: 32MB
- Media Device: 48x DVD/CD-ROM Drive
- Network Device: 10/100 Base T Network Adapter

Optional Peripherals:

- A sound card to play alerts when an alarm event occurred
- A printer to print reports