SECURITY AND ACCESS CONTROL SYSTEM SPECIFICATION

Control Equipment Hardware.

Ref: PC 28/7/2009

TABLE OF CONTENT

A General Tender Requirements

1. The tender person shall include for the design, cost estimation, supply, installation, commissioning of the system as specified, and all the wiring and door locking devices. The system shall broadly comprise the following:

    a. Central Control System c/w surge protection system, monitor, remote control Door open and all accessories.

    b. Door controllers and door functions.

    c. Readers, door monitoring contacts and exit switches.

2. The tender shall provide a complete and functional system, which including Power Supply Unit c/q, Standby Battery c/w battery charger, User ID Cards c/w all accessories. All cabling and accessories for complete installation, Painting and labelling. The tender person has to be familiar with all the system requirements and installation.

3. The tender person shall seek clarification of any relevant matters such as Access Controller Unit c/w Programmable Time Zone, PIN Numbers programming, Anti-Passback System, Door Alarm Outputs and all accessories

4. The tender person shall demonstrate his competence with the equipment he is tendering by either:
    a. The tender person shall obtain a letter of signature by the company director or the trainer from the original equipment manufacturer. The letter must state the name of the tendering company and a statement that who had sufficient competence to install the tendered equipment

    b. The tender person shall provide proof in the form of training certificates from the original equipment manufacturer. Certificates will contain named individuals and the course applicable to the equipment being tendered. The named individuals must be employed by the tenderer and play an active part in the installation of equipment.

5. The tender person shall submit their tender at (insert where tender shall be sent or handed) by (insert time and date of closing).

B General System Requirement

1. System Equipment

a. Supply of Equipment
   i. Each item of equipment supplied shall be a standard product of an established, reputable manufacturer. Custom hardware and/or custom operating firmware will not be acceptable.

b. Host PC
   i. The system must provide an option for connection to a host PC, however full system functionality must be maintained with or without the Host PC connected.

c. Integration
   i. The system shall be a single integrated access control and alarm monitoring system. The system shall also provide integrated control of lighting, heating, ventilation, air-conditioning and other custom applications as required

d. Modular design
   i. The system shall be of a modular hardware design allowing for detection and control devices to be connected to system modules within their immediate vicinity and also providing for expansion and modification of the system to meet future requirements.

2. Power Supply

a. AC Mains Supply Voltage.
   i. All field equipment powered from the AC mains supply shall operate on a supply of 240V AC +/-10%. (Terminal voltage at input to Transformer or Plug pack)

b. DC Supply Voltage
   i. All field equipment powered from a separate DC power supply shall operate on a nominal supply of 12V DC. Normal operation shall be maintained over a supply range of 11V to 14V DC.

c. Batteries
   i. All field equipment powered from the AC Mains supply shall incorporate a dedicated connection for a re-chargeable Sealed Lead Acid battery of at least 12.7 AH capacity to provide backup power in the event of Mains supply failure. The equipment shall provide a suitable circuit to charge the batteries during normal operation.

d. Power Detection
    i. The equipment shall include detection for power failure, low battery status and low battery Cut-off State. During power failure it will send a signal back to reports there was a power failure occurs at which controller.
    ii. If the backup battery run low, it shall provides signal to consul to indicate low battery status.
    iii. In the events of power failure and battery low state of lower than 10.6V, the controller shall release the door locks and reports it status. Every events of detection shall records in the system includes date, time, which unit and status.

3. Cabling

a. For the connection of readers to door controllers then the following sized cables shall be used:
    i. For distances up to 250 metres - 0.22 mm
    ii. For distances up to 500 metres - 0.5 mm
    iii. For distances up to 1000 metres - 1.0 mm

b. Alarm monitoring inputs shall be wired using dual end-of-line resistors installed at the detection device such that the system can monitor Seal, Alarm (Un-seal), Open Circuit (Tamper) and Short Circuit (Tamper) states.

c. Each detection device shall be connected to separate Zone Input for individual monitoring and reporting unless otherwise stated.

d. The system shall allow Detection devices with Normally Closed or Normally Open outputs to be wired to general purpose Zone Inputs in the same manner. A programming option shall be provided to define each of the inputs, whether the device connected utilises Normally Closed or Normally Open outputs. The default setting shall cater for Normally Closed outputs.

e. The system shall operate reliably over the following cable types:
    i. Category 5 cable (CAT-5).
    ii. Belden CAT – 5 or CAT – 6 cable.

f. Data Rate: RJ-45 communication shall operate at 100MB/s.

C General System Functionality

1. Card

a. The access control system shall be capable of interfacing with a range of reader technologies including magnetic Stripe, proximity, wiegand 26-bit, contact and contact-less smart chip cards and for low security areas code only operation.

b. The magnetic stripe, proximity, wiegand 26-bit and smart card reader technologies will include a with keypad option for card and PIN operation when required.

c. The card shall have a unique pre-programmed code. This is set by the manufacture and must not acceptable to have reproduced.

d. The ID Card shall conform to the standard credit card size. The card shall be classified into priority/security level and allow the printing of a photo ID directly on to the surface of the card.

e. The ID Card shall water-proof and not easy to broken.

f. The Card shall carry lifetime manufacturer's guarantee against electronic failure.

2. Reader and Reader Housing

a. The readers shall be designed for general purpose to read the card information and be suitable for outdoor and indoor. It must be slim and made of flame retardant metrical. All reader must carry lifetime warranty to avoid electronic failure.

b. The card reader shall support the stand size of Motorola proximity reader, size: 4" (10.2cm) with proximity card or Fingerprint reader

c. The readers shall be able to mounting on internal and external without any additional protection. And it must be weather-proof where it is located outdoors.

d. Access door release switch/button shall be provided inside the protected area at the access door. In addition protection, an emergency overrides must provided in case of fire alarm activation.

e. All the reader shall be mounted on a metallic or non-metallic materials without any adverse effect when reading the card information.

f. The reader cabling shall use multi-stranded unscreened 8-core cable and the reader shall be capable of operating up to 100 metres from its control unit without the need of an additional power supply. Cable from the reader shall be permitted to run next to mains carrying conductors without adverse effect.

g. The proximity card reader shall came with a high quality reader head and the LED status indicator. It designs for low visibility condition. Entry readers are usually located outside the room near the door.

h. The LED(s) will operate in the following manner:
   i. LED is red when door is closed and secure.
   ii. LED is green when successful access and remains green until the door is lock and back to secure.
   iii. LED is flash when unsuccessful access attempted has been made.

i. The Proximity & PIN Reader shall provide for higher security level. These areas a Card and PIN are needed. This shall be programmable from the administration PC.

j. The distance of Proximity and PIN reader shall be at least 65mm from the door controller.

k. The reader shall incorporate tamper detection to signal that the connecting wires have been broken. This shall be achieved without the use of a tamper switch.

3. Door Access Controllers

a. The access control system must be high integrity and no loss of functionality in the event of communications interruption.

b. The door controller shall store up to 2,000 transactions and which is expandable to 50,000 transactions. Supports 1000 card holders and which expandable to 20,000 card holder. It shall be possible to wire all the controllers in a star configuration, by the addition of a cable from each of the controller and connecting, it back to an Ethernet networks on the Systems.

c. The door controller shall store all the transaction and upload to PC administration system when system software is online.

d. Door controller communication shall use the available of the existing network or installed a new network structure for the building for communication.

e. The Access Controller Unit (AC) can store the information below:
   i. Controller information:

- Programmable Time Zones
  It shall be possible to assign different time periods for each day.

- Automatic Lock Release
  It shall be possible to programme the lock to be automatically released.

- PIN Numbers Programming
  It shall be possible to enable or disable the PIN by programming. When enable, the user must key in a number after swiping the card.

- Global Anti-Passback & Local Anti-Passback
  To prevent double entries or double exits for Global (a group of door controller) and Local (the door controller itself). Global Anti-Passback shall be able to function as long as the Ethernet still function even if the PC is down.

- Door Alarm Output
  The output activates when the door protected is forced open or left opens for too long.

- Dual Card Option
  Grouping a group of card to allow access to a door only with 2 cards is readied.

- Card Holder information:
  - Card Number
  - PIN Number
  - Time Zone
  - Card Name and Photo

f. The door controller shall fully monitor and control the access point doors with individually configurable, standard and extended, time periods for lock release, door open, and warning sounder for any alarm

g. The system offered should not only provide a flexible approach to expansion of the hardware but also cater for future cardholder capacity needs. When operating off line, all activity shall be capable to be stored within the controller's local memory.

h. The user interface shall display the status of all transaction and any alarm warning for the door controller. When an intrusion was occurred, the controller should audible a warning sound.

i. The all system must maintain a system clock and which is automatically synchronised for DATE and TIME when PC is online.

j. A back up power supply shall be included. This standby battery shall supply to ensure the information integrity when systems power failure. And the controller's data must maintain in a non-volatile memory.

k. The backup power shall provide 12.7V and last for 7 Hours under normal operation.

l. It shall provide 12V DC at 1Amp (max) for up to 2 locks. Power supply shall provide sufficient charges for 12.7V Amp Hour backup batteries.

m. The cable shall be shielded CAT-5 cable for communication (Ethernet RS-45 line).

n. The EM-Lock shall be a solid state device for security safe, It provide locking and uses electromagnetic field to hold the door from being open.

o. The solid state device must have a selectable output, capable of souring power to its attached lock at 12V DC at 3 Amp continuous.

p. The solid state lock output must be protected against short circuit and overload

.

q. The door controller shall control only a door. Anti-pass back and Dual Card shall only be implemented within a door.

r. Enable Dual Card shall have a limit of time allow the cardholder to key in the PIN, when using Card + PIN mode.

s. The door controllers shall be networked on to a data bus whose maximum length is not limited. The data bus shall use by Ethernet networking which is IEEE 802.3 compliant.

t. Visitor Card may require for allocated the start and end time for their validity on the system.

u. The door controller shall be mounted in safety cabinet in a sufficient size to enable easy cable handling and a room for the back-up battery. It shall have dimensions no greater than 310 mm (H) x 265 mm (W) x 70 mm (D)

v. The PC shall be connected to the Ethernet via networking. Ethernet network of this system shall support wireless (WiFi) networks via wireless Ethernet hub or switch. Therefore there shall be no distance limits constraint.

w. The system shall be programmable, and able to configure as a network master controller. The PC server should have a printer port link to printer output to print transactions and its database set-up.

x. The system shall provide a means to automate a back up of the system's main database including all history-related data in a schedule period of time.

y. Back up database to other device shall be done every week in manually by the end user to provide the back up data when system down.

4. Car Park Access Controllers

a. The car park access control system must be high integrity and no loss of functionality in the event of communications interruption.

b. The car park controller shall store up to 40,000 transactions and supports 20,000 card holders. It shall be possible to wire all the controllers in a star configuration, by the addition of a cable from each of the controller and connecting, it back to an Ethernet networks on the Systems.

c. The car park controller shall store all the transaction and upload to PC administration system when system software is online.

d. Car Park controller communication shall use the available of the existing network or installed a new network structure for communication with PC.

e. Goose Neck with reader shall be in appropriate height so that it is reachable by the user (at least 95mm – 100mm above the ground).

f. When a card user is prox upon the reader without the car is stops near the reader, the car park controller shall not open the barrier for him even it's a valid card

g. The Car park controller shall be able to controls 1 entry and 1 exit barrier in order to have the antipassback and global antipassback function for the whole system.

h. The barrier arm should be 3-4 meters long, just enough to block the vehicles from entering or exiting the car park area. The barrier itself should be able to unlock manually from the barrier alone in case of controls failure.

i. The whole system must maintain a system clock and which is automatically synchronised for DATE and TIME when PC is online.

j. A back up power supply shall be included. This standby battery shall supply to ensure the information integrity when systems power failure. And the controller's data must maintain in a non-volatile memory.

k. The backup power shall provide 12.7V and last for 7 Hours under normal operation. The backup power supply charger shall provide sufficient charges for 12.7V Amp Hour backup batteries and able to detects main fails and battery low.

l. The cable shall be shielded CAT-5 cable for communication (Ethernet RS-45 line) and the car park controllers shall be networked on to a data bus whose maximum length is not limited. The data bus shall use by Ethernet networking which is IEEE 802.3 compliant.

m. The PC shall be connected to the Ethernet via networking. Ethernet network of this system shall support wireless (WiFi) networks via wireless Ethernet hub or switch. Therefore there shall be no distance limits constraint.

5. Alarm Monitoring (Optional)

a. Alarms generated by all card access controllers shall be prioritised. Alarms generated at each card access controller can be acknowledged locally.

b. The Alarm input shall be able to be program or change from via the central administration system according to the area within 24 hour, and always be active.

c. The facility to customise audible alerts for each type of alarm shall be provided, using standard or custom generated multimedia wave files.

d. The door controller shall be able to detect and report all the condition it may occur, such as Valid Access request, Unknown Card, Wrong Time Zone, Invalid Card and Reader Tamper.

e. The system shall fully monitoring all door controller in access point doors with individually configurable, standard and extended, time periods for lock release, door pre-held warning sounder.

f. The alarm monitoring shall present the action door forced and door held conditions. Each door shall have a voltage free relay output to provide an output signal from the point of the door being released until the door re-close.

g. Alarm interface or the location of the door controller shall be display on the control system PC.

h. The Ordinary cardholders/key holders shall be able to gain entry at the main entrance to the premises once the Security cardholders/key holder has disarmed the alarm.

i. There shall be the facility to disable perimeter doors when the panel is armed by the use of reader inhibitor modules.

j. 5 input/1 output Expansion Modules
    i. Input zone.
        The 5 Input Zone Expansion Modules shall be short or open input. This input shall be programmable from Central Monitoring Control.

    ii. Relay Outputs.
        The 1 Relay outputs shall be capable of switching up to 10A to drive siren, strobe light, etc output

    iii. Optional Features
        There should be optional features as a LCD module interface and could be expand for more input and output.

k. 8 input / 8 output Expansion Modules
    i. 8 Input Expansion Modules
        The 8 Input Zone Expansion Modules shall consist of a standard 8 Input Zone Expansion Module with a plug-on 16 Input Expander board fitted. This is to ensure product consistency and ease of future expansion. Each input shall be a supervised input point (Normal, Open circuit, Short circuit).
    ii. 8 Output Expansion Modules
        The 8 Output Module each shall be configurable to Normally Open or Normally Close output point. Each output point shall capable of

switching up to 10A (e.g. for control of strobes, sounders, etc). All output point shall be dry contact point.

6. System Management

a. The door controller shall have a buffer of at least 2,000 events and which is expandable.

b. If the system fails, the door controller shall continue to function as standalone.

c. The system shall have auto-detection of controller through IP-address.

d. The system shall demonstrate the ability to export data, Example like standard office word processing packages such as Microsoft® Word.

e. The system shall be based on PC's running under Microsoft® Windows.

f. The system shall able to run on a standalone PC; it shall support word-processing or database programs.

g. The Server should have the specification stated below:

i. Processors
- Pentium Core Processors or greater/equivalent

ii. Memory and Storage Requirements
- 4GB RAM Memory (Preferable)
- 10GB Hard Disk Space (Preferable)

iii. Software Requirements
- Windows XP Professional or later (32-bit OS)
- Windows Vista Business and Ultimate (32-bit OS)
- Windows Server 2000 (32-bit OS)
- Windows Server 2003 (32-bit & 64-bit OS)
- Windows Server 2008 (32-bit & 64-bit OS)
- Microsoft Internet Information Service (IIS) 5.1 or above
- Microsoft .NET Framework Version 2.0
- **Windows Basic and Home Editions version are not supported**

iv. Internet Browser Requirements

To use all the advanced feature of the FALCOWeb, you will need to use the latest version of Microsoft Internet Explorer, Firefox or Opera on a Windows based operating system

v. CD-ROM Drive to install the software.

h. Client Workstation Requirements

i. Processors
- Pentium Core Processors or greater/equivalent

ii. Memory Requirements
- 2GB RAM Memory (Minimum)

iii. Software Requirements
- Windows XP Professional or later
- **Windows Basic and Home Editions version are not supported**

iv. Internet Browser Requirements

To use all the advanced feature of the FALCOWeb, you will need to use the latest version of Microsoft Internet Explorer, Firefox or Opera on a Windows based operating system

i. The system shall archive all the events and transactions, the hard disk shall store a range of 18,000 to 40,000 transactions per megabyte.

j. System Administrator
   i. The System administrator will be able to program, monitor and make reports from the central monitoring software. He will be able to add new system user and assigned level of access (role) to the new user.

k. System User Permission
   i. Each of the system shall have 3 roles of user. They will be System Administrator, who shall have the full accessible to all the system function, enable to add, edit and delete the information. System Operators; who shall have accessible to view the information within the system but not changeable and also monitoring purposes. Time Attendance, same access level with the Operator, but who can access to report, print and view the report. The entire system user shall have independent system User Name and password. The system shall record the information when the operator currently logged on. An authorised operator should present their User ID and Password.

l. Department or Cards Grouping
   i. When adding a new cardholder, it shall be able to assign a department and a work group to the cardholder. The department can be used to determine the card user department in reporting.

m. Access Level

i. The system shall have ability to be not more than 72 access levels. Each access level limits the access of a group of cards to the door controller according to settings.

n. Reporting in Text file format or HTML file format
    i. The system shall have a facility to exporting all the data in text format or HTML format. The data shall contains the information of Date, time, Card No, Controller, transaction type.

o. Transaction Reporting
    i. The system shall provide to view all transaction events; it shall able to search function. The report shall allow generating by a period of time selected by the operator.
    ii. A system report shall provide for total hours on site report, in order to calculate the salary. The report shall provide not only transaction report and also detail information report for all filed.

p. There shall have a function to report all the database information that is currently on site.
    i. The system shall have an attendance report facility. This report shall provide the total time of the time for each cardholder or some cardholders on site.

q. Transaction Online and Graphics maps
    i. The system shall provide two type of viewing for the operators when transaction was occur One of the types shall be show as a map to view out the location of entire door controller, and the other as a list of transaction events. The system shall display live video image of the particular alarm of the particular site through network when the alarm triggered.
    ii. The alarm manager shall keep track of all the alarm events.

r. Time Profiles
    i. The system shall have a minimum of 50 time profiles per division. Each time profile shall consist of at least three time periods. Each time period shall have a start time and end time and the days of the week it will operate. This shall include system holidays.

s. Photo ID
    i. The system shall have photograph for cardholder in the database for optional to store into the database. This shall be same as the photo print on the card.

t. Backup Database
    i. The system operator shall do backup in every week or two-week or annual backup to avoid system down. System shall provide auto backup

as well as schedule backup of database settings. It shall provide backup and restore function.

u. Ethernet specification
   i. Ethernet 10/100 Mbps transceiver (EPHY)
   ii. IEEE 802.3 compliant
   iii. Digital adaptive equalization
   iv. Half-duplex and full-duplex
   v. Auto-negotiation next page ability
   vi. Baseline wander (BLW) correction
   vii. 125-MHz clock generator and timing recovery
   viii. Integrated wave-shaping circuitry
   ix. Loopback modes

v. Controller specification

i.	Card Holder	1,000 upgradeable to 20,000
ii.	Event	2,000 upgradeable to 40,000
iii.	Reader	1 in, 1 out for 1 door (Expandable: 2 in, 2 out for 2 doors)
iv.	Controlled Doors	Single Door Controller (Expandable: Two Door Controller)
v.	Alarm Points	2 (Expandable: 32 Alarm Points)
vi.	Output relays	1 (Expandable: 64 Output Relays)
vii.	Communication	10/100 Mbits/s (TCP/IP)
viii.	Holidays	50
ix.	Time Zones	50
x.	Time Sets	50
xi.	Time Sets interval	3
xii.	Access Level	72
xiii.	Software User Level	Unlimited
xiv.	Elevator Floors	64
xv.	Elevator Access Level	50 controls of 64 floor
xvi.	Card holder photo	Yes
xvii.	Floor Plan	Yes

D General Software Functionality

1. FALCO Web Description

a. Web-based Applications
   i. With no PC software to install, customers who choose the web interface have no worries about operating system compatibility, virus attacks or other computer issues such as hard drive crashes or system lock-ups. This software application is deployed on a web server. Through an Internet browser, FALCO can deliver extensive web-based access control capabilities without the need to load or administrate local software. Any existing PC with a web browser and an Internet connection can be used to take advantage of FALCO Web's access control functions. As a result, it's delivered at a lower cost and is easy to maintain and manage

b. Cross Platform Compatibility
   i. Most web based applications are far more compatible across platforms than traditional installed software. Typically the minimum requirement would be a web browser of which there are many. (Internet Explorer, Firefox, Netscape to name but a few). These web browsers are available for a multitude of operating systems and so whether you use Windows, Linux or Mac OS you can still run the web application.

c. More Manageable
   i. Web based systems need only be installed on the server placing minimal requirements on the end user workstation. This makes maintaining and updating the system much simpler as usually it can all be done on the server. Any client updates can be deployed via the web server with relative ease.

d. Highly Deployable
   i. Due to the manageability and cross platform support deploying web applications to the end user is far easier. They are also ideal where bandwidth is limited and the system and data is remote to the user. At their most deployable you simply need to send the user a website address to log in to and provide them with internet access.

   ii. This has huge implications allowing you to widen access to your systems, streamline processes and improve relationships by providing more of your customers, suppliers and third parties with access to your systems

e. Secure Live Data
   i. Typically in larger more complex systems data is stored and moved around separate systems and data sources. In web based systems these systems and processes can often be consolidated reducing the need to move data around.

ii. Web based applications also provide an added layer of security by removing the need for the user to have access to the data and back end servers.

f. Reduced Cost
    i. Web based applications can dramatically lower costs due to reduced support and maintenance, lower requirements on the end user system and simplified architecture.

    ii. By further streamlining your business operations as a result of your web based application additional savings can often be found.

g. Immediacy Of Access
    i. Web-based applications need not to be downloaded, installed and configured. You access your account online and they are ready to work.

h. Multiple Concurrent Users
    i. Web-based applications can indeed be utilized by multiple users at the same time. No more need to screen share or send a screenshot when multiple users can see and even edit the same document together. Web conferencing and online collaboration companies are in for some key transformations and users need to explore what it really means to effectively work and co-edit documents together.

i. Constant Updating
    i. Web-based applications are always updated to the last release, without requiring the user to take pro-active action, and without needing to prompt or interfere with user work habits in the hope that they will be initiate new downloads and installation procedures.

2. Web-based Workforce Administration

a. Fully configurable to match the needs of each manager, the easy to use screen layouts prove to be a real administrative partner. The system has been designed to be as intuitive as possible and so minimize the time required to administer working time. FALCO takes the native qualities of Open Options and makes them available to help manage the daily administration tasks either through your intranet or the Internet.

b. FALCO has a single simple to use view for clearing exceptions to planned attendance. Absences may be booked using plain English codes with the system automatically checking entitlements to ensure they are not exceeded. FALCO

offers a resource planning function that allows you to view rosters in a meaningful report. By viewing manning levels and skills availability you are more equipped to make decisions when booking absences or changing shift patterns.

3. Employee Self Service – the WEB Kiosk

a. FALCO allows your employees to have access to their own records relating to their personal details and their absence and attendance record. Using their own unique ID and password individuals can register attendance and request absences. An electronic time sheet within FALCO also allows them to book activities that are then reconciled against their attendance details. Personal information can be updated to reduce the administration of personnel records. Employees can also enquire on their attendance, holidays and flexi-balance through FALCO. Where organizations are using Open Options Workforce Scheduling they can also view their planned work rosters

4. General Capabilities of FALCO Web

a. System Administration
    i. The administrator sets up the system to be used on a daily basis. The administrator can add other users and assign them privileges, i.e., authority to perform specific functionality throughout the system. The administrator will also need to set up the system company information and user defined fields. If needed the administrator performs diagnostics and database import export functions.

b. Event Monitoring
    i. The user will monitor the facility by responding to Alarms, monitoring and controlling Doors, and viewing Cardholder activity. Although Presidio monitors a facility continuously, a user must have his web browser up and be logged into the Presidio system to receive notification messages (with the exception of those explicitly routed to a pager or email).

c. Cardholder Data
    i. The user can manage all of the cardholder records in their system. Users can add, delete, and modify cardholder database records. They can also generate cardholder data queries for downloading or printing.

d. Reports

i. The user can run and schedule reports of information about the system as well as event and alarm activity.

e. Historical Log
    i. The user can view all historical activity filtered by time, type, and category.

f. Hardware Configuration
    i. The user can configure all of the hardware installed in the building(s). All Controllers, Readers, Doors, Inputs, Outputs, Elevators, Regions, and Card Formats are defined here.

5. Key Features of FALCO Web

a. Unlimited software users
b. Data Import / Export Capability using SQL Express database
c. Video with data management system
d. Card Tracking module
e. Fire Alarm Automated door release functions
f. Integrated with Milestone & NUUO NVR platforms
g. Integrated Guard Tour management module
h. Integrated Car Park Video comparison module
i. Integrated 32 zones real-time alarm handling
j. Integrated Elevator Control (up to 64 floors)
k. Integrated Visitor Management System
l. Numerous Reports Standard with report scheduling / E-Mail
m. Configurable Holidays, Time Sets, Time Zones, Regions and Groups
n. Automatic, Periodic Data Archiving
o. Global Anti-Passback, Normal Anti-Passback and Card Lock-out Functions
p. Real-time Event & Alarm Monitoring
q. Multiple, Simultaneous Users / Operators
r. Critical Alarm and Event Routing - Multiple Devices / Paths
s. Global Account Management
t. Software development kit available

E FALCO Power Over Ethernet (PoE) Controllers

1. Power Over Ethernet (PoE) Functionality

a. PoE is now offered on FALCO's renowed controller. Power-conserving controllers (FALCO PoE) offers significant energy savings resulting in lower cost of ownership and unsurpassed reliability for end users. With power reduction up to 33 %, FALCO PoE offers a cost effective and environmental friendly product to help you not in one but both ways.

b. FALCO controller connects directly to the IP network and utilizes the 802.3 af PoE (Power Over Ethernet) standards to power itself and any industry standard locking mechanism. This is a new ways for cost-cutting alternative of supplying power to door readers, door controllers and electromagnetic locks via the building's Ethernet.

2. Product Features

a. Cost Saving Installation
b. Eliminates the use of power cable, conduit, power socket and manpower.
c. Reduces the amount of infrastructure to deploy.
d. Speeds up installation with neat cabling and design.
e. Easy Installation
f. Controller connects directly to your IP network and utilizes the PoE switch to power it.
g. Easily installed by integrators, installers or end-user.
h. Reduces electrical surges and lightning strikes by using only isolated TCP/IP.
i. Reduces energy consumption by up to 33 % compared to normal controllers.
j. Product Differentiation
k. Performances of our controllers are maintained although the energy consumption has been reduced.
l. Labelling on cost effective efficiency for this technology can be effective in the marketplace.
m. Network-ready with international power over ethernet (PoE) standard 802.3af
n. Native TCP/IP Ethernet device (RJ45 Ethernet)
o. Low cost single cable deployment (CAT5e or CAT6)
p. Configured with Web Browser
q. Supports TCP/IP, IPv4, 10/100 half/full duplex
r. Supports magnetic locks and door strikes from a variety of manufacturers
s. Dual Lock Outputs (Normal & Inverted; lock doors open or closed)
t. Door Sensors, Key-switches, Local Emergency Exit Break Glass
u. External Trigger, NC/NO 'no-volt' contacts, Panic Input (Open Up or Lock Down)
v. Timed, toggle, lock & unlock door operations

F FALCO WEB TIME ATTENDANCE

1. Time Attendance Software

a. FALCOWeb time attendance allows you to use one or many Windows based operating system to track and record your time attendance information. It completely replaces outdated time attendance tracking systems and will save you time and money every time you use it. It has features built into the software to export data out for 3rd party software to utilize.

2. Time Attendance Specifications

a. Data collected at many computers but processed and reported on central database
b. Information can be adhered in just seconds rather than hours spent on manual calculations.
c. Work Time Configuration
d. Able to set working time on a weekly basis with grace period allowance
e. Able to set lunch time or break time accordingly
f. Overtime setting available
g. Duty Organizer And Configuration – Advance Module
h. Pre-schedule your employees' working rooster on a monthly basis
i. Flexible Shifts are available; suitable for FMCG industry
j. Time Attendance Reporting
k. Search by any of the following field; Date, Card Number, Card Name, Access Level, Door Controllers and Department
l. Available report types; Daily Complete, Daily Incomplete, Daily Lateness, Daily Early Out, Daily Overtime, Daily Absentee, Daily Combination, Daily In-Out Detail, Break and Lunch report

G PEER – TO – PEER COMMUNICATIONS THROUGH VIRTUAL PRIVATE NETWORK (VPN)

3. Virtual Private Network

a. Communication between controller and server can be made via internet.

b. Both sites A and B where site-A installs with door controller and site-B may install with server PC. Via router connection to internet both end shall be link together by Virtual Private Network (VPN) connection.

c. Controls of doors shall be similar as LAN as it is for WAN.

d. Alarm event shall be monitored and recorded into the server PC via internet without the use of CMS module. CMS monitoring is therefore possible be done by our own personnel in the centre monitoring station.

e. Network router shall be provided by contractor to obtain the network functionality.

f. In future monitoring of alarm and access control shall be possible for multiple sites.

H COMMISSIONING AND TRAINING

1. Standard Practice

a. The system shall be programmed with the information supplied. The system must be fully working with all system parameters and token holder's information. It is the tenderer's responsibility to ensure that all the necessary information is obtained before commissioning the system.

b. The training shall provide to at least 1 - 4 members of staff from the company to be operators. These operators must have sufficient training for the operation and configuration of the system that enable these operators to train others people.

c. The training shall be providing by the manufacturer's training staff or other certified staff.

d. A CD contains of PC user manual, installation guide and technical path shall provided.

e. The tender person shall supply detailed "as installed" drawings of the entire system.

I MEMORY EXPANSION MODULE

1. Default Settings

    a. Built-in 8Mbits of Flash Memory

    b. High speed data transfer rate up to 1M Bit/sec

    c. Supports up to 20K user database and 40K event log

J INTERFACE BOARD

2. Default Settings

    a. 12 VDC power input from the door controller or a separate 12V battery-backed power supply

    b. 5 input port can be configured for 24 hour detection or normal detection, activate high (open circuit) or activate low (short circuit), and configured to trigger the relay output

    c. 1 relay output for maximum switching up to 10A

K LCD Module Board

3. Default Settings

    a. 16 x 2 character LCD module with back-light
    b. Wire length can be up to 15M from the interface board

– END OF TENDER SPECIFICATION–