# Enterprise Buildings Integrator

# R600 Guide Specification

# Version 3 – April 2020

# 1. General Specification

## 1.1. System Architecture

### 1.1.1. General

The Integrated Building Management System (IBMS) system shall use a Client Server architecture based around a modular PC network, utilizing industry standard operating systems, networks and protocols. It shall be delivered with an integrated cloud connection to deliver value added services, analytics and mobile applications.

The system shall allow the distribution of system functions such as monitoring and control and graphical user interface etc. across the network to allow maximum flexibility and performance. The architecture shall include support of various Wide Area Networks using standard hardware and software to link nodes into a single integrated system. The network protocol used shall be industry standard TCP/IP and HTTPS. The system shall also support remote configuration and operation using standard intranet or internet connections.

The IBMS system shall allow communications with a wide variety of control devices utilizing off the shelf driver packages. It shall support LON, BACnet, Modbus and OPC standards for open system communications. To support integration at an enterprise level the IBMS will also support Service Oriented Architecture (SoA) based on Web 2.0 web services standards.

Using appropriate hardware, the system shall be Listed by Underwriters Laboratories Inc (UL) for use in energy management (category PAZX), critical process (category QVAX), security (category APOU), and as the primary control and monitoring device for smoke control (category UUKL) and fire alarm systems (category UOJZ).

### 1.1.2. Hot Backup Server

This shall enable the IBMS system server to operate in high availability architecture with no single point of failure.

The system must be capable of running a pair of similarly configured computers in a hot backup configuration where at any point in time, one is the acting Primary and the other acting as the Hot Backup.

Simply scanning I/O on two separate systems and processing independently is not acceptable. The database duplication must be performed on a per-transaction basis for several reasons:

- To ensure that the duplicated Backup database is consistent at all times with the Primary database
- To avoid unnecessary loading of field devices caused by duplicate polling
- To avoid a Windows Operating System issue or PC hardware fault, from causing the failure of the IBMS system

It must be possible to remove one of the redundant systems for maintenance without interrupting operation, and upon its reinstatement, re-synchronize the databases, again without interruption to system operation. A method of manually initiating a fail over must be provided to assist with such maintenance operations.

Failure of either system must be announced audibly and visually via the alarming subsystem.

To accommodate recoverable faults, the failed system must be able to reboot automatically after non-fatal errors and assume the role of acting as Hot Backup automatically.

### 1.1.3. **Communications Redundancy**

The system must be capable of supporting fully duplicated communications links to Operator Workstations and field devices that support this type of connection.

The system and its associated Operator Workstations must be capable of connecting to two fully independent Ethernets run in parallel. No repeater or bridge connection between the Ethernets is acceptable as a means of achieving this function.

Operator Workstations must be capable of switching automatically between the two server computers in the event of a fail over, and switching between two Ethernets automatically in the event of an Ethernet failure.

### 1.1.4. **Distributed System Servers**

A method shall be provided for monitoring and control of points on remote IBMS servers. Specifically, real-time and history values in any IBMS server must be available to any other server for monitoring and control. Features supported must include:

> **Access**: Access to data shall be global, such that users at Operator Workstations on one server can access data, history, point detail displays, etc. for points on any other server. It shall not be necessary to configure system wide, more than one point for each data value or signal, regardless of the number of servers accessing the data.
>
> **Security/Filtering**: It shall be possible to nominate sets of points to be accessed on a server-by-server and user-by-user basis. The mechanism shall be the same as the mechanism to control individual operator and workstation access to data for single server systems.
>
> **Alarms / Messages**: Operators and workstations at any server must be able to see alarms from any other server. It shall not be necessary to configure alarms more than once, regardless of the number of servers accessing the data.
>
> **Trending**: It shall be possible to configure real time and historical trends that combine data from any connected server on a single trend. It shall not be necessary to configure more

than one point for each data value or signal, regardless of the number of servers accessing the data.

**Graphics / Reports / Applications**: All graphics, reports, and applications at a server shall have the same distributed access to data on other servers as described above for operators and workstations. It shall not be necessary to configure more than one point for each data value or signal, regardless of the number of servers accessing the data.

**Cardholders**: All cardholders in the IBMS shall be distributed to all servers so that cardholders need only be enrolled into one server and will automatically then have access to all other servers if desired. Access requirements for all servers will be set up at the time of enrolment in one server.

**Events**: All system and operator events across the IBMS array of connected system servers, shall be centrally stored into a Central Event Server, which can be queried by operators to provide a single unified view of alarms, operator changes and system events

**SoA web services**: The important web services that enable extension of the IBMS system, must also provide seamless access to points, alarms and history from any Distributed System Server, without needing to directly address each individual server. The data across the Distributed System Servers shall be seamlessly integrated into the Web Services.

The system shall support identical point names on any of the connected servers in this distributed system. With the exception of scope of operator responsibility assignment, there shall be no engineering effort to connect these distributed systems. Self-discovery of all points and alarms in this distributed design shall ensure that zero manual or engineering of linked points or parameters is required.

Connections between servers can be made through local Ethernet connections, the plant's LAN, or the corporate LAN and WAN. Connections must be optionally redundant. Both redundant and non-redundant servers must be supported, and no additional engineering effort shall be required to connect both kinds of servers.

#### 1.1.5. **Network**

The Server Computer and Operator Workstation hardware shall be capable of interfacing to an IEEE 802.3 Standard Local Area Network (LAN), and also capable to operate using IEEE 802.11 Wireless Local Area Network (WLAN). Support for 3G and 4G cloud connected services and mobile applications must also be included

### 1.2. **Hardware**

#### 1.2.1. **Server Computer**

The system server computer shall comprise of the following minimum hardware:

- CPU with CPU Passmark score of 5000+

- Example:
    - Xeon Quad-Core 3.4GHz (E-2124G or equivalent)
    - 16GB of RAM
    - Graphics card capable of 1280x1024 pixel resolution and 65K colors.
    - 12 function-key keyboard
    - Mouse pointing device
    - 128 GB Hard disk drive
    - TCP/IP adaptor
    - UL Listed server computer platform shall be used when UL compliant system is required.
- Larger computer specifications may be required for high end applications and large complex projects

### 1.2.2. **Operator Workstation**

The system shall be capable of supporting up to 80 simultaneous Operator Workstation connections using a TCP/IP Local Area Network (LAN). The Network connection must allow a limitless number of casual users access to the 80 connections on a first-come-first-served basis.

The Operator Workstation shall comprise the following minimum hardware:

- CPU Passmark of 5000+
- Example
    - Intel® Core™ i5-9400 2.9 GHz 8GB RAM
    - Graphics card capable of 1280x1024 pixel resolution and 65K colors
    - A 50 GB Hard disk drive
    - A 12 function-key keyboard
    - A mouse pointing device
    - TCP/IP adaptor

### 1.2.3. **Thin Client Browser Agnostic Client**

The IBMS must be provided with a zero footprint thin client that is browser agnostic. No Java Runtime applications shall be required. This thin client shall be supported operating a full workstation experience from devices such as, but not limited to:

- Android smart phone
- Apple iPhone 6 or above
- All tablet computers with a modern HTML5 browser.
- The solution without any changes, must work on all modern web browsers including Safari, Mozilla, Firefox. Edge and IE.

### 1.2.4. **Remote Access via Mobile User Interface using LAN and WAN technologies**

The IBMS shall be available with a real time Mobile user interface using a direct connected On-Premises based VPN connected technology. The direct connect solution shall be supported operating on any modern Smart Phone device with network connectivity, such as but not limited to:

- Smart Mobile telephone with internet access (such as Nokia)
- Blackberry
- iPhone
- Android
- Windows Mobile Device

The web based design shall also allow this interface to be supported on any modern PC with a browser

#### *1.2.4.1. Network Agnostic*

The Mobile user interface shall operate over standard TCP network connection, and perform well down to standard mobile 3G speeds. The interface shall be optimized to ensure very high performance across these different network topologies:

- LAN, both internet and local network
- WAN, DSL, ADLS and other standard TCP based connections
- Mobile 3G, 4G or higher

#### *1.2.4.2. Browser Agnostic*

The Mobile user interface shall be written with HTML5 web standards and be browser agnostic. It must not deploy or use ActiveX controls, nor shall it require installation of the Java Runtime engine.

#### *1.2.4.3. IBMS features integrated into Mobile solutions*

The Mobile user interface solution shall incorporate full scope of responsibilities of the IBMS operators for the remote mobile users, allowing them to view or control points within their assigned facility locations. Other standard IBMS features required include:

- Real time updates of point information from the standard html pages with no custom programming
- An Alarm Dashboard, indicating the most recent 20 alarms at a minimum. Users shall be able to acknowledge these alarms directly into the IBMS database
- Simple trending objects shall be integrated into mobile solution, enabling historized IBMS data to be viewed in simple trend widgets.
- Wildcard searching must be provided to allow remote users to search for points in the IBMS system and with suitable access privileges; they can then monitor and control this plant data

#### *1.2.4.4. Operable within normal PC desktop browsers*

Without alternation, the mobile user interface shall be operable within any standard internet browser from a normal personal computer. These clients shall include Linux based operating systems, Macintosh OS, and the following browsers shall be supported from any current Operating System:

- Internet Explorer
- Safari
- Chrome

- Firefox
- Edge

#### *1.2.4.5. Cloud Connected Mobile App for Alarm Notifications*

The IBMS solution shall be provided with an integrated mobile app, to work anywhere a smart phone with data access can work. It shall not need VPN technologies, nor different ports to be enabled. It shall be true cloud connected, secure based Alarm and Notification Application.

- The application shall be available for easy installation from the Apple iTunes store, or Google App store
- Using 3G or greater, the Application shall securely authenticate each user
- The mobile based app shall support notifications of all critical alarms with contextual trend displays to ensure the impact of critical incidents in minimized.
- It shall also support collaboration by field service providers and subject matter experts, to minimize impact of incidents.

### 1.2.5. **Tablet Access solution**

Along with the optimized smart phone user interface, a dedicated Tablet Access user interface must also be available, optionally providing full operator workstation functionality, on a tablet style device such as:

- iPad
- Android
- Amazon Kindle Fire
- Google Nexus
- Samsung Galaxy Note
- Microsoft Surface
- And similar

#### *1.2.5.1. Tablet Access Features*

The Tablet interface shall support all standard Operator Workstation features, and shall be operable using off the shelf technology such as Windows Remote Desktop, or VMWare VSphere, or Citrix XenApp. All standard IBMS operator workstation features must be operator including full operator scope of responsibility

### 1.2.6. **Printers**

Printers shall be available for printing either reports or online alarms. Report printers shall be any Windows compatible printer such as a laser printer. Alarm printers shall be 132 column printers to allow real time alarms to be printed as they occur.

## 1.3. **Communications**

The IBMS system shall provide communications over a variety of physical media topologies as follows:

- Ethernet
- Proprietary Networks

The system shall support greater than ninety separate communications links to networks of control devices. Each connection shall operate independently of the others and facilities shall be provided by system displays to individually place these links in service or out of service.

Where supported by the controller, it shall be possible for serial connections to the IBMS Server to be routed via a terminal server and the LAN as an alternate to connecting directly to the host computer. TCP/IP based Terminal Servers are suitable and must be Ethernet connected to the IBMS server directly.

Given the sufficient level of system privilege, it shall be possible to view, manipulate and analyze all data in the system from any Operator Workstation in the system, including those operating remotely via dial-up modem links or internet connection.

Once a control device is configured and placed in service, the system shall automatically begin background diagnostic scanning of the device to ensure that communications are monitored independently of any monitoring scanning.

The system shall perform checks on data integrity of all data acquired from the device. If an invalid or time out response is received, the data shall be ignored and the system will record the transaction as an error. Statistics shall be kept and displayed by the system on errors encountered in communication by means of a communications barometer. The barometer shall increment for every failed call and decrement for each successful call. In addition, the system shall alarm separate *marginal* and *failure* conditions based on user-defined limits to advise the operator of the device and link that has failed. Communications statistics shall be displayed as standard on the system and shall also be available as part of the reporting system or custom displays.

## 1.4. **System Software**

The IBMS system server shall be based around the Microsoft Windows Server operating system (Windows Server 2016). It shall not be supported running in a client workstation grade computer like Windows 10 or Windows 7.

Standard services supported by the server computer operating system will include the following:

- Multi-tasking Multi-user support
- Real Time and relational databases to integrate connected systems into unified presentation layer
- IBMS Application software

Software at the Operator Workstation shall comprise of:

- Windows 10
- IBMS Client Application software
- TCP/IP Networking

The networking software shall use the industry standard TCP/IP LAN protocol.

The server computer or an alternative network connected computer shall be capable of acting as a File Server for graphic displays and cardholder photo images. All LAN connected Operator Workstations shall be able to view custom displays and photo images from the server computer.

All system peripherals shall be capable of being connected to the server computer via the LAN.

### 1.5. **System support for Virtualization**

The IBMS system shall be qualified and supported on a leading Virtual Machine platform such as VMware ESX and Windows HyperV. This support shall include operations of the IBMS server software, and also related communications gateways and storage devices.

Completed test plans demonstrating the offered IBMS solutions support for Virtual Machine platforms shall be available. Also characterizations of performance results and required Virtual Machine settings shall be available.

### 1.6. **Operator Interface**

#### 1.6.1. **General**

The operator interface provided by the system shall allow for efficient communication of operational data and abnormal conditions. It shall provide a consistent framework for viewing of information. Critical areas (such as alarm icons) shall be visible at all times. A predefined area on the screen shall provide operator messaging, and this area shall also be visible at all times. A set of standard displays for configuration, and navigation around the IBMS system are to be provided with every system and shall not require any engineering. The IBMS shall also have an unlimited number of custom (facility specific) displays created to meet the needs of the specific facility.

The operator interface software shall be capable of running in the Windows 10 or Windows Server 2016 environments, or via a thin client browser agnostic user interface. The operator interface shall be interactive and totally graphics and/or icon based. Graphic displays shall be supported on newer UHD based displays as well as traditional lower resolution displays (down to 1280*1024 pixels).

The operator interface shall employ standard Windowing conventions so as to reduce required Operator training. In particular, standard tool bar icons and drop-down menus shall be available on all standard and custom displays to allow easy access to common functions. The tool bar and pull down menus shall be fully configurable. Similarly, such functions shall also be available via a standard set of Function-Key based pushbuttons without requiring configuration.

The operator interface shall support the ability to “full screen lock” the window so users cannot access other applications. If “full screen lock” is not enabled, support for copy and paste facilities shall be provided between the operator window and other Microsoft applications.

### 1.6.2. **Web Browser Operator Interface**

The operator interface shall also be fully available through the internet via an Internet Explorer browser. From Microsoft’s Internet Explorer, an operator shall be able to perform all functions on the same standard and custom graphics as used in the standard operator interface. All custom graphics, alarm graphics and standard graphics shall be available without modification or reengineering through the Internet in an Internet Explorer browser user interface and shall be fully functional.

The browser interface shall provide login and security authentication in the same way as the standard operator interface. It shall be possible to operate the facility through the browser user interface in the same way as the standard user interface and perform all functions described in section 1.6.6 for example: acknowledge alarms, view graphics, control points, execute reports, modify configuration settings and the similar. A large number of casual users shall be permitted without any additional licensing burden. Licensing shall be based on the number of simultaneous operator connections on a “First Come First Served” basis. Those users with casual access shall automatically disconnect from the IBMS server after an idle timeout period.

### 1.6.3. **Operator Interface Connection**

The operator interface shall be flexible in its connection to the IBMS server. An Ethernet LAN or Internet connection shall be used between the Server and the Operator Workstations and Browser Clients. The operator interface shall provide standard remote access support using industry standard tools like VNC, RADMIN, and Windows Terminal Services. Where used, these remote connections must use password protected user authentication and encrypted network / internet protocols

The operator interface LAN connection shall also be flexible to support both permanent and casual access to the IBMS server either through the standard operator interface. A large number of casual users shall be permitted without any additional licensing burden. Licensing shall be based on the number of simultaneous operator connections on a “First Come First Served” basis. Those users with casual access shall automatically disconnect from the IBMS server after an idle timeout period.

To minimize bandwidth on LAN links, it shall be possible for the operator interface to only require updated dynamic information from the IBMS server. All static information (such as display backgrounds) can be stored locally.

### 1.6.4. **Operator Interface Characteristics**

The system shall provide a Windows operator interface with the following minimum capabilities as standard. No custom programming or scripting shall be necessary to produce these:

- Window re-size, Zoom in, Zoom out with display resolutions continuously resized to fit available window size
- Dedicated icons and Pull Down Menus to perform the following:
- Associated Alarm Display
- Alarm Summary
- Alarm Acknowledgement
- Display Sequence Forward/Backward
- Previous Display Recall (minimum of 8 displays)
- Graphic Call-up
- Trend Call-up
- Point Detail Call-up
- Card Holder Detail
- Pop up face plates
- Alarm Banner showing highest priority, most recent (or oldest) unacknowledged alarm
- System Date and Time Zone
- Current security Level
- Workstation connection number
- Alarm Annunciation
- Communications Fail Annunciation

### 1.6.5. **Operator Input Devices**

The operator interface shall be capable of being mouse driven and simultaneously support keyboard data input. Both fixed menus and configurable function keys shall be supported to aid novice and experienced operator respectively. The interface shall also be capable of supporting a touch-screen for pointing and command input.

The operator interface shall use a Tool Bar for common operator commands. The operator shall be able to request display of commonly used displays and activate system functions via Drop-Down menus

All operator interface input shall be possible using only the pointing device and QWERTY section of the keyboard.

Fast access to common functions shall be possible using predefined function keys on the keyboard. A Keyboard overlay shall be available to assist operators with using these function keys.

### 1.6.6. **Operator Functions**

The following functions shall be performed through the operator interface:

- Display and control of field equipment
- Acknowledge alarms on a priority basis
- Initiate printing of reports
- Archive and retrieve event logs
- View historical plant information on predefined trend windows
- View intranet or information from the Internet in a secure environment
- View ActiveX documents
- Use ActiveX controls
- Change own password
- Monitoring of data communications channels
- Configure system parameters

### 1.6.7. **Operator Security and Sign-On**

#### *1.6.7.1. Security*

If necessary, each operator may be assigned a user profile that defines the following:

- Security and/or Control Level
- Operator Identifier
- Unique Password
- Operator Scope of Responsibility Assignment
- Start Graphic for that operator

- Timeout Value for that operator

All actions initiated by the operator shall be logged in the Event database by operator identifier. In addition, any control actions to a given point shall only be allowed if the control level configured in the operator's profile exceeds the level assigned to the controlled point.

Utilities shall be provided to allow administration of the operator passwords.

#### *1.6.7.2. Security Levels*

The system shall support at least six levels of operator security. The functions allowed from each security level shall be as follows:

Level 1: View Only Mode - This allows operators with defined scope of responsibility to view only displays and point values.

Level 2: Permit Level 1 functions and in addition the operator shall be able to view displays and point values, and acknowledge alarms as they occur.

Level 3: Permit all Level 1 and 2 functions and in addition the operator shall be allowed to control points such as start/stop, disable/enable, etc. and acknowledge alarms as they occur. This is for normal operators.

Level 4: Permit all Level 1 through Level 3 functions in addition to accessing master time schedules, system peripherals allocation, change point engineering parameters, build reports and use most standard system configuration displays. This level shall typically be reserved for the building supervisor.

Level 5: Permit all Level 1 through Level 4 functions in addition to accessing the engineering functions such as building and linking displays, allocating keyboard push button assignments, etc. Reserved for the building engineer.

Level 6: This is the highest level of station security and shall allow the user unlimited access to all station functions. This is typically reserved for the building manager.

#### *1.6.7.3. Sign-On/Sign-Off*

The operator shall be permitted to sign on to the system if their individual Operator Identity and the Operator Password have been entered. This password shall be encrypted. It shall also be possible to have the system authentication integrated directly into Windows, Windows Group Accounts, or an LDAP Server such that the operator uses the pre-existing account details to sign on to the IBMS system. This ensures that operators only need to remember 1 set of credentials for both their workstation and the IBMS

After a series of three (3) unsuccessful attempts to sign-on the Operator Workstation interface shall be locked for a configurable period of time. The lockout period shall be set via system configuration

displays. During Operator Workstation lockout the other Windows functions of the computer running the Operator Workstation software shall not be affected.

It shall be possible to assign operators either single or multi-user accounts. Single user accounts enable the operator to sign-on to only a single Operator Workstation thus preventing simultaneous sign-on by the same operator from different workstations. Operators with the highest sign-on security level who may require simultaneous access to more than one Operator Workstation would typically use the multi-user password.

Each operator shall be assigned a password and a defined Scope of Responsibility which defines the locations in the facility that may be managed and controlled by the individual operator.

The operator may sign-off at any time by issuing a sign-off command.

A keyboard time-out feature shall be provided such that the operator shall be automatically signed off after a defined period of keyboard inactivity. It shall be supported to configure automatic call-up of a "logged-out" display when this occurs to hide restricted information for example.

#### *1.6.7.4. Location Assignment / Scope of Responsibility Profile*

Each operator shall be assigned one or more specific areas of the building with the appropriate monitoring and control responsibility (no view, view only, alarm acknowledge only or full control). A Location shall be defined in this context as a logical entity comprising of a set of points in the system. This in turn may represent a physical space in the building. Locations shall be used to partition the IBMS database in such a way as to assign operators control over certain areas and prevent unauthorized access to other areas.

The system shall support individual tenant access by means of Scope of Responsibility assignment. Likewise, an operator’s ability to control or monitor certain parts of a facility can be controlled by means of Scope of Responsibility assignment.

The IBMS system shall support the creation of Scope of Responsibility profiles, which combine locations and time periods, and which can be assigned to operators with the same location access requirements. By using scope of responsibility profiles in this way, location access can be specified to apply during certain time periods, allowing different areas of access at different times of the day or week.

With cardholder management and access control, the IBMS system shall allow each cardholder to be assigned to an Organization in the system. For example a company name. Once assigned, the IBMS shall allow all operators to be assigned to view one or more organizations in the systems, thereby ensuring Security persons may not see or monitor cardholder details for Organizations not in their scope of responsibility.

#### *1.6.7.5. Duress*

The system shall support an operator duress function, so that an operator may discretely indicate that they are signing in the IBMS system under duress. The system shall recognize that the operator is signing on under duress and it shall then be able to issue a control to alert appropriate assistance.

### 1.6.8. **Standard System Displays**

The following displays shall be included as part of the system:

- Alarm Summary Display
- Summary Display of Shelved Alarms
- Event Summary Display showing all alarms and events
- Point Detail Template Displays (for each point in the database)
- Trend Set Template Displays
- Group Control and Group Trend Template Displays
- Communications Status Displays
- System Status Displays
- Face Plates for all common point types
- Configuration Displays

In the case of the Trend and Group displays, configuration of these displays shall only require entry of a point name to completely configure the display at runtime, with correct user credentials. The Alarm Summary, Event Summary, Point Detail, Communications Status, System Status shall not require any configuration.

Systems without standard graphical displays presenting all parameters for each system Point shall not be acceptable.

#### *1.6.8.1. System Status Display*

A system status display shall be available on each Operator Workstation. This system status display shall be automatically built by the IBMS system and shall require zero engineering to add additional devices to be monitored. It shall display the following information in a hierarchical system tree:

- Points in alarm condition pending ACKNOWLEDGE command
- Points which remain in an alarm state but which have been acknowledged
- Communication failures

- Printer status
- Operator Workstations status
- Communication links status
- Controller status
- System interfaces status
- Additional connected server status

#### *1.6.8.2. Administration Displays*

The system shall provide the following full screen displays:

- Master system menu
- Report summary
- Alarm summary
- Event summary
- Display summary
- System Status display
- System parameters configuration
- Operator Workstation configuration
- Scope of Responsibility assignment
- Time Schedule assignment
- Calendar assignment (Holidays/special occasions)
- History assignment
- Push-button assignment
- Operator definition
- Operator message board
- Events archive and retrieval
- Time Period summary and configuration

- Point Detail for every configured Point

### 1.6.9. **Creating Custom Graphical Maps / Displays**

#### *1.6.9.1. Graphic Display Building Editor*

The IBMS shall provide a Graphic Display Building editor for the creation of site specific graphic displays. It shall allow one-step online building of display static and dynamic objects. It shall be a WYSIWYG editor (what you see is what you get) allowing the displays drawn using the editor to appear exactly the same when viewed from an Operator Workstation.

Displays shall be created in the HTML (Hypertext Markup Language) format. This is essential so that the displays can also be viewed through a web browser as well as the normal IBMS operator interface. The displays must be saved in the standard HTML format. All graphic elements shall be available as HTML elements. It is not acceptable to have an HTML format which merely links to a proprietary object or bit map of the entire display. It shall be possible to view and edit the resulting HTML file using a text editor. Systems which do not support HTML displays will not be acceptable.

Static objects created using the Graphic Display Building Editor shall include static text, rectangles, arcs and circles. It shall be possible to animate static objects to give the dynamic characteristics of the real-world object the point represents.

It shall be easy to link dynamic objects to the IBMS database. They shall allow information to be displayed from the database or to allow an operator to interact with them in order to make changes in the database and to perform control actions. Dynamic objects shall include dynamic text, push buttons, indicators, charts, check boxes, combo boxes, pop up boxes, ActiveX controls, schedule controls and scroll bars.

It shall be possible to include static and dynamic display objects on the one display. The editor shall allow display objects to be manipulated by pointing, clicking and dragging. The editor shall allow display objects to be drawn, re-sized, copied, grouped, rotated, aligned and layered over each other. It shall be possible to copy and paste objects within and between displays.

The Graphic Display Building Editor shall support the following features:

- One step display building (both background and dynamic information)
- Point and click operation
- Paste to and from the Clipboard
- Absolute positioning object placement
- Z layer control and support
- Cardholder Badges design and Layout

- Control for display status of system schedules
- Ruler and grid
- Configurable tool, color and line palettes
- Dialog boxes for definition of object properties
- Shape and page building
- On-line help
- Import graphics from third party packages including WMF, BMP, TGA, GIF and JPEG formats.
- Standard library of IBMS industry objects
- Live video element
- Building of Face Plates
- ActiveX controls
- ActiveX documents
- Display Scripts written in either JavaScript or VBScript
- Multilevel undo and redo
- Object manipulation including combine, union, intersection
- Polyline node editing
- Transparent images
- Popup Displays
- Standard Alarm symbols
- Real time and historical trend object supporting up to 32 points on 1 trend
- Schedule controls presenting summary of operating plant schedules

#### *1.6.9.2. Display Scripting*

It shall be possible to further animate display elements using standard HTML scripts such as JavaScript or VBScript. A script editor supporting one of the standard script languages shall be provided. By using script programs, individual elements on the display may be manipulated. A

proprietary scripting language or additional scripting and drawing package shall not be acceptable. It shall be possible to perform a variety of animations, which include but are not limited to:

- Move objects
- Resize objects
- Recolor objects
- Pop up messages and dialog boxes etc.

Scripts may be activated on displays using the following events:

- On mouse click
- On mouse enter
- On mouse move
- On page call-up
- On a timer
- On value or state change of a point on the display

#### *1.6.9.3. Live Video*

Both the Graphic Display Building Editor and the Operator Interface shall have built in support for the creation and display of live video objects without the need for programming. The size and position of the video object shall be configured on a per display basis.

Systems, which show the live video object in a separate window from the operator interface, or on a separate monitor screen, shall not be acceptable.

The Live Video control shall support display of multiple camera views.

#### *1.6.9.4. Web Technology*

Displays created in the Graphic Display Building editor shall be usable in a Web Browser such as Microsoft's Internet Explorer without modification. All displays shall be usable in this manner enabling operators to completely operate the system through a web browser via the internet. Displays may also incorporate data from an intranet, the Internet, or ActiveX documents along with other building data.

#### *1.6.9.5. Launching External Applications*

It shall be possible to launch applications (such as Microsoft Word, Excel, custom help files or any third party applications) from a custom display. If supported by the application, it shall be possible to launch the application with a specified file opened within the launched application. Launching of

such applications shall also be possible from the Operator Workstation pull down menus or from a push button on a custom display.

### 1.6.10. **Internationalization**

The IBMS Operator Interface shall be fully translatable into the local language. This includes languages, which do not support the European character set e.g. Traditional Chinese.

### 1.6.11. **Help and Documentation**

The IBMS operator interface shall also have access to online help and online full system documentation. Online help shall be fully searchable and cross referenced to all relevant sections of the documentation. It shall be possible to browse the online help and set “favorites” which link to commonly used sections of the help information. All manuals shall be available online.

## 1.7. **Monitoring and Control**

### 1.7.1. **Monitoring**

The system shall support acquisition of data using the following techniques:

- Periodic Scanning
- Report by Exception
- Data on demand

In order to minimize communications traffic, the system shall automatically group together data requests using contiguous addresses and the scan intervals to generate scan packets, optimizing throughput for a given scanning load. The system shall also provide utilities to examine scan packet allocation for each scan interval, and compile aggregate statistics on communication link usage.

Where supported by the controlling device, Report by Exception (RBE) protocols shall be used to reduce the scanning load of the system while improving system response. If necessary, periodic scanning may be used in conjunction with RBE to ensure data integrity.

### 1.7.2. **Device Control**

Control transactions issued by the operator shall be communicated to control devices using a write followed by read to ensure the integrity of the transaction. If the read following the write to the device indicates that the control action has failed, the operator shall be informed by means of a control failure alarm. The priority of the control failure alarm shall be configurable by the user.

It shall be possible to optionally assign a control confirmation message to individual points. This message shall request the operator confirm the requested supervisory control action prior to sending the entered value to the controller.

### 1.7.3. **Single and double signature control**

In highly regulated environments, it shall be possible to provide an additional level of control by enforcing signoff of certain controls with either a single or a double signature. A single signature

requires the operator to re-enter their Operator Identity and password along with selecting a reason for issuing the control. This ensures that a control is performed by the nominated operator and that the control is logged for future reporting purposes in the event summary. A double signature requires the operator to re-enter their Operator Identity and password along with selecting a reason for issuing the control. In addition to this, a supervisory operator must also enter their Operator Identity and password to confirm the operation. This functionality shall be required for any IBMS system being used to control a regulated environment such as that found in a Pharmaceutical plant.

### 1.8. **System Database**

The system shall provide a real-time database incorporating data from analog, logical or pulse inputs. The database shall be configurable by the end user without the need for any programming and shall be able to be modified on-line without interrupting operation of the system. In addition to point-based information, the database shall also provide historization capabilities for analog, digital, pulse and event based information. This information shall be accessible by all facilities of the system such as custom displays, reports, trends, user written applications, etc.

#### 1.8.1. **Database Structure**

The real-time database shall support collection of data and storage using the following structures:

- Access Point Structures
- Analog Point Structures
- Status Point Structures
- Accumulator Point Structures
- Flexible Point Structures
- Historical Data Structures
- Event Data Structures
- User Defined Structures

Each of the Point database structures shall be comprised as a composite point with a number of associated parameters, which may be referenced relative to a single tag name. Specifically, each of these parameters shall be accessible by various sub-systems such as the Graphical Operator Interface, Report Generation system and Application Program Interface in a simple POINT.PARAMETER format without the need to know any internal storage mechanism.

The system shall maintain portions of the database requiring frequent high-speed access as memory resident information and other less frequently accessed data as disk resident data. Memory resident data shall be checkpoint to disk every minute to minimize loss of data in the event of loss of power or other system failure.

Database backup shall be possible with the system on-line including backup of historical based data. The backup shall be possible via standard Microsoft Windows operating system utilities.

Point data shall be stored in a composite point database structure that provides a wide range of configurable information including but not limited to:

- Point name and description
- Multiple locations for data storage and device scanning addresses
- Scan period
- Multiple types and instances of alarms
- Multiple deadband or hysteresis settings (analog points)
- Monitoring and Control access restriction information
- Location of operator alarm handling instructions
- Location of ancillary information associated with the point.
- A list of all recent events pertaining to that point
- All points shall display all recent events on their point detail displays, using a direct link to the IBMS Event System.

### 1.8.2. **Access Points**

Access points represent card readers when using access control with the IBMS. The point represents the state of the card reader and whether access was granted to a cardholder or whether access was denied.

### 1.8.3. **Analog Points**

Analog data shall be stored in an analog point type in the database. This is a composite point type, which consists of multiple point parameters. For example, it is possible to have the analog set point, process variable and output all represented in one single point in the IBMS.

### 1.8.4. **Status Points**

Status (digital) information shall be stored in a Status Point type in the database. The status point shall be a composite point capable of processing from a single to a three-bit digital input, allowing up to eight possible states.

### 1.8.5. **Accumulator Points**

Data associated with pulsed inputs shall be stored in the system in a composite point database structure that shall provide automatic tracking of instrument rollover.

### 1.8.6. **Flexible Points**

Data from some devices does not fit neatly into the standard point types defined above. In this case, it shall be possible to define flexible point types which can be structured to meet the requirements of the data structure they are being used to represent.

### 1.8.7. **Grouping of Points**

The IBMS system shall provide a means by which a number of alarm inputs, outputs and other related points can be grouped together for more convenient monitoring and control without the need for custom graphics.

### 1.8.8. **History Management**

Collection of historical point data shall be configurable as part of the point definition. Once configured, this historical data shall be collected automatically using an inbuilt history engine. The system shall not require a remote database to story history dat. Historical data collection shall be provided for both snapshots and averages with intervals ranging from 1 second to 24 hours.

Once assigned to history, point data shall be available by POINT.PARAMETER access used in conjunction with a history offset to locate the particular value of interest. The graphical operator interface, trend, report generation and application interfaces shall be able to access historical data.

Modifications to the history collection of a point shall be possible on-line without the loss of previously collected data for the point being changed or any other points in the system currently being historized.

History shall be easily configurable to be archived to an alternative file system or offline media. Different archive settings shall be available for different history types.

The history engine shall support 3 separately managed collections of up to 100,000 point values each, and shall automatically archive the data to either local or remote disk, to preserve the information for more than 10 years given appropriate storage on the hard disk.

### 1.8.9. **Trending**

The system shall provide flexible trending allowing real-time, historical or archived data to be trended in a variety of formats. Trend data types shall be able to be combined to allow for comparisons between data e.g. current real-time data versus archived data. In addition, event database information shall be available for comparison and analysis purposes in the same display and shall allow filtering of the event data display based on time and location.

#### *1.8.9.1. Trend Capabilities*

The system shall provide trending capability with the following functions:

- Real time trending
- Historical trending
- Up to 32 points on each trend window

- 1000 separate trend displays automatically built in every system
- Optional extension of this 1000 trend limit, to support 30000 trends displays.
- Trend with Event Summary integration on any and all of these 1000 trends
- Archived History trending
- Trend Scrolling (using scroll bar or by directly entering the beginning and ending time of interest)
- Trend Zoom
- Engineering Unit or Percent
- Auto-scaling trended values
- Cursor readout of trend data
- Trend comparisons between archived, real-time and historical data (for example, this year vs. last year). Comparisons between the same point offset in time, or different points must be possible.
- Trend De-cluttering via per-pen enable/disable on multi-plot style trends
- Independent Y-axis per point on multi-plot style trends. It must be possible to display the Y-axis for any point on the trend by simply selecting the point using the mouse or keyboard
- Copying the currently displayed trend data to the clipboard for pasting into spreadsheet or document
- An additional and unlimited number of trends may be used inside custom displays. This is outside of the existing requirement for 1000 system trends

Configuration of trends shall only require the entry of the Point Name into the desired trend template to produce the trend. All trend configurations must be possible on-line without interruption to the system. Historization of data shall not be affected by changes to trend configuration. All configurations to the trend configuration shall be possible from any operator interface. It shall be possible to save any changes made to the trend configuration from any operator interface. Systems that only provide trending via a third party package will not be acceptable.

The trend must also support annotations with system events within the one display window, allowing operators to view historical plant information in a real time window with system events. This shall include support for filtering the events by location and other standard filters available within the event management system.

#### *1.8.9.2. Trend Types*

The system shall be able to present real-time, historical or archived data in a variety of formats, including single, dual and multiple value trends of up to 32 points. For each trend set display it shall be possible for operators to configure the number of historical samples and ranges displayed. Points configured in trend sets shall be changeable on-line.

The system shall allow the operator to display the trend data in multiple different views. User shall have the option to view a full screen of the trend only, view trend with events, and trend with tabular history. Each of the views shall have the option to hide or show the legend. It shall be possible to filter the event summary details by the trend time as well as by selecting the location of interest from the hierarchical location pane. Icons indicating the correct event type shall be displayed in the timeline of the trend view to facilitate analysis.

Operators shall be able to zoom in on information displayed on trend sets for closer inspection by dragging out an area of interest with the mouse or other pointing device. From such a selection, it shall be possible to copy the underlying data to the Windows clipboard for subsequent pasting into a spreadsheet application such as Microsoft Excel. Systems that do not provide support for Microsoft Excel in this respect shall not be acceptable.

Scroll bars as well as time selectors for direct entry of beginning and ending times shall be available to move the Trend set backwards and forwards across the historical records. The trend sets shall automatically access archived history files without operator configuration.

It shall be possible to embed trend objects as part of custom displays.

### 1.8.10. **Event Management**

As a standard function, the IBMS shall log all events automatically into a relational database, and optionally print each event to a dedicated event printer. The event journal shall contain the following event information:

- Alarms
- Alarm Acknowledgements
- Return to Normal
- Operator Control Actions
- Operator Login & Security Level Changes
- On-line database Modifications
- Communications Alarms
- System Restart Messages

- Database changes

A standard Event Summary Display shall be provided to show the current event journal file with the most recent event at the top of the display. Subsequent page forward actions shall allow display of progressively older events. Sorting and filtering of the journal shall be possible directly on screen. Filters shall be able to be saved for future use. Filtered events shall be able to be printed as an event report directly from the Event display.

The event database entries shall contain the following information as a minimum:

- Time & Date Stamp
- Database partition code
- Source
- Operator
- Event Type
- Condition
- Action
- Alarm Priority
- Description
- Value
- Engineering Units
- Comments

Events may be sorted by time and date, database partition or source of the event. It shall be possible to apply filters to the list of events to limit the view of events to those which match the filter. Filters may include multiple dimensions and wildcards and shall also be able to be saved and restored for reuse.

The Event display shall support two column sorting. It shall not be limited to sorting only on 1 column.

There may be additional fields which are relevant for different types of events. It shall be possible to enter comments on all events so that operators can annotate an event with relevant information.

It shall be possible to manually create an event if the operator wishes to record an incident on the site which is unrelated to system equipment.

The event database must also be accessible from other sub-systems such as the Operator Interface, Report Generation and Application Programmers Interface.

It shall be possible to store event files as large as the disk capacity can accommodate. For example, given the appropriate disk space it shall be capable of storing 10,000,000 (ten million) events on-line. The system shall be able to automatically or manually archive these online events periodically, at a time period specified by the user. Operators shall be notified by an alarm that event archiving is required if manual operation is chosen. Events may be archived to tape, or to other media such as DVD, or to other disk based file systems. If archiving does not take place, the event system shall continue to collect events until it reaches a nominated disk space limit. It shall then overwrite the oldest events until archiving takes place or more disk space is made available.

Archived events may be restored to the IBMS at a later time if required for reporting purposes.. The IBMS shall indicate to the operator the range of events in a particular archive file.

The event management system shall be fully integrated with the standard reporting system. The system shall automatically reference the restored archive file if a report is requested containing a time search window covered by the current archive file.

The operator shall be able to restore previously archived files and review or print them from the Operator Workstations.

It shall be possible to directly generate an event report from the event database filtered online without using the reporting system.

#### *1.8.10.1. Central Event Storage*

In an array of connected IBMS systems, a centralized event storage must be supported, to enable the integrated consolidation of events from subordinate IBMS systems into 1 store. This centralized event store shall integrate all events into 1 single location allow detailed real time review of all alarms, actions and events in 1 location.

### 1.8.11. **Alarm Management**

The IBMS shall support several different types of alarms for analog points, including:

- High alarm
- High High Alarm
- Low Alarms
- Low Low Alarm
- Deviation High Alarm

- Deviation Low Alarm
- Rate of change Alarm
- Unreasonable value alarm

Any four of these alarms shall be assignable to each Analog or Accumulator point on an individual point basis as part of the point configuration process.

Status points shall allow each individual state to be alarmed.

#### *1.8.11.1. Alarm Priorities*

Each monitored point in the system shall be able to be assigned one of four alarm priorities to individual states. The meaning of the priorities shall be as follows:

**Journal**

Changes of state shall be journalized to the Alarm/Event Log and optionally printed on the Alarm/Event printer.

**Low**

Change of state will generate a Low priority alarm, which will appear on the Alarm Summary. Optionally, the alarm may be printed on the Alarm/Event printer or generate an audible tone.

**High**

Change of state will generate a High priority alarm, which will appear on the Alarm Summary. Optionally, the alarm may be printed on the Alarm/Event printer or generate an audible tone.

**Urgent**

This is the highest priority. Change of state will generate an Urgent priority alarm, which will appear on the Alarm Summary. Optionally, the alarm may be printed on the Alarm/Event printer or generate an audible tone.

Within each of the four alarm types there shall be 15 sub-priorities available.

Each alarm priority shall have a configurable color, which shall automatically be presented to the operator in all graphics and alarm display across the IBMS system. There shall be no engineering effort to support this alarm priority color from being synchronized across the IBMS system. It shall be possible to configure a time such that if a low priority alarm is not acknowledged within this time the alarm's priority is elevated to high priority. If a high priority alarm is not acknowledged within a configured time, its priority is elevated to urgent priority.

For each alarm priority, it shall be possible to configure a point such that if any alarms of this priority occur, the point is controlled to the configured state. This could be used to drive external enunciators such as sirens or lights.

When an alarm is acknowledged, it shall be possible to automatically issue a reset to a controller to indicate the alarm is acknowledged and to attempt to reset the alarm point.

#### *1.8.11.2. Alarm Enunciation*

Alarms shall be enunciated by:

- Most recent, highest priority alarm message appearing on dedicated alarm banner on the operator interface.
- Alarm message appearing on alarm summary display.
- Available Tone - based on a "*.wav" or other sound file for each alarm priority
- Alarm message printed on the alarm printer
- Alarm indicator flashing on the operator interface

Alarm conditions will be indicated in a clear unambiguous manner, and unacknowledged alarms shall be indicated differently to acknowledged alarms. Where alarm conditions are indicated with blinking indicators, the IBMS shall ensure these indicators blink synchronously. This shall not require programming or tuning of display driven timers.

Alarms shall be enunciated at the Operator Workstation even if there is no operator currently signed-on. This feature shall be available on network connected Operator Workstations when the computer running the Operator Workstation software remains logically connected to the network. If the Operator Workstation is minimized in the Windows environment, then the Operator Workstation icon will indicate an alarm. An audible tone shall be able to be generated and this tone shall be specified by a sound file for each alarm priority.

Points shall be enunciated while in alarm. If a point is set to alarm inhibited the point shall no longer cause annunciation. If a point goes into an alarm state whilst inhibited and then is still in the alarm state when the point is set to alarm enabled, the point shall immediately cause annunciation.

#### *1.8.11.3. Alarm Processing*

Assigning an alarm to the point shall automatically cause the system to perform the following actions when an alarm occurs:

- The alarm shall be time stamped to the nearest milli-second and logged in the Event database with the Point Name (source), Alarm type, Alarm Priority, Point Description, New value and Engineering Units

- The point value which is in alarm shall turn red (or other configurable color) and flash on any standard or custom display which uses that point
- An Unacknowledged alarm entry shall be made in the system alarm summary for Low, High and Urgent Alarms
- The audible alarm shall sound (if configured)
- The alarm annunciation indicator shall flash synchronously on all displays

In addition, the alarm banner of the Operator Interface must show the most recent (or optionally oldest), highest priority, unacknowledged alarm in the system.

When used for Life Safety applications such as fire alarm or smoke control, the alarm management system shall be automatically configured to comply with the requirements of UL864 Category UOJZ and the system shall be so listed.

#### *1.8.11.4. Alarm Summary*

Alarms shall be able to be viewed in a consolidated alarm summary which shows all current or pending alarms on the system. This summary display shall be a standard display and require zero engineering to setup and commission. The Alarm Summary display shall support filtering by time and date, database partition or source of the alarm. The fields shown on the alarm summary must be configurable and it shall be easy to move or change the alarms fields displayed. It shall be possible to apply filters to the list of alarms to limit the view of alarms to those which match the filter. Filters may include multiple dimensions and wildcards and shall also be able to be saved and restored for reuse. More detail about an alarm shall be obtained from a configurable details screen which shows all fields associated with that alarm. It shall be possible for the operators to add comments to the alarm and these comments shall be stored with the alarm.

The alarm summary shall be capable of displaying a summary of the current alarms by location as well as the highest priority alarm within the corresponding location. The alarm summary shall be filtered based on the selected locations from the location pane.

The alarm summary shall support a simple method to reconcile recurring alarms into a common alarm message. This will prevent nuisance alarms from flooding the alarm summary display. When the same alarm from a plant device recurs, the alarm display shall use a counter to represent how many times this alarm has occurred since last acknowledged. This alarm counter shall be a filterable field in the alarm display for all alarms. Each time an alarm recurs, the count shall be increased by 1 and the alarm message must have its date / time updated with the newest alarm instance. Each alarm message shall indicate when each alarm first occurred and how many times its recurred since last acknowledged. Whilst this alarm consolidation shall minimize alarm messages for the operator, the IBMS will always track each new alarm into the Event Subsystem thereby ensuring all alarms are present regardless of how often they have recurred.

#### *1.8.11.5. Integrated Workflow for Shelving of Distracting / Nuisance Alarms*

The IBMS system shall allow you to temporarily hide a distracting/nuisance alarm without requiring other options or custom engineered solutions. This is a standard feature. When you shelve an alarm it is silenced, acknowledged, and removed from normal view. However, alarm messages, if configured, are still shown on the Message Summary. Also, further instances of the same alarm are combined with the existing shelved alarm, which continues to remain shelved.

A shelved alarm is automatically unshelved at the end of the shelving period, which depends on a number of factors, such as the reason it was shelved. Alternatively, you can manually unshelve it before the shelving period has expired.

#### *1.8.11.6. Dedicated Alarm Banner and Alarm Indicator*

A dedicated alarm banner shall appear on all displays showing either the most recent or oldest (configurable), highest priority, unacknowledged alarm in the system. This banner shall be clear when there are no unacknowledged alarms for the operator to process.

An alarm indicator shall also appear on all displays. This indicator will flash red (or another configured color) when there are any unacknowledged alarms pending in the system. This indicator will remain solid red if there are alarms, which have not returned to normal but which have all been acknowledged. The indicator will be clear if there are no points in an alarm condition.

#### *1.8.11.7. Alarm Logging*

As well as being logged on the printer, alarms shall be logged to an event file for future retrieval in alarm reports or archived to removable media.

#### *1.8.11.8. Alarm Response Function Keys*

The following dedicated function keys shall be provided on the keyboard for alarm action:

**ACKNOWLEDGE**

After moving the cursor to the point in alarm on the screen and selecting the point the operator shall be able to acknowledge an alarm by pressing this key. This action shall be logged in the event file and on the printer showing the operator ID with the alarm.

**ALARM SUMMARY**

By pressing a dedicated key at any time the operator shall be able to view a display showing all currently active alarms. The alarm messages shall be color-coded showing priorities. The operator shall be able to view the alarms according to priority or sorted based on other fields. It shall be possible to acknowledge alarms from this display and also go to the associated display defined for the point.

**ASSOCIATED DISPLAY**

After moving the cursor to the point in alarm on the screen and selecting the point the operator shall be able to bring up the display applicable to that alarm by pressing this key.

Just selecting the associated display key directly will bring up the associated display for the point currently on the alarm banner. This is generally a custom graphic showing the location of the alarm in the facility.

#### *1.8.11.9. Alarm Acknowledgement*

The system shall provide for efficient alarm acknowledgement in a number of ways as follows:

- Selection of any POINT.PARAMETER from a custom graphic and pressing the dedicated acknowledge push-button
- Right-clicking on any POINT.PARAMETER from a custom graphic and selecting 'Acknowledge Alarm' from the standard drop-down menu
- Selection of the alarm banner and pressing the dedicated acknowledge button
- Selection of the alarm in the alarm summary display and pressing the dedicated acknowledge button
- By performing a page acknowledge from the alarm summary display. In UL restricted IBMS systems this page acknowledgement shall be disabled.

On acknowledgement by the operator, the flashing indicator shall turn steady, and the point value shall remain colored with the alarm priority color, on any system or custom graphic. The acknowledgement shall also be logged in the Event database identifying the operator or station that acknowledged the alarm. If the point goes out of alarm before being acknowledged by the operator, the alarm shall be shown by a different indication and remain in the list until specifically acknowledged by the operator. If a point is not acknowledged within a configurable period of time, then an additional alarm can be generated and reassigned to another Location to allow other operators to take action

#### *1.8.11.10. Alarm Filtering*

The Alarm Summary shall be able to filter the alarms displayed to the operator. All columns on the alarm summary shall be able to be used as part of a filter allowing sophisticated filters to be configured e.g. all alarms from this particular point, with this value, during this period. Filters shall be able to be saved and restored so that previously configured filters can be reused. It should also be obvious to operators when a filter has been applied to the Alarm Summary.

#### *1.8.11.11. Alarm Link to Digital Video Recordings*

The system shall allow the linking and display of digital video recordings pertaining to alarms. If there is any video footage in digital format which is relevant to an alarm, then the alarm summary shall indicate this by the use of a special icon on the alarm. By selecting the icon, the operator can then replay the relevant digital video footage of the alarm incident.

#### *1.8.11.12. Print Alarms as a Report*

The filtered alarm summary should be able to be printed directly as a report. From the alarm summary page, it shall be possible to view the current filtered list of alarms via a print preview button. This shows what the alarms will look like when printed to the configured report printer. From the alarm summary, it shall be possible to print the alarms directly using the print button.

#### *1.8.11.13. Additional Alarm Information*

The IBMS system shall provide support for an additional message to be tagged to the alarm. This message shall provide the operator with additional information on the alarm but shall not clutter the alarm summary. It shall appear in a separate message summary at the same time as the alarm appears in the alarm summary. The messages can be pre-configured and then simply attached to individual points by means of a message ID.

#### *1.8.11.14. Advanced alarm management*

The IBMS shall be capable of advanced alarm management, which includes set stages of alarm handling. The stages shall be:

- Silence alarm condition
- Acknowledge and action alarm condition
- Respond to alarm condition by using pre-defined responses
- Optionally reset alarm

All actions shall be recorded in the event file for retrieval and auditing purposes.

When an alarm is silenced, an instruction page for the alarm will be displayed. The alarm may then be acknowledged from this page and alarm handling action completed.

Once the alarm is acknowledged and appropriate action has been taken, the operator may move to the response page to select from up to 100 user-defined responses to be logged in the event file. Alternatively, the operator shall be able to enter his or her own response, which will also be logged in the event file. At the same time the alarm is removed from the alarm file. Optionally, the point shall remain on the alarm summary until a manual reset operation is performed.

It shall be possible to enable/disable this feature on a point-by-point basis given the appropriate system privilege level.

### 1.8.12. **Reporting**

The system shall support a flexible reporting package to allow easy generation of report data. The reports provided shall include pre-configured standard reports for common requirements such as Alarm Event reports and custom report generation facilities that are configurable by the user.

A report detail display shall allow naming of reports, scheduling information and the destination of the report. The report destination shall be a printer, operator interface or internal file. The report output format shall be HTML (Hypertext Mark-up Language), Microsoft Word or RTF format.

#### *1.8.12.1. Report Activation*

Reports shall be activated in one or more of the following ways:

- Periodic activation at user specified intervals
- Operator Demanded
- Event Initiated e.g. Alarm from a point value
- Application Initiated
- Printed directly from the alarm/event summary

#### *1.8.12.2. Standard Reports*

The following pre-formatted reports shall be available on the system:

- Access Level Report
- After Hours Report
- Alarm/Event Report
- All Points Report
- Cardholder (visitor) Detail Report
- Cardholder List Report
- Card Usage Report
- Cardholder Zone Report
- Door History Report
- Employee List Report
- Group Card Trail Report
- Occupancy Report

- Operator Trail Report
- Point Attribute Report
- Point State Changes Report
- Present in Zone Report
- Time Period Report
- Unused Cards Report
- Unused Door Access Report
- Zone Access Report
- Zone Information Report

(Note: additional application specific reports shall be described later in this document)

Configuration of these reports shall only require entry of the schedule information, and other parameters such as Point Name or wildcard, filter information, time interval for search and destination printer to fully configure the report. Specifically, no programming or scripting shall be required.

#### *1.8.12.3. Access Level Report*

Lists all access levels matching a specified search criteria filtered by the zones and allocated Time periods.

#### *1.8.12.4. After Hours Report*

A report shall be provided to produce a summary of all Alarms occurring during the period specified by the operator as “After Hours”

#### *1.8.12.5. Alarm/Event Report*

A report shall be provided to produce a summary of all events of a specified type for nominated points occurring in a time period. The time period may be specified as an absolute start and end date and time, or as a period relative to the current time. This report shall also be able to produce a summary of all changes made by a specific operator.

#### *1.8.12.6. Alarm/Event SQL Reporting Services Report*

This Sample reports lists a summary of alarms and events by location and by date and time. It includes a graphic summary.

#### *1.8.12.7. All Points Report*

A report shall be provided to produce a list of point information, including point name, description, point type, engineering units, and current values. Report configuration shall allow filtering based on a wide variety of criteria.

#### *1.8.12.8. Cardholder (visitor) Detail Report*

Lists all information for cardholders who correspond to a specified search criteria.

#### *1.8.12.9. Cardholder List Report*

A report shall be provided to produce a comprehensive listing of cards and cardholders.

It shall be possible to provide searching and filtering criteria based on any cardholder field. The cardholder details on which the report is based shall allow details to be specified as a range, or as matching or partially matching as applicable.

#### *1.8.12.10. Card Usage Report*

A report shall be provided which calculates the total number of access movements (including no movements) for cardholders over a given period of time. The time period may be specified as an absolute start and end date and time, or as a period relative to the current time. This report shall provide the ability to search by cardholder fields as defined by the specified search criteria based on any cardholder field.

#### *1.8.12.11. Cardholder Zone Report*

Lists all cardholders who have access to the specified zones.

#### *1.8.12.12. Door History Report*

A report shall be provided to list all cardholders who presented a card at any specified door or group of doors monitored by the IBMS within a specified time period. The time period may be specified as an absolute start and end date and time, or as a period relative to the current time. The report shall contain the time and date and card number for each card presentation.

#### *1.8.12.13. Employee List Report*

Lists all employees in a defined organization

#### *1.8.12.14. Group Card Trail Report*

A report shall be provided so that when requested, the report shall search the database for cards corresponding to specified search criteria based on any cardholder field. It shall then show all doors accessed by these cardholders in a specified time period. The time period may be specified as an absolute start and end time, or as a period previous to the current time. The report shall contain the date and time of access and the point identifier of each door accessed.

#### *1.8.12.15. Occupancy Report*

A report shall be provided so that when requested, the report shall determine which cardholders are in a specified zone at that time. Listing the Doors accessing the area for both the IN and OUT

directions shall specify the area. It shall be possible to include only certain cardholders in this report, as defined by the specified search criteria based on any cardholder fields.

#### *1.8.12.16. Operator Trail Report*

A report shall be provided to produce a summary of all operator actions relating to a specific operator in a specified period.

#### *1.8.12.17. Point Trail Report*

A report shall be provided to produce a summary of all events of a specified type occurring in a period on nominated points.

#### *1.8.12.18. Point Attribute Report*

A report shall be provided to points selected by one of the following attribute criteria:

- Out-of-service
- Alarm suppressed
- Abnormal input levels
- In Manual mode

#### *1.8.12.19. Point State Changes Report*

Lists all information about Time Periods matching a specified search criteria.

#### *1.8.12.20. Present in Zone Report*

Lists all cardholders present in defined zone. Useful for auditing and mustering.

#### *1.8.12.21. Time Period Report*

Lists all information about Time Periods matching a specified search criteria.

#### *1.8.12.22. Unused Cards Report*

Lists cards that have not accessed any door or zone within defined date / time range. Useful for compliance auditing

#### *1.8.12.23. Unused Door Access Report*

Lists Doors that have unused access privileges, to enable further tightening of security to support compliance audits and threat modeling.

#### *1.8.12.24. Zone Access Report*

List all cardholders that have accessed a Zone in predefined date / time range. Used for compliance auditing.

#### *1.8.12.25. Zone Information Report*

A report shall be provided which lists zones in the facility to which cardholders have access. This report is to allow system administrators to check which parts of their facility are accessible by which cardholders.

#### *1.8.12.26. Access Data Import/Export Report*

An export feature must be provided to create a file containing cardholder related details in an ASCII format ready to be exported from the IBMS into a third party database package. It shall also be possible to import ASCII files into the IBMS to update the IBMS from information from other third party database systems. The following information shall be able to be configured for import or export in the report:

- Cardholder Details
- Zones
- Time periods
- Access permissions

In order to reduce duplication and export data file size, the operator shall be able to choose to only include cardholders that have been modified since a particular date.

It shall be possible to configure the report such that after an import operation, a download to the field devices shall take place automatically.

### 1.8.13. **Custom Reports**

In addition to standard reports, configurable report generation facilities must be provided to allow custom reports to be produced. They shall be able to be configured at any time with the system online, and shall be able to access any database values. At least three methods of custom report generation shall be available, including the following:

#### *1.8.13.1. Microsoft Excel Report*

The IBMS shall provide the facility for the use of Microsoft Excel as a reporting tool – allowing calculations such as summations, maximal, minimal and standard deviations, and the production of graphs, charts and tables. Systems that do not provide support for Microsoft Excel in this respect shall not be acceptable.

Data accessible for Excel reporting shall include alarms, events, and point parameter values.

#### *1.8.13.2. ODBC Report*

The IBMS shall be capable of providing selected data in an ODBC format for the purpose of extracting data and creating custom reports. It shall be possible to access tables of data from the IBMS through an ODBC compliant tool such as Crystal Reports or SQL Server.

It shall be possible to incorporate the activation of custom reports created through the ODBC compliant tool through the standard IBMS report subsystem. Example reports shall be provided to illustrate how to access the ODBC data in the IBMS.

#### *1.8.13.3. SQL Server Reporting Services Custom Report*

Being based on SQL Server, the IBMS system shall support a simple custom report format using the SQL Server reporting services. This shall enable customer reports to be designed in either Reporting Services, or Visual Studio and shall enable access to all point data, cardholder data and alarm and

event data. The design of the SQL Custom Reports solution shall be available from any of the LAN connected Operator Workstations. No addition license fees shall be required to utilize this standard custom reporting solution. To facilitate rapid development of simple custom reports the system shall be delivered with template reports.

### 1.8.14. **User Definable database**

In order to support other types of data such as user entered or calculated data from application programs, the system shall also provide a User Definable database area that can be fully integrated into the system. Data contained in this database must be accessible by:

- Custom Graphics
- Custom Reports
- Application Programs
- Network Applications using a Network API

### 1.8.15. **Point Initiated Programs (PIPS)**

In addition to standard point processing functions, the system shall allow additional processing through the use of standard PIPS that may be attached to any points. Typical functions to be provided by these PIPS are listed below:

Arithmetic Calculation

Boolean Calculation

Maximum/Minimum Value

Composite Alarms

Integration

Run Hours Totaled

Group Alarm Inhibit

Report Request by Point Change

Application Program Request (By point value change or cyclic period)

Alarm Transportation

Value Transportation

Door Activity Task Request

Security Area Seal / Unseal

Alarm or Point Value Change Graphic Call-up

Value Change Group or Area Alarm Inhibit

These PIPs shall be either configurable standard algorithms, or preference is that a VBscript can be written as a library function and attached to points within the IBMS.

### 1.8.16. **Historical Data Archiving**

The system shall support archiving of historical data to allow a continuous record of history to be built up over a period of time. Archived data may be stored on the hard disk of the system or a remote network drive or moved off-line to removable media such as DAT tape, or optical disk. The number of archives maintained on the system before transferal to off-line media shall only be limited by the size of the hard disk or remote network drive. The system shall allow the user to define the specific intervals of history to be archived to avoid archiving of unnecessary data.

Once archived, the data shall be available for re-trending through the system trend facilities in combination with the current on-line history or other archives. Providing the archived history is present on the IBMS Server's hard disk or remote network drive, the trend facilities must be able to access it transparently for display, when a user scrolls beyond current on-line history limits.

The IBMS will support display of trend data from up to 10 years of age. Any required upgrades or updates to the IBMS system shall also be capable to preserve the Historical information to enable review of data from any earlier release of the system

### 1.8.17. **Time Schedules**

It shall be possible to specify time schedules for the control of all IBMS points. It shall be possible to control a range of a single point to a large number of points from a single schedule. A single time schedule shall define the control to any combination of day and time.

The IBMS scheduling management system must be more flexible than providing weekly schedules with a provision for a finite number of special occasions/holidays. The IBMS scheduling system shall allow schedules to be entered that recur on a non-weekly basis or only occur once on a given day in the future.

Examples:

- Schedules shall be capable of recurring on any multiple of weeks (every 1 week, every 2 weeks, every 7 weeks, etc.)
- It shall be possible to enter a schedule that only occurs once on any given day in the future

The IBMS time schedule must also provide the ability to override the normal schedule for holidays or special occasions. The user shall be able to create multiple different grouping of dates (Calendars) that can be assigned to individual points as applicable.

Examples:

- Daily or weekly recurring time schedules; capable of recurring until a specified date or without end (Mon-Fri 7:00 to 18:00, Thursday 7:00 to 22:00)
- Time schedules active for greater than 24 hours (Saturday-Sunday 9:00 to 14:00)
- Time schedules that occur on a specified group of Calendar Days (e.g. Holidays)

Configuring time schedules must be done through a graphical user interface whereby the operator selects the appropriate time span from a calendar. Systems where times and days must be manually entered or managed by an external spreadsheet type form are not acceptable. The user interface must support the capability of navigating to any future date to allow the user to enter a time schedule. The user interface must provide graphical feedback to indicate to the user whether the time schedule is a:

- One-off exception schedule
- Part of a recurring series
- Recurring schedule that has been altered from the series
- Part of a calendar schedule
- Active Schedule
- Schedule that has completed
- Successfully downloaded schedule to the device (if applicable)

The user interface must allow the user to view time schedules that have been configured in the past, present, and future in a graphical calendar interface. It shall be possible to increase or decrease the amount of time on a schedule which is currently active.

Where the control device supports an internal time schedule program, the IBMS shall be able to upload, display, modify and download the control device time schedules. Support for the control device time schedules shall be in addition to the IBMS time schedules.

## 1.9. **Open Systems Integration**

Any of the following Open Protocol Standards shall be used for integration of 3rd party devices or systems

### 1.9.1. **Modbus**

The IBMS server shall provide an integrated interface to devices using the Modbus RTU protocol, where the IBMS server shall be the 'master' and the external device or system shall be the "slave". The Modbus Interface shall support the following function codes:

| *Modbus Function Code* | *Meaning* |
|---|---|
| 01 | Read Coil/Status |
| 02 | Read Input Status |
| 03 | Read Holding Registers |
| 04 | Read Input Registers |
| 05 | Force Single Coil |
| 06 | Preset Single Register |
| 16 | Preset Multiple Registers |

The IBMS shall also support user definable data formats for Modbus devices to accommodate the wide variety of formats in use in the industry.

### 1.9.2. **BACnet (ANSI / ASHRAE 135)**

The IBMS system shall be capable of communicating to other building subsystems using the ASHRAE standard BACnet. The IBMS shall be capable of acting as both a BACnet Advanced Operator Workstation and also BACnet Gateway. The IBMS must be BTL tested and certified to comply with the minimum standard of BACnet AWS V1.15 (revision 15) and the PICS statements and certification shall be published on the BTL website. The BACnet capability shall support all of the following standard BACnet objects:

- Accumulator
- Analog Input
- Analog Output
- Analog Value
- Averaging
- Binary Input
- Binary Output
- Binary Value
- Calendar

- Command
- Device
- Event Enrollment
- File
- Group
- Loop
- Multistate Input
- Multistate Output
- Multistate Value
- Notification Class
- Program
- Pulse Converter
- Schedule
- Trendlog

#### *1.9.2.1. BACnet Advanced Operator Workstation*

An integrated BACnet AWS Workstation shall be provided which allows the monitoring of BACnet devices via data acquisition and control.

The BACnet Operator Workstation shall support the following BACnet Interoperability Building Blocks:

| | | |
|---|---|---|
| **Data Sharing** | Data Sharing - ReadProperty-A | DS-RP-A |
| | Data Sharing - ReadProperty-B | DS-RP-B |
| | Data Sharing - ReadPropertyMultiple-A | DS-RPM-A |
| | Data Sharing - WriteProperty-A | DS-WP-A |
| | Data Sharing - WriteProperty-B | DS-WP-B |
| | Data Sharing - WritePropertyMultiple-A | DS-WPM-A |
| | Data Sharing - COV-A | DS-COV-A |
| | Data Sharing - COVP-A | DS-COVP-A |
| | Data Sharing - COV-Unsubscribed-A | DS-COVU-A |
| | Data Sharing - View-A | DS-V-A |
| | Data Sharing - Advanced View-A | DS-AV-A |
| | Data Sharing - Modify-A | DS-M-A |
| | Data Sharing - Advanced Modify - A | DS-AM-A |
| **Alarm & Event Management** | Alarm and Event - Notification-A | AE-N-A |
| | Alarm and Event - ACK-A | AE-ACK-A |
| | Alarm and Event - Alarm Summary View-A | AE-AS-A |
| | Alarm and Event - LifeSafety - A | AE-LS-A |
| | Alarm and Event Management - View Notifications-A | AE-VN-A |
| | Alarm and Event Management - Advanced View Notifications-A | AE-AVN-A |

| | | |
|---|---|---|
| | Alarm and Event Management - View and Modify-A | AW-VM-A |
| | Alarm and Event Management - Advanced View and Modify-A | AE-AVM-A |
| | Alarm and Event Management - Alarm Summary View-A | AE-AS-A |
| | Alarm and Event Management - Event Log View-A | AE-ELV-A |
| | Alarm and Event Management - Event Log View and Modify-A | AE-ELVM-A |
| **Scheduling** | Scheduling - Advanced View and Modify-A | SCHED-AVM-A |
| | Scheduling - View and Modify-A | SCHED-VM-A |
| | Scheduling - Weekly Schedule-A | SCHED-WS-A |
| **Trending** | Trending - Automated Trend Retrieval-A | T-ATR-A |
| | Trending - Automated Multiple Value Retrieval-A | T-AMVR-A |
| | Trending - View-A | T-V-A |
| | Trending - Advanced View and Modify-A | T-AVM-A |
| | Trending - Archival-A | T-A-A |
| **Device & Network Management** | Device Management - Dynamic Device Binding-A | DM-DDB-A |
| | Device Management - Dynamic Device Binding-B | DM-DDB-B |
| | Device Management - Dynamic Object Binding-A | DM-DOB-A |
| | Device Management - Dynamic Object Binding-B | DM-DOB-B |
| | Device Management - Device Communication Control-A | DM-DCC-A |
| | Device Management - TimeSynchronization-A | DM-TS-A |
| | Device Management - UTCTimeSynchronization-A | DM-UTC-A |
| | Device Management - ReinitializeDevice-A | DM-RD-A |
| | Device Management - Backup and Restore-A | DM-BR-A |
| | Device Management - Restart-A | DM-R-A |
| | Device Management - List Manipulation-A | DM-LM-A |
| | Device Management - Object Creation and Deletion-A | DM-OCD-A |
| | Network Management - Connection Establishment-A | NM-CE-A |
| | Device Management - Automated Network Mapping-A | DM-ANM-A |
| | Device Management - Automatic Device Mapping-A | DM-ADM-A |
| | Device Management - Automatic Time Synchronization-A | DM-ATS-A |
| | Device Management - Manual Time Synchronization-A | DM-MTS-A |

#### *1.9.2.2. BACnet Functions available from the User interface*

This shall be document in the BACnet PICS statement as compliant to BACnet AWS v1.15

### 1.9.3. **OLE for Process Control (OPC)**

The IBMS server shall provide an integrated OPC Client, integrated OPC Data Access Server, and OPC Alarm and Event Server.

- The OPC Client shall support the OPC Release 2.0 Data Access as a minimum.
- The OPC Server shall support OPC Release 1.0A and OPC Release 2.0 Data Access OPC interfaces as a minimum.
- The OPC Alarm and Event Server shall allow an OPC alarm and event client to receive alarm and event information and be compliant to OPC Version 1.02 foundation Alarm and Event Specification.
- The OPC Historical Data Access (HDA) Server shall be designed to support remote OPC HDA Servers from connecting to the IBMS system and reading all stored point history.

### 1.9.4. **LonWorks**

The IBMS server shall provide a LonWorks Client to allow communication to LonWorks Controllers. The LonWorks interface shall use Echelon IzoT Net Server Network to maintain, monitor, and control LonWorks networks. It shall be based on the OpenLNS Server that is the foundation for the most capable, popular tools for designing, installing, maintaining, and monitoring IzoT and traditional LonWorks systems, and it ensures interoperability of devices, applications, and tools.

## 1.10. **Data Exchange and Data Transfer**

The IBMS system shall have the capability to interface to the point database of other IBMS systems (i.e. nodes) on a TCP/IP network. This shall enable both the acquiring of point data and issuing control outputs to and from connected IBMS systems.

This data exchance shall support report by exception communincations, with a fixed background poll period that is easily changed.

## 1.11. **Data Exchange with Microsoft Excel**

The system must be capable of exporting bulk data to Microsoft Excel. As a minimum the following shall be supported:

- Allow retrieval of data either periodically or snapshot
- Allow retrieval of data via POINT.PARAMETER requests
- Allow retrieval of tag names, descriptions etc
- Allow retrieval historical data
- Writing of values from Excel back to the supervisory system

1.12. **Accessing the IBMS from third party web pages**

Web-page controls and a web server interface to the IBMS shall be optionally provided, which allow tenants or other users to monitor & control a variety of IBMS-supervised functions via their own Web pages created for their own Intranet or Internet and viewed from a standard web-browser. For example, it shall be possible for building tenants to be able to view floor graphics via a dedicated or existing building Intranet, and to be able to monitor and control floor lighting and ambient temperature information.

It shall be possible to limit web browser access to IBMS facilities by means of standard web and networking techniques.

1.13. **Paging and external annunciation of System Alarms**

The IBMS shall optionally provide a facility for sending alarm text from configured points to the following external systems:

- Alphanumeric pagers
- Digital mobile phones with text message (SMS) support
- Email
- SNMP message

Each point's paging priority threshold shall be individually configurable, and individually enabled or disabled. Each external device configured in the system shall have individually selectable times and days of operation, an alarm priority threshold, and an alternative device for use in escalation of unacknowledged alarms.

1.14. **Acknowledgment of remote alarms received from paging system**

For alarms received on Digital Mobile phones via SMS message, the IBMS shall optionally provide a ability to allow acknowledgement of these alarms via the same SMS solution. This is to allow remote users to clear the alarm status thereby indicating the alarm status has been received and acknowledged.

1.15. **Database configuration tool**

A database configuration tool shall be provided with the IBMS system that shall allow configuration of all point records, printers, controllers, and Operator Workstation connections. This utility shall be in the form of a relational database and operate in client workstation computer using a modern graphical environment such as Windows 10. The utility shall also have the ability to export information to and import information from Microsoft applications such as Microsoft Excel. Systems that do not provide support for Microsoft Excel in this respect shall not be acceptable

Only users with sufficient security access shall be able to configure the database, and this shall be possible while the system remains on-line. Configuration shall not require the need for any programming, compiling or linking and shall not require shutting down or restarting of the system.

In addition, historical data collection shall not be interrupted for points not affected by configuration changes.

It shall be possible to launch the database configuration tool from the operator workstation interface. The utility shall have the ability to configure database changes and download them either from the IBMS server directly or remotely via the network. The remote download is to provide password protection.

It shall be possible to modify a range of communications and other parameters for each device. The parameters of a particular device made available for modification shall be specific to the device or hardware item being configured – for example baud rate, parity, data and stop bit information in the case of serial devices. Hardware configuration utilities that rely solely on text-based configuration files shall not be acceptable.

All documentation for the configuration utility shall be provided on-line. The help facility shall operate using standard Microsoft features such as context sensitive help using the F1 function key.

The utility shall provide features that reduce configuration time of the IBMS system. These features shall include adding multiple points, controllers etc. at once. The utility shall automatically increment names or numbers of any information that is required to be unique by the IBMS system (such as point names). The user shall be able to select multiple items (such as points) and then edit fields that are common to all selected items to assist in global changes. Standard copy and paste facilities are to be provided by the utility.

The utility shall provide functionality to create a hierarchical structure of locations to model the system. This model is to be used to manage system information (such as points) as well as user scope of responsibility. The hierarchical model shall support a 10-layer deep architecture. It shall be possible for the locations in this model to span multiple servers.

The utility shall also support free format text fields, which the user can use for additional information such as cabinet or wire numbers. These additional fields shall be simple extensions to existing items in the database such as IBMS points.

A filtering mechanism shall be provided with the utility so that the user need view only relevant information. The filter shall provide standard choices for the user to select, and also provide user defined filtering.

Database management reports shall be provided by the utility as standard. The utility shall also provide support for ad-hoc reporting facilities for engineering use.

### 1.16. **Application Programming Interface**

Two types of application programming interface (API) are required, the first is for applications written on the IBMS server and the second is for applications that are required to run on network based clients (that are not necessarily Operator Workstations).

The IBMS system API's must have support for either Visual Basic or C++ or both. Proprietary programming languages are not acceptable.

The API on the IBMS server requires the following functions as a minimum:

- Read and write to points in the database
- Access to historical data
- Initiate supervisory control actions
- Access to the alarm/event subsystem
- Access to user-defined database
- Provide a prompt for operator input.

The API on the network-based clients shall be designed using modern web services and support the following functions as a minimum:

- Read and write to points in the database
- Access to historical data
- Initiate supervisory control actions
- Ability to search for points and return matching list
- REST based services

### 1.16.1. **Automation Engine**

The IBMS must be delivered with a simple to use Automation Engine that enables quick on-line configuration of routine, repetitive tasks to be performed automatically and offloaded from an operator onto the IBMS platform. This shall be fully supported and require zero custom programming. The automation must self-document all the automation rules, to enable quick understanding from support and management personnel.

Automation rules can be configured to perform various routine tasks such as:

- Sending live video from a camera located by a door to a selected Station if that door is forced open.
- Calling up a plant display on a specific Station when a point associated with the plant goes into alarm.
- Locking all doors in a specific area if an alarm is raised.
- Automating repetitive tasks to enable a faster response to events in the facility with greater precision and accuracy.

The Automation rules shall support exporting from one IBMS server and imported into another to facilitate system configuration and maintenance.

Automation Rules shall support use of wildcard on input conditions, to enable 1 rule to be applied across every point in the IBMS system.

The output actions from the Automation Rules shall support numerous tasks on each rule and shall include:

- Video recording on associated cameras
- Video callup on surveillance monitors
- Control of points
- Time delay between upto 15 output actions
- Callup of an associated graphic map on the associated operation station. This indirect association shall be automated with no programing, and is designed to support as an example, up to 65000 points events from calling up their matching graphic map in event of an alarm all from 1 simple rule.
- Upto 3 automatic retries on output control requests
- Automatic filters to prevent nuisance alarms from actuating many repeated output actions.
- Integration with an cloud based remote alert management system, to enable rapid broadcasting of an action to tens of thousands of personnel.
- Cardholder comparison from their cardholder image against the CCTV surveillance monitor

Configuration of the rules in the automation engine, shall be protected by scope of responsibility and passwords inside the operation workstation.

### 1.16.2. **Server Scripting Engine**

The IBMS system must have the ability to extend its functionality easily by the addition of small script code to certain server functions. This will enable additional customer specific functionality to be easily added to point, report and server processing. For example, a script shall enable a calculation to be performed and a number of points to be controlled based on another point going into alarm state. Scripts shall be able to be attached to point processing, report generation, server startup and shutdown, or executed on a periodic basis.

The scripting engine must support a standard scripting language such as Microsoft's VBScript. Access to the scripts shall be through an inbuilt scripting editor which provides key work support and syntax checking as well as an extensive range of online help including a large number of worked examples. Proprietary scripting languages shall not be acceptable.

Scripting functionality shall be in addition to a full Application Programming Interface as described in section 1.16.

### 1.17. **Diagnostic Capabilities**

The IBMS system must enable easy diagnostics of the health of the system.

#### 1.17.1. **Diagnostic Framework**

The IBMS system must make all diagnostic information viewable through an easy to use user interface and shall be able to be easily exported as a stand alone collection of material for later analysis. The capabilities shall include the ability to run automated tests, record the reproduction of a failure, as well as collection and organization of all available diagnostic information (files, logs, and system settings).

Automated tests shall be possible to determine the health of the IBMS. The automated tests shall automatically set the appropriate debugging parameters and store the results for viewing at anytime. The results shall be stored in a file that can be sent for assistance in remotely diagnosing an issue.

The ability to record all system information at the time of issue reproduction shall be automated from within the diagnostic framework. The recordings shall be capable of being defined to capture the necessary level of system information at the time of issue reproduction.

All available IBMS diagnostic information shall be collected and organized for viewing as well as to create a diagnostic package to simplify remote issue resolution. This information shall include the following:

- Communications traces to selected controllers
- All system log files
- Details on system software installation
- Application status information

It shall not be necessary to be an expert user in the system to gather diagnostic information.

# 2. BUILDING Management Specification

1.18. **General**

The Integrated Building Management System (IBMS) to be provided shall perform the following general functions:

- Building Management and Control
- Monitoring and Control of Controllers, Remote Devices and Programmable Logic Controllers including sensors, actuators, environmental delivery systems (chillers, boilers, room climate control, lighting systems, electrical systems etc.)
- Operator Interface to allow general supervision of room controls
- Video display integration
- Data collection and Historization
- Alarm Management
- Trending
- Report Generation
- Network Integration
- Controller Scheduling
- Data exchange and integration with a diverse range of other computing and facilities systems using industry standard techniques.

The system shall employ all standard features and functions as described in Section 1 to monitor and control building equipment. At a minimum, the following data shall be accessible:

- Space temperature
- Space temperature set point
- Occupancy status
- Operating mode
- Window status
- Valve positions
- Air volume flow

- Percent terminal load
- Time schedules
- Zero energy bands
- Room name
- Terminal type e.g. fan coil

In the event of a power failure or disconnection from the IBMS, the controllers shall continue to be fully operational with full time program capability.

## 1.19. **Specific Building Management Functions**

### 1.19.1. **BACnet AWS certification**

The IBMS must be corticate by BTL to be compliant to the BACnet AWS V1.15 standard, and this must be evidenced on the BTL website. Essential to this compliance is clear evidence of the BTL testing results, and the IBMS PICS statement to conform compliance.

### 1.19.2. **LonWorks Capability**

The system shall provide a direct Interface to LonWorks. The interface shall provide the functionality necessary to normally operate a building management system based on LON devices including alarming, data acquisition, supervisory control, and trending.

This interface shall use standard components such as PC LonTalk Adaptors (PCLTA) or Ethernet to LonTalk routers such as the Echelon I-LON routers to connect the IBMS to the LonWorks network and devices. Solutions requiring gateways or data servers (e.g. OPC to LON) are not acceptable.

The IBMS Interface to LonWorks should be based on LON Network Services (LNS) Release 3.2 or later. The interface shall allow access to be configured for any Network Variable (NV) or Configuration Property (CP) in the LON device. Any LON devices conforming to LonMark functional profiles shall be easily integrated into the IBMS without the need for software changes in the IBMS.

The system shall allow standard graphics to be created for configurable LonWorks devices so that it is possible for all instances of points for the same device type to use the same graphic.

The LonWorks Interface shall be compatible with any LonWorks vendor whose products conform to standard LonMark profiles.

The Lonworks interface must be tested to support thousands of Lon devices, separated across separate subnets when needed, into 1 single synchronous IBMS database. Evidence of this scalability is essential.

### 1.19.3. **Controller Scheduling**

A controller scheduling tool shall be provided for creating, editing and maintaining controller time schedules. The controller scheduling tool shall be constructed in a way that allows compatibility with new controller types with minimal additional development.

The controller scheduling tool shall allow downloading of schedules to several (supported) controllers in a single operation by provision of an integrated graphical interface.

The controller scheduling tool shall provide a clear, graphical indication of the status of each downloadable schedule element, and shall automatically recover and complete any schedule download which, for any reason, has failed or been interrupted.

### 1.19.4. **Smoke and Critical Process control**

The building management portion of the IBMS shall be able to provide for control and monitoring of HVAC functions associated with smoke control and when used with appropriate hardware shall be listed by UL under category UUKL for this purpose. When used for critical process or other safety functions, such as boiler safety monitoring, the system shall also be UL Listed under category QVAX.

For further information on controllers and field devices, insert *General Guide Specification for Building Management systems Section: 3 Primary Plant Controllers, Section 4:Room Control Units, Section 5: Field Devices* here to define panel and field device functionality.

# 3. LIFE SAFETY Management Specification

1.20. **General**

The IBMS shall control and monitor the Life Safety Systems including full controls for fire alarm and smoke control functions.

The IBMS shall include:

- Operator Workstations for operators (Guard and/or Building Management)
- CCTV Switchers or Integration with Digital Video Systems
- Fire Alarm Controls and associated devices

1.21. **Interface and integration**

1.21.1. **General Interface Features**

The IBMS shall provide the following features though a tightly integrated interface to a range of fire panels:

- UL864 Category UOJZ Listed as the primary means to control and monitor the fire system.
- UL864 Category UUKL Listed as the primary interface for the smoke control/smoke management system.
- Ability to configure with fully redundant servers and communications channels.
- Support for either Token-Ring or Ethernet communications directly to the fire panels to eliminate proprietary networks and additional wiring.
- Support for direct connection of FS90 fire and security busses to the server.
- Point displays that combine the real-time analog value returned from a smoke or heat detector to be combined with the state of the device to improve alarm assessment and facilitate troubleshooting.
- Support for over 300,000 life safety points through any single IBMS server.
- Support for over 350,000 life safety points using the Distributed System Servers as defined in section 1.1.4.
- Support for up to 40,000 points from a single LAN interface connection

- Display of the operating system software versions and database versions from XLS fire panels.
- The following command functions will be provided for all integrated fire alarm panels: Reset, alarm silence, change sensitivity setting, audio channel select, audio message select, enable by point or zone, disable by point or zone, output on/off.
- The system shall display analog values from and provide trending capability for addressable devices such as smoke and heat detectors.
- A standard facility for verifying a manual action that is required to occur within a specified time period. Such a facility can be used to effect confirmation of a person's presence.
- Detailed fire panel diagnostic information shall be displayed from the IBMS such that the cause of a trouble signal can be remotely determined.

### 1.21.2. **Controller Features**

For further information on controllers, insert either:

- *FS90Plus Guide Specification* or
- *XLS200/1000 Guide Specification or*
- *XLS3000 Guide Specification, or*
- *XLS80e Guide Specification, or*
- XLS2000 Guide Specification, or
- XLS140 Guide Specification

in this section, to define panel and field device functionality.

# 4. SECURITY Management Specification

1.22. **General**

The IBMS shall control the following subsystems within a building:

- Access Control System
- Security System
- Digital Video System
- Ancillary Control System

The IBMS shall include:

- Operator (Guard and Building Manager) Stations for operators
- Access Control panels, card readers, electric strikes, door contacts, drop in bolts and the like
- Security control panels
- Passive infrared detectors, reed switches and the like
- Programmable Logic Controllers
- Digital Video Management

1.23. **Interface and Integration**

1.23.1. **General**

The IBMS server computer shall be capable of interfacing to the following panel types. The electrical interface technique shall conform to approved standards for:

- Security Controller
- Access Controller
- Lift/Elevator Access Controller
- Programmable Logic Controller
- Digital Video System

1.23.2. **Sub-system Local Databases**

All controller subsystems shall have distributed intelligence. Normal access control decisions shall be made at the local panel without reference to the IBMS Server.

In the event of failure in the communication link between a sub-system panel and the server computer, the access control sub-system shall be capable of buffering a minimum of 500 access transactions until communication are re-established with the server computer.

Similarly, the lift/elevator access controller shall be capable of maintaining its access time schedules for securing floors in the event of communication failure with the server computer. The local time schedules shall be uploaded to the server computer once the communication is resumed.

Changes in the server system database shall be capable of being downloaded to the relevant access controllers and the local databases of the connected sub-systems via the same physical communication links. Such downloading of data shall not disrupt normal data communications over the same links.

### 1.23.3. **Distributed System Servers**

#### *1.23.3.1. Cardholder Management System*

A method shall be provided to allow geographically separate IBMS servers to manage their own locally connected access controllers while sharing and interchanging data with other IBMS servers that are connected via a Wide Area Network.

Specifically, it shall be possible, within the limits of the configured operator permissions, to view, edit, and download card and cardholder information across a network of geographically distributed IBMS servers.

Card and cardholder access details specified from one IBMS server shall be available to remote IBMS servers to allow cardholders appropriate access to buildings and facilities whose access control is managed by the IBMS servers.

##### Downloading

A download of newly entered card or cardholder information shall automatically be initiated on each remote IBMS server when manually initiated on any local IBMS server. Such downloads may include multiple sets of cards or cardholders.

A method shall be provided for reporting of any failed remote download back to the requesting server.

There shall be an Operator Workstation display containing a list of all outstanding local downloads and outstanding locally initiated individual card downloads to remote sites. This display shall be restricted to viewing by operators with appropriate authorization.

Information on the download status of each item shall be available as part of the standard display for each card or cardholder.

##### Remote Server Availability

Failure of software or hardware in any one IBMS server, or loss of communications to any one geographic location, shall not cause loss of supervisory operations of the system as a whole.

Loss of communications to any one geographic location shall not impede supervisory operations to the controllers at the unreachable site if communications are still available locally.

It shall be possible to enter access cardholder details at any of the geographically separate IBMS servers, and have that information automatically copied to each other remote site where the cardholder requires access. If access is removed from a site, the local record shall be deleted from that site's server.

The local time of last modification, as well as the site of modification, shall be stored on each card and cardholder.

A flexible and consistent scheme shall be provided for restricting operator permissions to access card and cardholder information at remote sites.

### 1.24. **Cardholder Management System**

The IBMS shall store security related cardholder/passholder information in a relational database such as Microsoft SQL Server.

The cardholder database shall support at least 1,000,000 cardholders. The cardholder database shall be delivered with over 90 user definable fields for storing data specific to the requirements of different IBMS systems. It shall be possible to increase or decrease this number of user definable fields. Systems without the ability to increase the number of user definable fields shall not be accepted.

#### 1.24.1. **Cardholder database**

It shall be possible to define labels and field types for each of the user definable fields. It shall be possible to define lists of choices for certain user fields to avoid unnecessary typing, for example, defining a list of department names. It shall also be possible to modify the layout of cardholder fields on the display screen to alter the look to particular user's requirements. It shall also be possible to create more complicated calculations between user fields. For example, creating the value of one user field based on the value of two others. It shall be possible to define default values for all user fields, which shall be applied when the cardholder is first added to the system.

##### *1.24.1.1. Searching and sorting*

It shall be possible to define which user fields in the cardholder database are searchable fields. All searchable fields shall be able to be used to call up a list of cardholders who match a certain criteria. In addition, it shall be possible to search on multiple cardholder characteristics at one time, for example, all cardholders in department "X" who have a supervisor of "Y". A list of matching cardholders shall be displayed and an appropriate choice may be made.

##### *1.24.1.2. Multi-selection*

It shall be possible for multiple cardholders to be selected and a single edit to be performed on all of these cardholders selected. For example, it shall be possible to select all cardholders in department “X” and change their address to “Z” in a single operation.

#### *1.24.1.3. Templates*

The IBMS shall define templates in order to add groups of cardholders with predefined characteristics. A template shall contain all the relevant details for a particular group of cardholders such as all their user fields and access levels. When adding a new cardholder to this group using the template, the cardholder shall be added with the same characteristics as defined in the template.

### 1.24.2. **Cardholders and Cards**

It shall be possible to assign a single cardholder multiple cards for use in the IBMS. Multiple cards assigned to a single cardholder shall be able to be in different states. For example, it shall be possible for a single cardholder to have both an “active” card assigned and an “inactive”, “lost” or “stolen” card assigned.

It shall also be possible to support different technologies of access control cards in the one system. For example, a single cardholder may have a proximity card, a magnetic stripe card and a biometric template assigned to them.

Cards may be created and assigned to cardholders separately. It shall be possible to “return” a card when a cardholder no longer requires it, and then reassign it to another cardholder without having to delete and recreate the card.

When cardholders or cards are deleted or expired, or when a card is returned from use by a cardholder, the system shall automatically download this to the field controllers so these cards no longer provide access.

### 1.24.3. **Access Permissions, Time Periods and Zones**

#### *1.24.3.1. Time Periods*

The IBMS shall support a minimum of 256 time periods.

The operator shall be able to access a summary display listing all time periods and their descriptions. From this display the operator shall, if the operator is configured for the time period’s Organization code, be able to go to a time period detail display showing the time periods configurable parameters.

Once the changes have been saved the IBMS shall automatically download the new data before it is enabled in the Access Control System. This shall allow operators to make a number of changes but only be required to download once.

Each time period detail display containing changed data that has not been downloaded shall clearly indicate this to the operator via a flashing warning message. Download of this data shall cause the warning message to disappear.

#### *1.24.3.2. Zones*

The IBMS shall support up to 1024 zones. Each zone shall consist of the following:

- Description
- Organization
- Up to 128 card readers or floor points

The operator shall be able to access a summary display listing all zones and their descriptions. From this display the operator shall, if the operator is configured for the zones assigned Organization, be able to go to a zone detail display showing the zone configurable parameters.

Zones shall be automatically created when card readers are configured in the system. Zones are defined by the card readers, which allow entry to the physical space, which the zone represents. One reader may only be defined as entering one zone. Each reader will indicate the zone it allows entry to and optionally the zone from which one has exited.

#### *1.24.3.3. Access Permissions*

The IBMS shall support up to 1024 access permissions. Each access permission shall consist of the following:

- Description
- Organization or Company / Department
- Up to 256 zone and time period pairs.

The operator shall be able to access a summary display listing all access permissions and their descriptions. From this display the operator shall, if the operator is configured for the access permission's Organization, be able to go to an access permission detail display showing the access permission's configurable parameters.

Once the changes have been saved the operator will be required to download the new data before it is enabled in the Access Control System. This shall allow operators to make a number of changes but only be required to download once.

Each access permission detail display containing changed data that has not been downloaded shall clearly indicate this to the operator via a flashing warning message. Download of this data shall cause the warning message to disappear.

### 1.24.4. **Security**

Managing cardholders shall only be available to operators who are at a certain security level. Both cardholders and cards shall also confirm to standard IBMS Operator Security features such as Organization and Scope of Responsibility assignment as detailed in section 1.6.7.4

It shall be possible to define an operator as only a cardholder administrator. All other functions in the IBMS will be restricted to this operator except for cardholder administration functions.

#### *1.24.4.1. Assigning Access to Cardholders*

Cardholders may have any number of different access levels assigned to them. This shall not be limited by the FMSIBMS system. Each of these access levels may define a separate set of readers and times that will allow the cardholder access. Operators shall be presented with a list of all access levels already assigned to the cardholder and all access levels that are currently unassigned.

#### *1.24.4.2. Deleting Cardholders*

Cardholders may be deleted but retained in the database for future reference if required. It shall then be possible to "undelete" the cardholder should this be required. It shall also be possible to permanently delete the cardholder record in order to prevent unnecessarily large databases from developing.

#### *1.24.4.3. Card/Cardholder Expiry*

Cardholder and card expiry dates may be defined down to a resolution of date and time in minutes.

It shall be possible to assign cardholders and cards separate expiry dates, enabling a card assigned to a cardholder to expire before the cardholder expires. However, it shall not be possible for the card expiry date to exceed the cardholder expiry date of the cardholder to which a card is assigned.

Expiry dates may be set up by default to be a particular given date, or a relative period from the time the cardholder was created (e.g. 1 year).

It shall be possible to assign a cardholder a commencement date and have their assigned cards automatically become active on this commencement date.

#### *1.24.4.4. Cardholder alarms*

It shall be possible to specify that the cardholder generate an alarm when they use their card. This setting may override the alarm setting of the reader to which a cardholder may be presenting their card.

### 1.24.5. **Cardholder events**

All changes to cardholders in the system shall be logged in the event summary and shall list the new value of the cardholder field. Similarly, any time a cardholder accesses a card reader; an event will be listed in the event summary. It shall be possible to automatically view all the events generated for a particular cardholder directly from the cardholder displays without having to run a separate report.

#### *1.24.5.1. Uses before Expiry*

It shall be possible to define the number of times that a cardholder may use their cards. This number shall be decremented every time the cardholder uses their card at a reader until the number is 0, when the cardholder shall no longer have access.

#### *1.24.5.2. Photo Identification Badges*

It shall be possible to capture portraits and signatures for all cardholders and then create photo identification badges using these images.

Image capture and printing of photo identification badges must be fully integrated into the IBMS system and must use the same database. Any system, which uses a separate photo badging system or separate database, will not be acceptable.

Capture devices must include Video Capture cards, Digital Cameras, scanners and signature tablets and capture facilities must support the MCI or TWAIN standards for image capture. Devices may be connected directly via PC boards or through serial or USB ports. If using a Video Capture card for image capture, a live preview facility must be provided. Import and export facilities for images shall also be available.

The IBMS system must provide a tool for the creation of photo badging card layouts. This must allow the incorporation of standard display creation facilities such as image import, a variety of fonts and text effects, a variety of tools for drawing objects and a facility for linking to the cardholder database and any user fields within this. This tool shall be the same tool as used for the creation of custom graphics in the IBMS system as described in section 1.6.9 so as to reduce training and maintenance requirements for the system.

In addition, it shall also be possible to incorporate bar codes and automatic magnetic stripe encoding facilities into the photo badging system.

### 1.24.6. **Biometric support**

The IBMS shall provide the ability to use biometric devices such as hand geometry readers for high security access control. These devices shall be fully integrated into the IBMS system allowing centralised template management of biometric templates. The IBMS system shall be the master database for all cardholder information including biometric templates. The IBMS shall allow for hand geometry changes over time by automatically uploading validated hand templates and downloading them automatically to those hand readers to which the user has access rights.

#### *1.24.6.1. Visitor Management System*

The IBMS shall optionally provide the ability to manage and track visitors to the facility. This shall include both visitors who are given access control cards and visitors who are merely escorted by employees. It shall be possible to store information that defines who the visitor is, what company they represented and whom they were visiting in the facility. This information shall be displayed on a different display to that of a standard cardholder so that operators can enter visitor information easily and without the distraction of all the standard cardholder user fields.

The system shall be capable of doing the following:

- Manage Incoming visitors : Record their data, assign a badge and print a pass
- Manage outgoing visitors : Retrieve their badge and store the visit data

- Pre-Registering Visitors
- Visit analysis
- Temporary Badge assignment

The visitor management system shall have the ability to capture a visitors picture, and store data of ID documents such as a passport when used with the appropriate document capture tools like a scanner.

The visitor management system should be able to notify visitor arrival via email.

There shall be a provision for employees to pre-register their expected visitors using the company intranet, this shall work using Internet Explorer and should not need anything to be installed on the employees machine. This is provided that the user has the access rights for the advanced registration. At a minimum the web based visitor pre-registration should be able to do the following

- Check in and check out
- Visitor's pre-registration;
- Temporary card assignment and withdrawal;
- Cardholder present in zone report;
- User status

Based upon the visitor access rights it shall be possible to assign a visitor to an escort and require that access will be granted only when both the cards of the visitor and of the escort are shown to the reader.

It shall be possible to pre-register a visitor even when a visit is active.

All information about when a visitor arrived and when a visitor departed shall be recorded in the standard IBMS event summary as defined in section 1.8.10

For visitors who are assigned access control cards, it shall support the automatic expiry of their cards after 1 day to prevent visitors from removing valid cards from the facility.

It should be possible to use visitor data in multisite and Distributed Server systems as defined in section 1.1.4

### 1.24.7. **Cardholder Application Programming Interface**

A standard SOAP compliant service must be available to provide a direct XML interface to the cardholder database of the IBMS. This Services Oriented Architecture based interface, shall support reading and writing to the cardholder database allowing only controlled access to this secure

information. The purpose of this is to allow third party applications and services to be developed and able to read and write to the cardholder database in a secure and controlled method.

### 1.24.8. **Cardholder Management Subsystems**

#### *1.24.8.1. Data Exchange with Enterprise Management Systems*

The IBMS shall be capable of exchanging cardholder information with Human Resources modules of Enterprise Management Systems such as SAP and PeopleSoft. Cardholder information shall be able to be sent from the EMS to the IBMS on a regular basis and automatically imported into the IBMS in order to ensure that the Human Resources module and the IBMS cardholder database have the same information.

#### *1.24.8.2. Elevator Control*

**General**

The IBMS shall be capable of controlling access to different floors of a building by interfacing to an elevator controller. The elevator controller shall be capable of operating standalone in a separate hardware processor, and of supporting both low-level controls and high-level industry proprietary control protocols.

The elevator controller shall be capable of supporting many high level and/or low-level elevators, along with requires access groups and multiple landings per elevator.

**Scheduler**

The scheduling of floor access shall be done at the server IBMS computer and downloaded initially to the elevator controller.

The elevator controller independently of the server computer shall then maintain the schedule. In the event of communication link failure between the elevator controller and the server computer, floor access schedule shall continue unaffected.

With specific controllers it shall be possible to configure the way the elevator control works based on schedule, on event or manually, the following modes should be available

- Access mode: no card required to access the floors
- Secure mode: use of the card to access the floors
- Light Secure mode: Card for certain floors no card for the others

## 1.25. **Advanced Security Functionality**

The system should be capable of doing the following advanced security functionality with the appropriate controllers and or other hardware and or optional software modules.

- Path Control : Should be able to force a cardholder to follow a fixed path to reach a destination

- Severe double transit : The severe double transit requires the transactions of two card and both must be authorized in order to obtain the transit acknowledge for both cardholders.
- Escort : Allows a transit if a cardholder is escorted by another user with “escort” rights
- One shot transit : Cards that are valid for a single entry or single entry and exit
- Zone control
    - Maximum number of people authorised to be present simultaneously in the zone
    - Minimum number of people that at least must be present simultaneously in the zone
    - Time limit (duration) for each person to stay in the zone
    - All the rules can be applied at the same time if required
- Spontaneous messages : With the appropriate display hardware and controllers it should be possible to put LCD graphic displays at the door which allow an operator to provide fixed text messages to cardholders.
- Bulletin Board : With the appropriate display hardware and controllers it should be possible to put LCD graphic displays at the door which allow an operator to provide fixed text messages to cardholders that will be displayed when the system is idle.
- Enquiry : With the appropriate display hardware and controllers it should be possible to put LCD graphic displays with function keys at the door which allow cardholders to query the system on cardholder relevant data like holidays, hours worked etc
- Reasons : With the appropriate display hardware and controllers it should be possible to put LCD graphic displays with function keys at the door which allow cardholders to add a “reason” to an access transaction, this reason shall be a from a list of “reasons” that are available from the supervisory system
- Trace : It shall be possible to send an alarm to the host every time a certain cardholder uses a door.
- Transit on Transit : On certain door types and with appropriate hardware it shall be possible to permit a card holder to flash a card while the current transit is still ongoing.

- Multiple operation modes : With appropriate controllers and other hardware , It shall be possible to use either of the following, modes with the system..
    - Card
    - Card+PIN
    - PIN only

  It shall be possible to vary these modes based on schedule or event.

- Global Antipassback – With the appropriate controller type it then true global antipassback shall be supported across the system without having a host computer or FMSIBMS system running, this should be possible using peer to peer communications between the controllers.

### 1.25.1. **SAP/3® INTERFACE**

With the appropriate controller and other necessary hardware & software , the system shall include a optional certified SAP® Interface, this interface shall be bi-directional and allows personnel data from SAP to IBMS system and vice versa. Proof of SAP certification shall be provided by supplier on demand.

### 1.25.2. **Mustering**

It shall be possible with the appropriate controller and hardware to do manage muster points in an emergency situation using the system so that cardholders can assemble at the mustering point during an emergency and flash their cards to the mustering terminal, it shall be possible to locally print data using specific printers at the mustering station

### 1.25.3. **Encryption**

With appropriate controller and necessary hardware it shall be possible to have encrypted communications between the access controller and host system

### 1.25.4. **LDAP Integration**

With the appropriate controller and software options it shall be possible to integrate the IBMS with a LDAP system so that cardholder data is retrieved from a LDAP server.

### 1.25.5. **Canteen Management**

It should be possible to use the system with appropriate hardware to do Canteen Management, it shall be possible to choose a meal using a LCD display with function buttons, print a meal ticket with a specific printer and set the number of meals per day.

## 1.26. **Redundancy**

With the appropriate controller type and relevant hardware and software options then a highly available system using redundancy shall be available with fault tolerance at the following levels

- Controller redundancy
- Power Supply redundancy

- Redundant Host software – as described elsewhere in the document

1.27. **Other Security Features**

- Automatic Card disablement due to non-usage : With appropriate controllers type it should be possible to disable cards that are not being used regularly, it should be possible to set the number of inactive days.

- Cardholder Image comparison : With the appropriate controller type it should be possible to display the details of the event and cardholder information and live images from a DVM camera to provide a comparison between the stored image and the live image

- Event Video Link : The system shall be capable of generating a video link in the event and alarm summary for each item that has an associated video recording. Clicking this video link should start playing back the recorded video.

- Preset Triggering : The system shall support the trigger of a certain preset position of a CCTV camera based on a security event

- Multiple Facility Code: With the appropriate controller type it shall be possible to allow multiple facility codes to work in the same facility simultaneously on the same door.

- Random Checks :With the appropriate controller type and hardware / software options the FMSIBMS shall allow blocking of cards in a random manner to allow for manual checking as needed, it should be possible to do the following

    - To specify a percentage : for eg 1% would mean 1 in 100 cards would be blocked for checking

    - To specify different percentages for different card types

    - Activate on schedule

    - Activate manually from host

    - Activate from a local push button

    - Activate on a specific system event

- With the appropriate controller type , it shall be supported to reset the anti passback status for a single cardholder

- Special Card types

- With the appropriate controller type it shall support at least two special card types
- It shall be possible to execute different actions based on an access granted or denied of these special cards

- Status of Wiegand Reader
  - With the appropriate controller type and reader it shall be possible to monitor the status of a wiegand reader with regard to communications and tamper.

## 1.28. **Software Functions**

### 1.28.1. **Event Initiated Programs**

Physical and software outputs or groups of outputs shall be assignable through configurable algorithms to an input point. When an input changes state the outputs assigned shall be activated as specified by their physical or configured output modes.

When alarm events of individual or groups of points are suppressed by event initiated programs, any occurrence of such alarm events during the suppress mode shall not be enunciated, reported or journalized.

### 1.28.2. **Event Management**

Events shall consist of alarms, changes of state in a monitored status point, cardholder movements, changes in system status and operator actions.

All journal events shall be recorded as necessary to include event description, condition, message, time of occurrence, operator responsible and any other information or tags.

### 1.28.3. **Report Management**

The system shall support a flexible reporting package to allow easy generation of report data. The reports provided shall include pre-configured standard reports for common requirements such as Alarm Event reports and custom report generation facilities that are configurable by the user. A full list of required reports is detailed earlier in section 1.8.12

### 1.28.4. **Guard Tour**

A guard tour facility shall be provided whereby the security administrator shall have flexibility in programming guard tours, utilizing any logical combination of card readers and input points in the system as tour check points.

For each tour it shall be possible for the operator to enter up to 75 tour positions (made up of card readers or digital inputs). For every tour position the operator shall be able to enter a time allowance for the guard to get to that position and up to 16 door points or digital inputs requiring alarm inhibit.

For each tour that is programmed the operator shall be able to enter a Guard ID (equivalent to the guards card key number), the first tour position and the time allowance to reach the first position. If these conditions are not satisfied or the tour is already active, then a message shall be sent to the operator message zone of the Operator Workstation.

Once a tour has been activated, at each step of the tour, a series of points may be controlled. If a particular step is not reached or the next tour point is reached either too early or too late, alarms will be generated.

It shall be possible for operators to manually de-activate a tour via the tour detail display. When de-activating a tour the operator shall be prompted to enter a reason consisting of up to 30 characters. Upon activation, deactivation and successful completion of a tour an event shall be logged to the event file and sent to the printer. The event message shall include date and time, Guard ID, tour number and the reason message (in the case of de-activation). For each tour the latest reason for de-activating the tour shall be viewed from the tour overview display.

The Guard Tour facility shall include an overview display listing the current status of each tour and detail displays showing the configuration details for each tour.

### 1.28.5. **Deadman Timer**

The system shall provide a Deadman timer facility for continuous monitoring of each Operator Workstation to safeguard possible loss of guard operator.

The Deadman timer shall be able to function as follows:

1) If there is no operator activity for a configured period of time, then the operator will be signed off. If the operator does not sign back on to the system within the specified Deadman timer period, the system shall activate those output control points that are specifically configured for alerting external assistance. These special output points shall be referred to as Deadman points. A warning message can be configured to warn the operator before they are logged off.

2) It shall be possible for the Deadman timer to be configured such that if alarms are not acknowledged in a pre-configured period of time regardless of other activity on the system, then an alarm will be generated and a Deadman point controlled to a pre-configured alarm state. To facilitate the acknowledgement of these alarms, a special toolbar button is provided.

3) It shall also be possible to generate periodic Deadman alarms, which ensure that the operator has alarms to acknowledge regardless of the normal activity on the system.

### 1.28.6. **Reader Data Handoff**

It shall be possible to configure a reader such that when an access card is presented to a reader, information about the cardholder, reader name, date, time and other cardholder fields is dumped to a file or serial port in real time. A configuration file shall be available to change the order or fields that will be dumped in this manner. This information can then be accessed by other third party systems for the purposes of calculating time and attendance information.

### 1.29. **Asset Locator system**

The IBMS shall provide a real time system for the location of moveable people and assets throughout the facility as specified below.

#### 1.29.1. **IR/RF based Asset Location System (ALS)**

ALS system shall provide the ability to immediately identify where key high value assets are in the facility. The system shall use a combination of IR and RF tags and readers, to provide capability to tailor the tracking to general areas, specific rooms, specific doors, and even portions of rooms. If tagged assets move out of the detector's view, then alarms can be generated to alert operators to lost assets. Personnel tags shall also provide a duress function so when worn by staff they provide additional security and peace of mind. Equipment tags shall provide a tamper function, so that an alarm is generated if the monitored asset is opened or if the tag is removed. Equipment tags shall also have the ability to monitor an input contact wire, so that runtime hours of mobile equipment items can be monitored.

The RF readers shall have 360° coverage, with an effective read range of at least 60 feet (18 meters) indoors, and 80 ft. (25 meters) outdoors. Using an optional Yagi antenna, the outdoor read range shall be able to be extended to at least 500 ft. (150 meters). If more that one RF reader detects the tag signal, it shall assign the tag to the reader with the highest signal strength. The RF readers shall operate at an unlicensed radio frequency, and have all necessary regulatory approvals.

The IR readers shall have 360° coverage, with an effective read range of at least 40 feet (12 meters). If more that one IR reader detects the tag signal, it shall assign the tag to the reader with the highest signal strength. Using signal strength levels, multiple IR readers shall be able to be installed in a single room to narrow the location down to areas as small as a 4-foot radius.

The LF readers transmit a low frequency (for example: 125 kHz) RF field that is used to “wake-up” tags and force them to transmit their unique ID code within a half a second. The LF readers shall have an effective “wake-up” field that can be adjusted from a 3-foot width for a single door, up to a 30-foot width, with multiple LF readers, for a large entry area. If multiple LF readers are used to cover a large entry area, they shall support synchronization of their RF fields, so that zones do not exist where the fields cancel thereby generating zones where a tag would not see the “wake-up” signal. The RF field generated by the LF reader shall include an ID code (for the LF reader) that can be decoded by tags that enter the field.

#### 1.29.2. **RF-only Asset Location System (ALS)**

RF-only The ALS shall use small tags that affixed to mobile assets and personnel that transmit wireless (RF) signals to sensors mounted throughout the facility in order to track the tag location. ALS system shall provide the ability to immediately identify where key high value assets are in the facility. The system shall use RF tags and readers, to provide capability to tailor the tracking to general areas, and to specific doors, exits and gates. The RF readers shall support direct TCP/IP network communication back to the ALS server. Personnel tags shall also provide a duress function so when worn by staff they provide additional security and peace of mind. Equipment tags shall provide a tamper function, so that an alarm is generated if the monitored asset is opened or if the tag is removed.

The RF readers shall have 360° coverage, with an effective read range of at least 40 feet (12 meters) indoors, and 70 ft. (22 meters) outdoors. Using an optional Yagi antenna, the outdoor read range shall be able to be extended to at least 250 ft. (77 meters). The RF readers shall operate at an unlicensed radio frequency, and have all necessary regulatory approvals. Two different types of RF Readers output interfaces shall be supported: TCP/IP (Ethernet) and 26-bit Wiegand both operating in parallel.

The Low Frequency (LF) Activators shall be able to be mounted in the ceiling or walls, and shall support a variety of activator antennas for different applications (e.g. wall mounted antennas, under-carpet antennas, road-loop antennas, or ceiling mounted antennas. The LF Activators transmit a low frequency (for example: 125 kHz) RF field that is used to “wake-up” tags and force them to transmit their unique ID codes. The LF Activators shall have an effective “wake-up” field that can be adjusted from a 3-foot width for a single door, up to a 30-foot width for a large entry areas or car parking entry lanes. The RF field generated by the LF Activator shall include an ID code (for the LF Activator) that can be decoded by tags that enter the field.

# 5. Digital Video Management

The IBMS shall support a rich integration to a Digital Video Management system that allows viewing and digital recording of video from network connected cameras through the IBMS user interface.

### 1.30. **Architecture**

The Digital Video Management system shall have an easily scalable architecture based on network connected cameras and transmission of video information across a LAN or WAN. Cameras shall be locally connected to the LAN using off the shelf compatible Video Streamer devices or IP cameras. It shall easily be possible to move cameras to other locations in the facility by just disconnecting the camera from the network and reconnecting it to the network elsewhere.

Systems requiring the cabling of analog cameras back to a central PC using analog video cables shall not be acceptable.

### 1.31. **Integration**

#### 1.31.1. **Operator Interface**

The Digital Video management system shall be fully integrated into the IBMS. Operators using the IBMS can also view live video from cameras, initiate recording of cameras and configure different camera settings. All operator security settings as described in section 1.6.7 shall also apply to cameras and camera settings.

All operations to manage digital video shall be performed through the IBMS operator interface. Systems with a different operator interface for managing video shall not be acceptable.

#### 1.31.2. **Event Based recording**

Recording shall be able to be triggered by any alarm in the IBMS system. For any alarm that may occur, it shall be possible to specify which camera shall be recorded, the frame rate for digital recording and the duration of the recording. This may be in addition to other recording schedules that are already assigned to the camera.

### 1.32. **Operation**

For further information on the operation of the Digital Video Management system, insert the *Honeywell Digital Video Manager Guide Specification* here.

# 6. Services

The vendor should be capable of providing supporting services as detailed in the following sections.

### 1.32.1. **Vendor Requirements**

The vendor shall be a recognized leader in Facilities Integration, Security Management, Life Safety Management and Building Automation Systems capable of supplying all necessary support services including hardware and software support, configuration services, system installation and commissioning and on-going support.

### 1.32.2. **Quality Assurance**

The IBMS software supplied, as part of this system shall be developed in an ISO 9001 compliant environment.

### 1.32.3. **Training**

The vendor either at vendor's premises or on site should provide standard training on all aspects of the system.

### 1.32.4. **Configuration Services**

The vendor should be able to supply all necessary configuration services if required including controller configuration, database configuration, etc.

### 1.32.5. **Installation Services**

The vendor should be able to provide installation services for the system including validation services if necessary.

### 1.32.6. **Hardware Maintenance**

The vendor should be able to provide hardware maintenance and spare parts support if required.

### 1.32.7. **Software Enhancement & Software Support**

The vendor should be able to provide a comprehensive software maintenance and enhancement program for on-going support of the system. This shall include:

- Qualification of all Windows hotfixes and updates on a monthly cycle
- Delivery of qualified and supported Windows hotfixes through an automated tool
- Qualification of all cumulative updates and patches for the IBMS software
- Delivery of these qualified IBMS updates through an automated tool.