Contents

1 General Specifications

1.1 System Architecture

1.1.1 General

The Integrated Public Address and Voice Alarm (PAVA) system shall use a Client Server architecture based on a modular PC network, utilizing industry standard operating systems, networks, and protocols.

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. The system shall also support remote configuration and operation using standard intranet or internet connections.

The PAVA system via EBI, 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 system will also support Service Oriented Architecture (SoA) based on Web 2.0 web services standards.

1.1.2 Hot Backup Server

This facility shall enable the system server to operate in high availability architecture with no single point of failure. To achieve this:

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 is the Hot Backup. A real time on-line database and alarm and event duplication mechanism must be supported.

Simply scanning I/O on two separate systems and processing independently will not be 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 single Windows Operating System issue or PC hardware fault, from causing the failure of the entire 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 (DSA)

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.

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 responsibility assignment, there shall be no engineering effort to connect these distributed systems.

Connections between servers can be made through local Ethernet connections. 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).

2 Function and Features Specification

2.1 Main features

Main features of the Integrated Building Management System (IBMS) integrated with the VARIODYN D1 PAVA system are:

- Graphical representation of PAVA system devices
- Send live messages to individual or groups of zones
- Send pre-recorded messages to individual or groups of zones
- Monitor and record alarms and events from the PAVA system
- Modification of Alarms and Events
- Change volume levels of speaker circuits and inputs
- Adjustment of parametric levels

2.1.1 Point Detail Displays

The system shall employ all standard features and functions described in section 2.1 to monitor and control PAVA equipment. At a minimum, the PAVA system supports the following devices with individual Point Detail Displays (PDDs):

- Controller (Digital Output Module DOM)
- Digital Audio Line (DAL)
- PA Audio Output
- Speaker Circuit (radial)
- Speaker Circuit (Loop)
- Audio Output
- Audio Input
- PR Audio Input

- Amplifier
- System Communication Unit (SCU)
- Signal Generator
- Channel
- Network
- Input
- Output
- I/O

In the event of disconnection from IBMS, the PAVA system shall continue to be fully operational with full program capability and interaction with the fire alarm detection system. Once the connection has been reestablished any off-normal alarms present on the PAVA system shall be communicated to the IBMS.

The PDD pages shall have at least two tabs. One tab shall display all recent events related to that point. In the other tab, user can control parameters such as Volume, Maximum volume, Minimum volume, Alarm Volume by typing a value into the corresponding input box, wherever applicable.

The PDD page shall also display the device status. If the device is disconnected or the power is down, the status shall be *Offline*; otherwise, it is displayed as *Online*.

2.1.2 Alarms & Alarm Management

The following notifications must come in via an alarm as well as status:

All high priority alarms are reported in the Alarm Summary Page. All events with priority as *Journal*, are reported in the Events Summary Page. The Return to Normal (RTN) signals are reported in the alarms summary page, however an acknowledgement of an RTN or an alarm are reported in the Events Summary Page.

The alarms are listed in the table below.

Point type	**Alarm value shown in EBI***	**What this condition represents (Impact of the alarm)**
PR Audio Input (DCS Mic-In, DCS Line-In, UIM-Line-In etc.)	Fault Control	Indicates a hardware failure of the Variodyn D1 system. You cannot perform live paging if this alarm is raised.
PA Audio Output (DCS speaker, DCS line out, UIM line out etc.)	Fault Control	Indicates a hardware failure of the Variodyn D1 system.

Point type	Alarm value shown in EBI*	What this condition represents (Impact of the alarm)
Speaker circuit	Fault Control Radial	This alarm is reported when there is a failure in the speaker circuit.
Signal Generator of DOM or SCU	Fault Signal	This alarm indicates the hardware failure of a signal generator inside controllers.
IO	Fault Control Defect IO	This alarm indicates the failure of an IO point
DAL (DCS or UIM)	Fault Control Defect DAL	This alarm may be raised due to the failure of the DCS or UIM.
Audio Input (DCS Mic-In, DCS Line-In, UIM-Line-In etc.)	Fault OTN	This alarm is raised when there is a network communication error inside the audio input lines in a DCS or UIM.
Audio Output (DCS speaker, DCS line out, UIM line out etc.)	Fault OTN	This alarm is raised when there is a network communication error inside the audio output lines in a DCS or UIM.
Speaker circuit	Fault Earth Radial	This alarm indicates earth fault of a speaker circuit.
Amplifier	Warning Audio	Indicates hardware failure of amplifier.
PA Channel	COMMS D1PAVA Unavailable	This event is raised when the PA server is down.
PA Channel	Warning D1 Connection	This event is raised when the network connectivity is lost.
PA Channel	Fault PA CTRL	This event is raised when the communication between the PA server and controllers are down.
Controller	Fault Bat Fail	This alarm is raised when there is a problem in the battery voltage, or the battery voltage is low and does not provide power to run the system.
Amplifier	Fault Power Fail	This alarm is reported when there is a failure in either the main power supply or the battery supply.
Controller	Fault AC Power	This alarm is raised when the main power supply fails.
Controller	Fault AC Power	This alarm is raised when there is a main supply failure.
Controller	Fault Aux PSU Fail	This alarm is raised when there is a battery power supply failure.
Speaker circuit	Fault Radial Impedance	This alarm indicates a high impedance in the speaker circuit.
Speaker circuit	Fault Radial Impedance	This alarm indicates a low impedance in the speaker circuit.
Speaker circuit	Fault Radial Impedance	This alarm is raised when there is a short circuit error in the speaker circuit.

Point type	Alarm value shown in EBI*	What this condition represents (Impact of the alarm)
Speaker circuit	Fault Radial Impedance	This alarm is raised when there is an open circuit error in the speaker circuit.
Speaker circuit	Fault Earth Radial	This alarm is raised when there is an earth fault in the speaker circuit.
PA Channel	Warning Invalid Originator	This event indicates that the originator ID mapping is missing in the Variodyn D1 system.
PA Channel	Warning Invalid Checksum	This event indicates that the message is not functioning properly. The command sent by integration component may be corrupted.
PA Channel	Fault Alarm Retrieval Fail	This event is raised if the PA server cannot retrieve alarms.
PA Channel	Warning DVA down	This event is raised when the pre-recorded message fails to play because the SCU is down.
Speaker Circuit Loop	Fault LIM	This alarm is raised when the speaker circuit loop is off due to some reason.
Speaker Circuit Loop	Fault Loop Impedance	This alarm is raised when there is an open circuit error in the speaker circuit loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm indicates a high impedance in the speaker circuit loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm indicates a low impedance in the speaker circuit loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm is raised when there is a short circuit error in the speaker circuit loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm is raised when there is a fault in the impedance of the speaker circuit loop.
Speaker Circuit Loop	Fault Earth Loop	This alarm is raised when there is an earth fault in the speaker circuit loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm is raised when there is an error in any isolator in the loop.
Speaker Circuit Loop	Fault Loop Impedance	This alarm is raised when there is an error between any two isolators in the loop.
Speaker Circuit Loop	Fault Control Loop	This alarm indicates a hardware failure in the loop circuit.
Speaker Circuit Loop	Fault LIM	This alarm is raised when the loop circuit is working, but with some problem.
Amplifier	Warning Audio	This alarm is raised when the audio level is too high in the amplifier.
Amplifier	Warning Audio	This alarm is raised when the audio level is too low in the amplifier.
Amplifier	Warning Audio	This alarm indicates a high audio threshold in the amplifier.
Amplifier	Warning Audio	This alarm indicates a failure in the audio set point of the amplifier.
PA Channel	Fault Redundant PA Fail	This alarm is raised when the PA server is shut down.

Point type	Alarm value shown in EBI*	What this condition represents (Impact of the alarm)
PA Channel	Warning Command Invalid	This event is raised when the integration component sends an invalid command to the PA server.
PA Channel	Warning Operation Not Possible	This event is raised when the operation cannot be executed from the selected location.
PA Channel	Warning Invalid Zone Info	This event indicates that the zone information sent to the PA server is wrong.
PA Channel	Warning Invalid Message Info	This event indicates that the message information sent to the PA server is wrong
PA Channel	Warning Wrong Announcement ID	This event indicates that the announcement ID sent to the PA server is wrong
PA Channel	Fault PA Server 1 Inactive	This alarm is raised when PA server is active and running.
PA Channel	Alert Action Stopped by User	This event is raised when an action is stopped because of a request from the operator.
PA Channel	Warning Timeout Stopped Action	This event is raised when the action is stopped because of a timeout.
PA Channel	Warning Invalid Command	This event is raised when the live paging is not happening or command is invalid. For example, if you click Stop paging, immediately after the paging has stopped, but the announcement state was not updated in the display page.
PA Channel	Warning Channel Locked	This event is raised when the channel is locked by other station or user for paging and you try to access the channel.
PA Channel	Warning Channel In Use	This event indicates that the monitor speaker is being used by another operator.

It shall be possible to modify the priority of the alarms or disable any alarms which are not deemed necessary to specific site needs from an alarm management window.

2.2 Custom Graphics

An integral Custom Graphics generation tool shall be provided that can accept common building design format drawings. It allows an engineer to create Display Pages which an operator can directly interact with the PAVA system in real time.

Using the custom graphics package, the engineer shall be able to create the following functionality:

- Engineers shall be able to:
  - Prioritize and assign microphones to users
  - Assign a hierarchical priority of up to 250 individual settings to pre-recorded messages.
- Send pre-recorded messages or live announcements to a single zone or a group of zones
- Clear any selection made without having to page the zone
- See the status of speaker circuits:
  - Healthy
  - Fault

    - Offline
    - Busy
- See the status of all of the equipment outlined in section 2.1.1
- Control Speaker Volume and Alarm Volume
- Select Logical zone(s) for paging with:
    - Full connection - message will be played only after all physical zones are available.
    - Partial connection - message will be played in all available zones, then will be played in any zones currently unavailable once they become available.
    - Reconnection - intermediate saving and retry if blocked.
- Chime selection - 1x, 2x, 3x, or no pre-signal.

2.3 Announcement States

The custom graphics shall be able to communicate the following announcement states graphically to the operator:

- **Announcement faulty**: The announcement failed to transmit to the selected speaker zones.
- **Announcement initiated**: The announcement is initiated to transmit through the selected speaker zones.
- **Pre-signal announcement state while playing the pre-signal audio**: The pre-signal tone is being played before the announcement starts.
- **Announcement playing**: The announcement is being transmitted through the selected speaker zones.
- **Waiting for announcement or disconnection**: The system is waiting for the announcement to be transmitted.
- **Announcement completed**: The announcement is completed and the system has returned to normal state.
- **Announcement deleted**: The announcement has been deleted.
- **Announcement interrupted**: The announcement has been interrupted (due to other high priority announcement in the same zone) and the message may not have been fully transmitted.
- **Announcement queued**: The announcement is waiting for another message (which is already being played) to be completed.
- **Announcement prepared**: The system has prepared the announcement and will be transmitted soon.
- **Idle state**: The system is in idle state, waiting for any new message to be transmitted.

2.4 Adjustable Parameters

It shall be possible to adjust the parametric equalization from the head end as follows:

Parameter	Min Value (in Hz)	Max Value (in Hz)
High pass Frequency	20	20000
High pass Order	0	6
Low pass Frequency	20	20000
Low pass Order	0	6
PEQ1 Band Mid Frequency	0	22000
PEQ1 Bandwidth	0	22000
PEQ1 Band Gain	-24	1
PEQ2 Band Mid Frequency	0	22000
PEQ2 Bandwidth	0	22000
PEQ2 Band Gain	-24	1
PEQ3 Band Mid Frequency	0	22000
PEQ3 Bandwidth	0	22000
PEQ3 Band Gain	-24	1
PEQ4 Band Mid Frequency	0	22000
PEQ4 Bandwidth	0	22000
PEQ4 Band Gain	-24	1
PEQ5 Band Mid Frequency	0	22000
PEQ5 Bandwidth	0	22000
PEQ5 Band Gain	-24	1
PEQ6 Band Mid Frequency	0	22000
PEQ6 Bandwidth	0	22000
PEQ6 Band Gain	-24	1
PEQ7 Band Mid Frequency	0	22000
PEQ7 Bandwidth	0	22000
PEQ7 Band Gain	-24	1
PEQ8 Band Mid Frequency	0	22000
PEQ8 Bandwidth	0	22000
PEQ8 Band Gain	-24	1

3 Product & Service Development and Cyber Security

The provider must have received industry recognition for its excellent software and product development and process improvement practices, no less than Maturity Level 5 of Capability Maturity Model Integration (CMMI). CMMI is a process appraisal and improvement framework administered by the CMMI Institute to determine the maturity of an organization's software and product development processes against recognized industry best practices.

The provider that executes the development and support for the offering, must hold ISO9001 certification and demonstrate commitment and practice that products and services are designed, developed, tested and maintained using a formal, auditable Quality Management System that is based on internationally accepted standards.

The following examples must be available for review:

- Software Configuration Management procedures
- Change control procedures for typical application code components
- Standards used for code development and internal procedures applied to source code
- Methodology used for developing or modifying code
- Training program and documentation on developer's understanding of standards and methodology
- Quality Assurance procedures for independent internal review
- Allow the client to view source code for a typical, but inconsequential code module to get a feel for commenting levels, naming conventions, removal of dead code, etc.
- Share the testing conducted, demonstrating compliance with all documented procedures

Concerning Cyber Security the provider must have implemented a Secure Development Lifecycle standard for designing, developing and testing products, with regular evaluation of the security of the products and subjecting them to penetration testing to ensure they are as secure as possible in line with strict governance and mandatory auditing ensuring security policies are always adhered to.

Software components must be developed under a Secure Development Lifecycle standard with regular updates providing security enhancements to maintain security best practice as the threat landscape evolves over time.

The provider must exercise strict engineering standards to ensure products are deployed securely. Regular maintenance and disaster recovery procedures ensure secure operations over the lifetime of the system. These guidelines must be presented for review.

The provider must have an established process for reporting potential vulnerabilities, which are then managed by a team of cyber security experts until they are resolved. These details must be presented for review.

The provider must provide a company / corporate-wide cyber safety governance structure and process to implement DFARS 252.204-7012 and NIST SP 800-171, Rev 1.

The provider must comply with all 15 in-scope controls for FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. They must be aligned to industry-standard compliance frameworks, including but not limited to, National Institute of Standards and Technology (NIST) SP 800-171 and NIST SP 800-53, the International Organization for Standardization/ISO 27001, Payment Card Industry (PCI), and Sarbanes-Oxley (SOX) and 'Safe Harbour' certified annually.