VIGILANT

QE20
Emergency Warning System
Hardening Guide

DOCUMENT: LT0743
Issue 1.0 13 June 2023

QE20 is a product of

Johnson Controls
17 Mary Muller Drive
Christchurch
NEW ZEALAND

Phone : +64-3-389-5096

All specifications and other information shown were current as of document revision date and are subject to change without notice.

AMENDMENT LOG

13 June 2023	1.0	First Release

TABLE OF CONTENTS

1. Introduction

1.1 Introduction and Scope

Our practices provide peace of mind to our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

Because cybersecurity threats have become a risk impacting all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with QE20's functional operation.

This QE20 Hardening Guide provides cybersecurity guidance used in planning, deployment, and maintenance of QE20 systems, including the cabling, user accounts, permissions and roles, backup, redundancy, and firmware updates.

Johnson Controls provides general and specific advice on cyber security for its products at the following web address www.johnsoncontrols.com/cyber-solutions/.

1.2 Description of QE20

QE20 fulfils the functions of an emergency warning system as defined in AS 4428.16 and an emergency intercommunications system as defined in AS 4428.4. When it is activated, e.g., from a connected fire alarm system or manually via Manual Call Points (MCP) located at strategic positions in the premises, it will generate warning signals to the appropriate areas of the building via loudspeakers, supplemented with Visual Alarm Devices (VADs) – flashing beacons, where needed, to warn the occupants about the emergency and provide instructions on evacuating the building.

QE20 can provide non-emergency functions such as background music, public address, paging, recorded message generation, and warden phone communications.

QE20 is a modular system, with the specific combination of modules selected to meet the site requirements – in terms of the number of zones, amplifiers and power rating, power supplies, field wiring modules, and optional networking. A block diagram is shown in Figure 1.

QE20 is highly configurable and expandable up to 224 emergency zones.

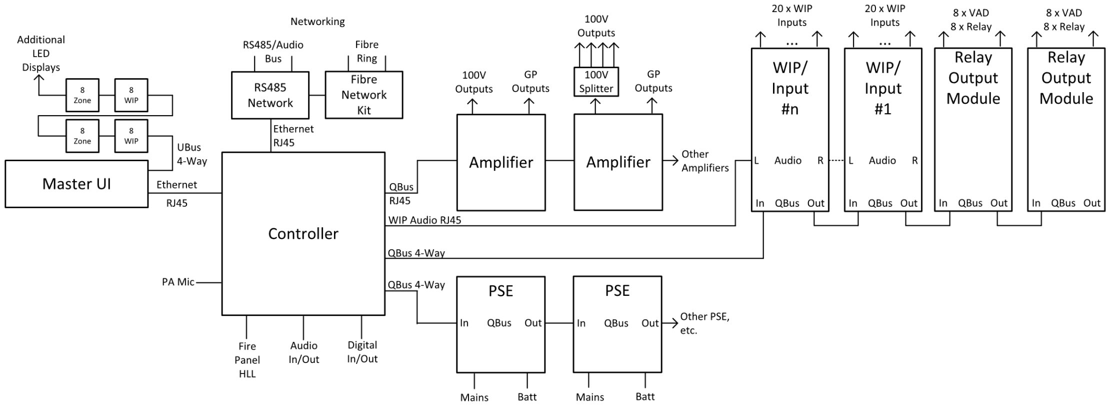

Figure 1 QE20 Block Diagram

The Controller is the brain. It contains the site configuration defining what other modules are present and how the inputs and outputs of those modules are organised. It controls the other modules and determines what needs to happen. Some common audio and digital inputs and outputs are provided by the Controller.

The PSE (Power Supply Equipment) provide a dc power supply for all modules from either mains power or backup batteries. They also provide battery charging.

The Master User Interface (MUI) and the optional 8 Zone and 8 WIP Expansion boards provide the user interface consisting of the LCD and touchscreen, System and All-Zone controls and indications, plus pushbutton and LED indications for the required number of zones and WIPs in the system.

The amplifiers provide 100V audio outputs to drive loudspeakers in the emergency zones. The number of 100V outputs and their power ratings vary with the different amplifier modules. Local audio inputs and switched 24V GP outputs are available.

Connection to secondary emergency control panels (SECP), remote equipment racks or other networked panels is provided by the RS485 Network Module. Copper wired networking is available directly, or fibre-optic cable is supported with the addition of a Fibre Network kit.

From a hardening perspective the key areas of interest are:

- Network copper cables or fibre optic cables
- QE20 installation
- QE20 site configuration
- Programming and configuration of the fibre networking components – PIB, ATA and fibre switch.

The QE20 makes use of IP networking internally (Controller, MUI and RS485 Network Modules) and with fibre networking. These are internal networks and must be kept separate from all other IP networks.

Do not connect the QE20 IP networking to any other network, unless adequate security risk analysis has been undertaken by a security expert and the appropriate hardening has been put in place.

1.3 Other QE20 & Product Manuals

1.3.1 VIGILANT QE20 Manuals

LT0711	QE20 Operator Manual
LT0709	QE20 Service Manual
LT0712	QE20 Installation Manual
LT0726	QE20 Design Manual
LT0732	QE20 Fibre Networking User Manual
LT0704	QE20Config User Manual
LT0705	QE20COST User Manual
LT0694	FP2001 27A PSE Install Guide
LT0695	FP2015 Extender Blank Install Guide
LT0696	FP2000 Controller Install Guide

LT0697	FP2002 Relay Output Module Install Guide
LT0698	FP2003 WIP/INPUT Module Install Guide
LT0700	FP2005 RS485 Networking Module Install Guide
LT0701	FP2006/7/8/9 Amplifier Modules Install Guide
LT0702	FP1187/89 QE20 Hinge Kit Install Guide
LT0703	FP1186 QE20 Module Mounting Frame Install Guide
LT0705	FP2023 2 x 4-way 100V Splitter Module Install Guide
LT0706	FP2010 Master User Interface Install Guide
LT0707	FP2011/12/13 Extender User Interfaces Install Guide
LT0710	FP2014 WIP Tray Install Guide
LT0713	FP2019 Fan Cooling Module Install Guide
LT0714	FP2024/25 Fibre Networking Module Install Guide
LT0715	FP2021/22 8 Zone / 8 WIP Expansion Board Install Guide
LT0716	FP2020 Battery Shelf Install Guide
LT0727	FP2027 Power Distribution Fuse Board Install Guide
LT0728	FP2028 Air Filter Install Guide
LT0738	FP2029 GP Mounting Bracket Install Guide

1.3.2 Other VIGILANT Manuals

LT0114	FP0539 Paging Console Operating and Installation Instructions
LT0229	Panel-Link Intelligent HUB (I-HUB) User’s Manual
LT0529	Panel-Link IP Bridge (PIB) User Manual
LT0346	PC Paging Console Wiring Diagram
LT0564	MX1 Networking Manual
LT0371	PA0688 Microphone Pre-amplifier Module Installation & Operating
FP0938inf	FP0938 WIP Install Sheet

1.3.3 Third Party Manuals

MOXA EDS-405A Ethernet Switch User Manual
Cisco ATA 191 and ATA 192 Analog Telephone Adapter User Guide
Cisco ATA 191 and ATA 192 Analog Telephone Adapter Administration

THIS PAGE INTENTIONALLY LEFT BLANK

2. Design Hardening Steps

2.1 Network Cabling

The appropriate Emergency Warning System Design and Installation standard (e.g., AS 1670.4, NZS 4512) defines the cabling requirements - fire and mechanical strength, redundancy, and transmission path fault detection, etc.

For secure environments additional mechanical protection may need to be applied to the cabling to provide resistance to accidental damage, tampering or eavesdropping. This may involve underground cabling, steel conduit, etc.

As required by these standards the network used for the QE20 must be dedicated to fire and evacuation, and must not be used for other functions unless permitted in the standard.

Therefore, the QE20 network (RS485 and fibre/IP) must not be directly connected to any other building systems.

2.2 QE20 Installation

The QE20 equipment should be installed in a location where security against unauthorised access or tampering is provided. This could be done by installing the QE20 in a public area where anyone accessing the QE20 can be observed, or by installing it in a more secure location with additional security.

The QE20 door keys must not be left in the cabinets, and all internal doors / blank plates must be left securely fastened.

Cabling entering and leaving the QE20 cabinet should be adequately protected.

2.3 Passwords

All devices on the networks must be assigned unique, robust passwords as per their instructions.

- In QE20Config the username and passwords are entered to allow access to the QE20 diagnostics port and to Level 3 access on the LCD Touchscreen. Create entries for only the minimum number of users needed, use passwords that meet or exceed the recommended security strength, enable only those functions that need to be assigned to the user, and use separate user accounts for diagnostics, site configuration download, and firmware updating, if possible. Keep the passwords secure. Refer to the QE20Config User Manual LT0704 for details.
- Each PIB needs to be configured with a suitable password as per Section 3.9 of LT0732 QE20 Fibre Networking User Manual.
- Each ATA needs to be configured with a suitable password as per Section 3.8 of LT0732 QE20 Fibre Networking User Manual and the ATA Administration Manual.
- Each Fibre Switch needs to be configured with a suitable password as per Section 3.10 of LT0732 QE20 Fibre Networking User Manual and the Fibre Switch User Manual.

2.4 Configuration Backups

The configurations that are prepared for each of the QE20s and its components need to be securely backed, so that they can be restored in the advent of a device failure / replacement.

In particular, the QE20 Site configuration (from QE20Config), PIB configuration, ATA configuration, and Fibre Switch configurations should be backed up as per the relevant User Manuals and kept securely.

2.5 Internal Ethernet Ports

The QE20 uses IP networking internally for connection between the Controller, MUI and RS485 Network cards. The Controller module provides 4 RJ45 ports for these devices. This IP network must not be extended outside the cabinet or connected to any other equipment.

The QE20 uses IP networking for its fibre networking between PIBs, ATAs and Fibre switches. The Fibre switch provides multiple RJ45 ports for these devices. This IP network must not be extended outside the cabinet (other than by using the fibre ring connections) or connected to any other equipment.

2.6 Modbus

The QE20 can be configured with a Modbus port for connection of a Modbus Master to poll the QE20 for information and, optionally, control the QE20.

When configuring the Modbus function in QE20Config, the **Control via Modbus disallowed** option should remain ticked, unless it is necessary for the Modbus master to be allowed control. If control is to be given to the Modbus Master, the QE20 should be dedicated to the Modbus Master (i.e., not have a user interface) and be programmed with only those remote QE20 SIDs, zones, groups and WIPs that the Modbus Master needs access to.

3. Maintenance Hardening Steps

3.1 User Accounts & Passwords

If users leave the organisation or no longer need access to the QE20 then their accounts should be deleted from all equipment. If the passwords become known to other users, then the passwords should be changed.

3.2 Retain Backups

Whenever the configurations for the QE20 or its components are changed, the new configurations need to be backed up and securely retained.

3.3 Firmware Updates

Johnson Controls, and the manufacturers of the third-party components used in the fibre networking (ATA and fibre switch), may make new firmware available from time to time.

The web sites for these products should be checked to see if new firmware is available that would be appropriate to be installed.