Digital Solutions Division

ACT Government | ACT Health

St-11 ICT Fire Standards

Version 2021.1.1 Approved

User Support: 02 5124 5000 | Division Administration: 02 5124 9000

Please Read

IMPORTANT COMPLIANCE REQUIREMENTS

Note: The following instruction applies to all documents in this library.

1. This is a controlled document and is reviewed every two years. The last review was carried out in March 2021. If you are viewing this document after March 2023, you will need to contact the sender to confirm you are working from the latest revision.
2. It is the responsibility of the contractor/vendor to read and adhere to the procedures, processes and guidelines set out in the following document when quoting for or carrying out work for the ACT Public Health System Sites.
3. If you have questions or require clarification of any of the procedures, processes or guidelines in the following document please contact the sender of the document in writing with your questions so that a formal response can be provided. If any specific requirement is unclear, it is expected that clarification will be sought from the ACT Public Health System's Digital Solutions Division (DSD) Critical Systems Infrastructure (CSI) Hub - Information Communications and Technology (ICT) architect(s), rather than a decision made and a design implemented and based on unclarified assumptions.
4. These standards are applicable to ALL ACT Public Health System Sites or any work funded by ACT Health Directorate (ACTHD) (e.g. Calvary, ACTHD provided NGO sites) unless specifically exempt.
5. All Greenfield ACT Public Health System Sites are expected to be fully compliant with all appropriate standards.
6. Brownfield ACT Public Health System Sites undergoing refurbishment should be fully compliant unless an exemption is provided by DSD's CSI Hub.
7. In the event of any design non-compliance issues, a Departures document must be completed and submitted to DSD's CSI Hub. These issues should be resolved, in consultation with DSD's CSI Hub, as soon as possible within the project process and explicitly prior to site handover.
8. While some test cases have been cited within these documents as examples, the list is not exhaustive, and all appropriate test procedures shall be formulated, approved prior to testing and testing shall be performed by the client system administrators before full acceptance can be signed off by the Senior Director CSI Hub.

IMPORTANT:

Any departure from the standard, whether intentional or in error shall require a completed Departures Document to be submitted to DSD infrastructure Hub for approval before acceptance can be assumed.

Any non-compliant designs without a pre-approved Departures Document by completion of the project or a nominated milestone or gateway, will require remediation by the Head Contractor at the Head Contractors cost.

Document Review High Level

(to review detailed document updates click here)

Version	Summary of Changes	Author	Date
2019.1.2	Update 'Compliance Requirements' page. Review the document and update as necessary.	David Richards, Nitin Saxena	18/09/2019
2019.2.0	Sent to the Technology Strategy Committee for approval to release	Mark Moerman	30/09/2019
2020.1.0	CSI Hub approval	Mark Moerman	30/03/2020
2020.1.1	Updated VESDA isolation switch details	Raj Mohan	06/08/2020
2020.1.2	General revision of text and minor additions	David Richards	13/10/2020
2020.1.2	Review made doc consistent with PO's Comments	Alkesh Hemrajani	16/12/2020
2021.0.1	Content changes and inclusion of fire penetrations	Raj Mohan	30/03/2021
2021.1.0	Document updates and final review	David Richards & Mitchell Jamieson-Curran	01/04/2021
2021.1.0	Rechecked document prior to CIO final review and approval by Technology Steering Committee for release	Alkesh Hemrajani & Mark Moerman	01/04/2021

Document Default Review Cycle

Date	Version	Comments
March 2020	2019 2.0	Original release date
March 2021	2021.1.0	Next review March 2023

Document Owner

Name	Location
Senior Director, CSI Hub	CSI Hub, Technology Operations, DSD ACTHD

Document References

Document	Version	Location

Contents

1. Introduction

1.1 Context and Background

This document forms part of a suite of documents that describe ICT specifications for the various ACT Public Health System's support systems.

Each ACT Public Health System's building contains several fire related items that **relate to ICT requirements specifically**; a Fire Indicator Panel (FIP), a Multipoint Aspirated Smoke Detection System (MASDS) combined with other smoke detection devices and fire proofing requirements for Communications rooms.

The FIP monitors the building for any signs of smoke or fire and if detected raises alarms onsite. Additionally, it sends messages (Intercommunication High and Low-Level messages) to the fire warden, ACT Fire and Rescue, campus Emergency Warning and System (EWIS), and to designated ancillary staff via messaging engine (e.g., security staff and supervisors within the specific building).

The MASDS shall detect smoke at very low concentration and in conjunction with a standard smoke alarms provides an early warning system for critical spaces related fires.

Communications rooms such as Building and Floor Distributor rooms (BD & FDs) in new buildings shall be designed to have a minimum two (2) hour fire rated to stop the spread of fire to critical systems.

1.2 Assumed knowledge and document dependencies

Relevant documents are mentioned in Appendix A.

1.3 Disclaimer

The following document provides **ICT ONLY specifications and requirements** for the designated ICT Specifications of Fire Indicator Panel, MASDS and fire detection configuration for communications rooms and fireproofing requirements of same and is by no means intended to cover all the comprehensive business requirements for the system. Additional business and user requirements will be presented in project specific documentation such as Business Requirements, Solution and Detailed designs.

2. Fire Systems and Requirements

2.1 General fire requirements

2.1.1 Fire extinguishers

2.1.1.1. Fire extinguishers shall be fitted within all communications rooms.
2.1.1.2. The location shall be easily accessible from the main entrance of the room.
2.1.1.3. The location shall be clearly marked.
2.1.1.4. The extinguisher shall be a 4.5kg.
2.1.1.5. Carbon Dioxide type preferred – Red with black band; or
2.1.1.6. Dry chemical fire extinguisher ABE powder – red with white band.

2.1.2 Emergency lighting

2.1.2.1. Emergency lighting shall be installed, operational and provide enough light to egress room for all points in the room.
2.1.2.2. Emergency lighting must be operational for minimum of 30 minutes.

2.2 FIP and MASDS Architecture

The architecture is consistent with the 3-tier split concentrator architecture as illustrated in the following diagram below. However, in this case the head-end server components are replaced by multiple head-ends or systems (e.g., non-FIP infrastructure such as Messaging Engine, Access control and Building Management and Control System (BMCS) controllers) that use the information to provide further processing. There is no central storage or processing required, as it is only providing information output on the occurrence of a fire related event and only provides secondary messaging.

The following diagram, Figure 1, illustrates fire systems architecture and integrations with various systems.

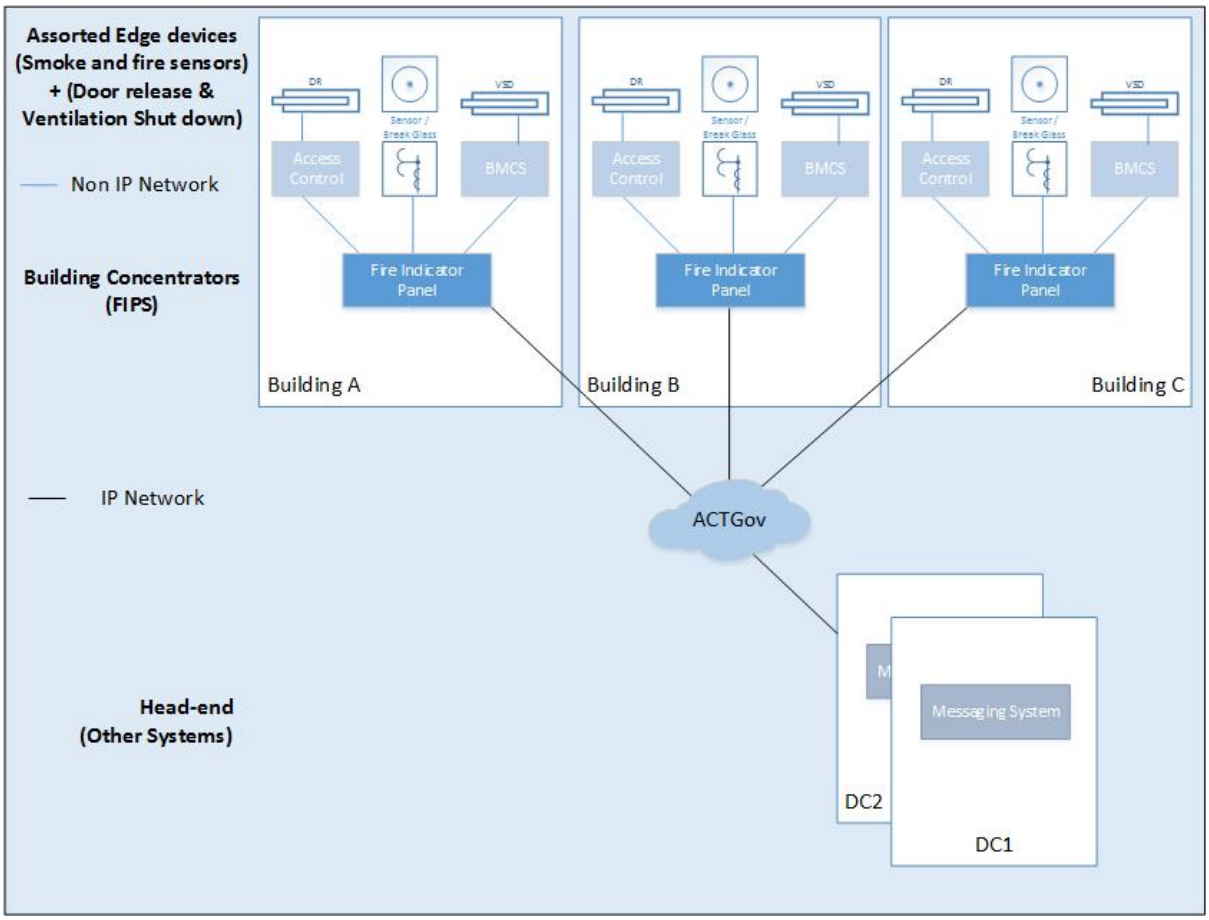

Figure 1 FIP Specific Implication of Architecture

2.2.1 Head-End Infrastructure

The head-end infrastructure is provided by a Central Messaging system, C-Cure access control system and BMCS (however access control and BMCS are interfaced through low level dry contact interfaces). Refer to Section 3.3 Integration with other systems for further information about the head-end infrastructure.

2.2.2 Building Infrastructure

The Building concentrator in this case is a combination of two devices (FIP and MOXA); An Ethernet/IP interface that can output IP based Alarm messages directly to a designated remote IP device shall be the desired choice, removing the MOXA as an additional point of failure.

The first part is the FIP itself and the second is a MOXA, serial to IP converter which allows all text outputted from the FIP printer port to be directed to the messaging engine (which first removes printer escape codes) and then deliver the messages to designated staff, e.g., Fire Warden in whatever format is required (SMS, email, T2V etc).

2.2.3 Endpoint Devices

The endpoint devices consist of the various fire and smoke sensors including MASDS (outputs) and Low-Level Interfaces (LLI) to the BMCS and Access Control systems (outputs) as designated by the Project Fire Protection Design Engineers initiate air handling procedures and door release/locking in areas of stage three alarms.

2.3 FIP Systems and Requirements

Most requirements shall be described by the project Fire Protection design Engineers in line with Australian Fire and Safety standards, however the following elaborates on the ICT components.

2.3.1 FIP Hardware

FIP as designated by Fire Protection design Engineers. In addition, an IP based Ethernet interface that can send messages to designated third-party devices is required.

The FIP shall have hardwired low-level interfaces to the following devices:

- Communications: -
  - EWIS (hard wired to Campus EWIS panel for building alert).
  - Moxa (Serial to IP device - Basic building alert to Fire Warden).
  - ACT Fire and Rescue (hardwired and two (2) different mobile carrier interfaces); and
  - WIP phone (hardwired FIP to EWIS panel Fire Warden intercom phone).
- Control:
  - BMCS – ventilation shut down; and
  - Access Control – Door open/lock down.

The FIP shall also have a dual ethernet termination outlet (TO) mounted inside the cabinet.

The following diagram, Figure 2, illustrates the physical layout of the FIP interfaces described above.

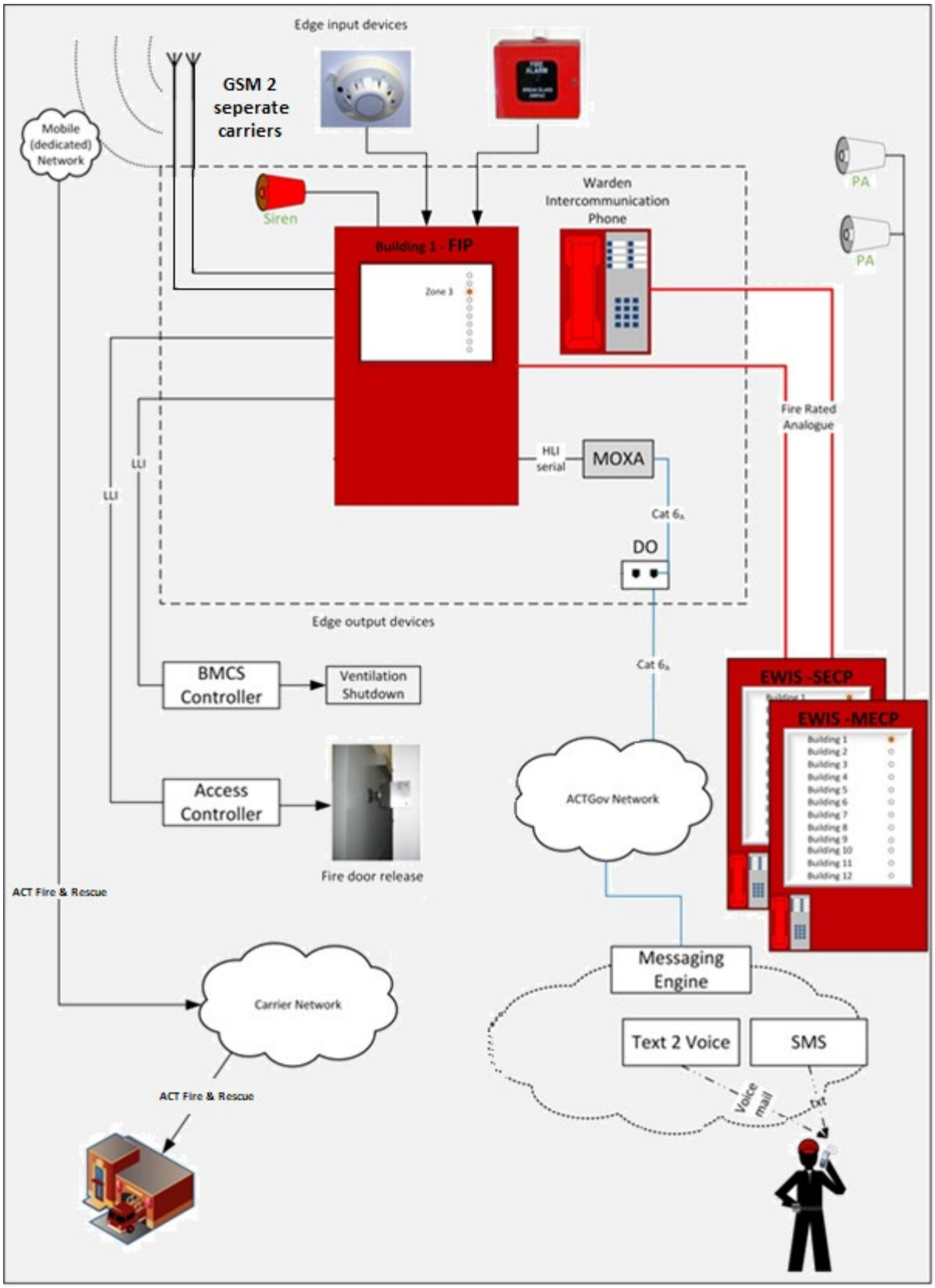

Figure 2 Physical FIP Interfaces

2.3.2 Maintenance and Support

When a separate MOXA is used (as a substitute for an IP message capable FIP), the "link" shall be configured to have the central system that "pings" the device with a "heartbeat" test, as a 24/7 assurance of the availability of the device. The central MOXA "monitoring software" system, shall be configured to include any new MOXA device. The MOXA should also be checked for correct operation at each FIP building during the fire testing to establish a message is generated and sent to the appropriate staff members listed as fire wardens for that building.

2.3.3 Network

The FIP network interface (or MOXA) shall require the following:

- IP address on the Security Virtual Routing and Forwarding (VRF) logical network.
- Configuration to send data to the IP address of the messaging engine; and
- The MOXA monitoring software to be configured to include the new MOXA IP address.

2.3.4 Power

MOXA shall be a Power over Ethernet (PoE) device and derive power from the ICT Uninterruptible Power Supply (UPS) backed, network switch. In rare circumstances where the MOXA needs to be linked via optical fibre due to distance constraints, either hybrid powered fibre shall be used or by directly wiring the DC voltage input of the MOXA to the FIP's battery system.

2.3.5 ICT Integration with other Head-End Infrastructure

2.3.5.1 Messaging Engine

As the FIP function does not implement any dedicated ICT central server architecture, it integrates with "other" systems by providing High Level and Low-Level interfaces to those other systems. As far as ICT integration is concerned, the FIP shall either be capable of sending IP alarm messages directly (IP enabled panel) or via a serial to IP "MOXA "unit, which will attach via a cable to the serial printer port of the FIP. As the output of this port is designed for a printer, it shall produce printer codes along with the fire alarm messages and these need to be removed to enable meaningful messaging.

The filtering is done by the Messaging Engine. The messaging engine knows the IP address of the MOXA and will strip these redundant printer codes out of the message accordingly based on the FIP model and then based on business rules send the message on to pre-determined persons or groups e.g., fire warden, building supervisors etc with a location precursor text string, (building and zone) based on the IP address the message originator FIP.

2.3.5.2 Access Control

The FIP shall also integrate using a Low-Level interface (LLI) between the Access Control System building concentrator allowing for instant/automatic fire door release or another door fail safe open or closed depending on the requirement.

2.3.5.3 BMCS

The FIP shall also integrate using a LLI between the BMCS building concentrator allowing for instant/automatic Fire Dampening of air conditioner ducts and ventilation to prevent recirculating smoke.

2.3.6 Software

- Provide a filter programmed on the messaging engine to suit the FIP.

2.3.7 Testing

The system must undergo comprehensive testing ensuring the system complies with the following criteria:

- All data is transmitted to the messaging engine.
- Only the desired text is sent to recipients (redundant printer codes deleted); and
- Programmed recipients in the building fire group only receive the correct message in the format designated for each recipient i.e., SMS, email, T2V etc.

2.4 Smoke /Fire Detection, MASD Design and Requirements

All Building Distributor (BD) / Floor Distributor (FD) / Server rooms shall be installed with a MASDS type system and a standard fire alarm as the primary warning system

The standard fire alarm shall act as the primary warning system rather than the MASDS, to comply with fire building codes and allow the MASD to be isolated during installations within the room.

Apart of the Standard feature requirements shall include:

2.4.1 Detector module mounted on the wall inside the communications rooms.

2.4.2 Display module (mimic panel) with audio alert mounted on the wall outside the main entry door to the communications rooms; and

2.4.3 Blue, Amber and Red strobe indicators shall be mounted as follows:

2.4.3.1 Ceiling mounted above the entry door outside the communications rooms; and

2.4.3.2 Ceiling mounted in the centre of the ICT room/s.

2.4.4 Strobes and sounder shall be Yellowtec litt series or similar product.

2.4.5 The system shall have three alarm stages, with the third stage integrated into the building Fire Indicator Panel (FIP) and CCURE system provided as part of the building. The three alarm stages shall initiate the following:

2.4.5.1 Stage 1 Alert shall initiate a mutable audible alert operating outside the communications rooms at the MASDS panel, with the visual blue strobe light to be operating in both locations.

2.4.5.2 Stage 2 Action shall initiate a mutable audible sounder alarm operating outside the server room/s at the MASDS panel, with the visual amber strobe light to be operating in both locations. CCure integration shall generate an email to CHS Assistant Director, Fire Safety and Transport for CHS sites: and

2.4.5.3 Stage 3 Fire 1 shall initiate the operation of the visual red strobe light in all locations and activate an alarm on the FIP. CCURE system shall also generate an email to CHS Director, Fire Safety and Transport for CHS sites. Where fitted the Stage 3 Fire 1 shall also initiate the operation of the shunt trips on the communications room's switchboard.

2.4.5.4 Messaging shall also be generated to the appropriate DURAsuite Fire Groups.

2.4.5.5 Visual and audible fire warning alarms shall also be provided on the CCURE terminals.

2.4.5.6 Maximum smoke obscuration levels and time delays between MASDS levels will be:

	Level	Obscurity	Delay in Seconds
Alert	1	0.04	10
Action	2	0.09	50
Fire 1	3	0.12	60

2.4.6 Shunt trips shall only be provided where the fire protection system design includes a double-knock between both MASDS (Stage 3 Fire 1) and optical smoke in rooms which DO NOT have a gas or hybrid mist suppression system and with a count-down and manual override.

2.4.7 MASDS shall have an eight-hour battery backup facility and shall be powered from the communications room's switchboard upstream of the power subcircuit shunt trip. MASDS shall be labelled "Isolate communications rooms Shunt Trip before Testing MASDS".

2.4.8 All ceiling-mounted strobe lights shall be labelled "MASDS Stage 1" "MASDS Stage 2" " MASDS Stage 3"

2.4.9 MASDA system to have the ability to monitor by referencing other detector the external environmental conditions to minimise nuisance alarms.

2.4.10 MASDA system shall be networkable and connected to the BMS ICT network for centralised remote monitoring, configuration and control.

2.4.11 MASDA system shall be compatible with any incumbent networked MASDA monitoring, configuration or control system.

2.4.12 MASDS location isolation:

2.4.12.1 MASDS systems shall have the capability to be locally isolated within the communications room for a maximum of four hours.

2.4.12.2 Reset can be either via manual reset or automatically reset after the duration is complete. Local audible alarm will generate 30 minutes prior to the systems resetting.

2.4.12.3 The local panel shall also have visual indicators when the MASDS is "ENABLED" or "DISABLED".

2.4.12.4 The main smoke/fire detection systems remain fully operational, and the Fire Panel will remain active when system is in isolation.

2.4.12.5 Local isolation should be keyed with 003 standard fire panel keys

2.4.13 MASDS system shall provide a low-level interface to the CCURE system. This shall be provided per MASDA panel in the form of separate dry contacts (NC/NO) for each alarm condition CCURE shall monitor the alarms and report these to the CHS Security Operations Centre (SOC) for CHS sites.

2.4.14 Provide all necessary MASDA interface panels and devices to allow the ready integration as part of the overall networkable solution.

2.4.15 MASDS Sensitivity Classes

Table as per AS 7240.20 Sensitivity Classes

Class A	**Very High Sensitivity** As ASD system with very high sensitivity that is capable of providing very early warning of a potential fire condition. Such systems are particularly relevant for high-risk areas where staged responses to the multistage alarm conditions are justified to ensure minimum down time of the protected area after a fire-related incident.
Class B	**Enhanced Sensitivity** An ASD system with enhanced sensitivity for applications where an additional degree of confidence is required for the protection of a particular risk. The enhanced capability of such systems is often required to compensate for other risk factors in the protected area such as unusually high ceilings or significant air flows.
Class C	**Normal Sensitivity** As ASD system design to give equivalent performance to a system of point detectors in accordance with AS 7240.7, AS7240.15 or AS7240.27.

The time taken for a system to transport a sample for a protected area shall not exceed the following:

(i) Class A 60s
(ii) Class B 90s
(iii) Class C 120s

The sensitivity class for all DB's will be **Class A** unless directed by CHS Security Ops.

2.4.16 MASDS Isolation Switch

2.4.16.1 where possible the isolation switch shall be recessed.

2.4.16.2 This switch locally only isolates the MASDS, the main smoke/fire detection system remains active and on the fire panel it shall appear as normal.

Figure 3 MASDS Isolation Switch

2.5 Fire Suppression Systems

Where required for building code compliance, Communications rooms shall be fitted with the following fire suppression systems:

2.5.1 Server/Datacentres/BD rooms Vortex hybrid mist/gaseous suppression system.

2.5.2 FD rooms two stage dry pipe sprinkler system; and

2.5.3 UPS/Battery rooms two stage dry pipe sprinkler system.

3. Vendor Requirements

The head contractors, vendors or their representatives must review these specifications and provide a "Departures document" for any non-compliance with these specifications. The Departures document must be provided prior to commencing any work including design, implementation, configuration, and testing. Vendor must provide a high-level vendor design (HLVD) as a return brief of requirements to establish that all scope is adequately covered.

The following requirements shall be supported by the FIP system.

Any additional requirements shall be specified as part of the procurement process.

3.1. Installation Support

The vendor will need to enable the printer port to print all messages if the system is not IP based. The printer port shall be used to send messages.

4. Cable Penetration Sealing

4.1. Process

4.1.1. The Contractor shall provide a DSD CSI Hub's Solutions Architecture and AS/NZS approved fire activated self-sealing pathway device or seal all openings (made or provided) in or through building Fire and / or Smoke walls, floors, etc. after all cable reticulation is completed for a particular project or work request.

4.1.2. The Contractor shall take photos of each proposed penetration site and then again after sealing and certifying is completed, such that the certified sticker may be seen.

4.1.3. The photos and certification details shall then be logged in the "building penetrations register" and a copy submitted to CSI Hub along with as-built documentation.

4.1.4. Where consecutive (with no time delay) and/or separate work requests require penetrations in the same location, permission may be sort in the DISST process or building contract, for the final contractor or work request to arrange for a single resealing and certification to occur. In this case, each work package or contractor, shall provide "before and after" shots and provide these for the building penetration procedure.

4.1.5. The Contractor shall fireproof any openings (made or provided), in or through building walls, floors, etc. with approved fire-retardant techniques, materials and /or devices, where such sealing is required for restoring fireproofing and/or smoke proofing.

4.1.6. The Contractor shall effectively seal all cable duct openings above ground level, and all cable entries from trenches into buildings to prevent the ingress of moisture and the entry of rodents or other vermin.

4.1.7. The Contractor shall ensure that all spare conduit and cable entries into equipment are effectively plugged and sealed to prevent the ingress of moisture, dust, rodents, and insects.

4.1.8. The Contractor shall ensure that all openings through roofs and external walls are made weatherproof including the installation of flashing and/or rain hoods to prevent.

4.2. Fire wall penetration solution Greenfield/Brownfield

4.2.1. All sites shall have the new Promastop fire wall penetration solution installed for new penetration.

4.2.2. Any new cabling requiring a penetration in a fire-wall which already contains a data penetration shall re-open the existing penetration and retrofit the Promastop solution to cover all cable runs and remediate existing.

4.3. Fire wall penetration Procedure

Prior to commencement of work, do the following:

4.3.1. Identify potential Fire Penetration points based on building floor plan and site plan.

4.3.2. Inspect site and keep a photographic record of each Fire Penetration point before commencing.

4.3.3. Provide cable path and penetration plan to Snr Director CSI Hub for approval.

4.3.4. Procure professional services for Fire Penetration sealing works.

4.3.5. Seek CHS DISST endorsement.

During work the following must occur:

4.3.6. HPR shall be required to attend site each day to conduct checks of the progress.

4.3.7. Update Fire Penetration location records and photographic evidence of before and after pictures which include certification sticker.

On completion of work the following must occur:

4.3.8. HPR shall be required to submit all Fire Penetration records and pictures to Director of ICT Infrastructure for approval.

4.3.9. Invoice/s for cabling and Fire Penetration sealing works must be approved by Director of ICT Infrastructure.

4.3.10. Submit DISST closure form.

4.4. Approved Firewall Cable Penetration Device

PROMASTOP®-IM CBox

PROMASTOP®-IM CBox 125 is an intumescent sealing system for cable penetrations.

Figure 4 Three views of approved firewall cable penetration device.

The Promastop® does not require additional sealing of the penetration due to the entire black material swelling beyond 65 °c, the projections also serve as smoke barrier.

4.5. Installation

4.5.1. Cut the penetration hole to size. A separate penetration shall be created for each service type (data, security, electrical, mechanical etc). Install the fixing system, use a drill of 4mm or 5mm diameter and use suitable securing hardware.

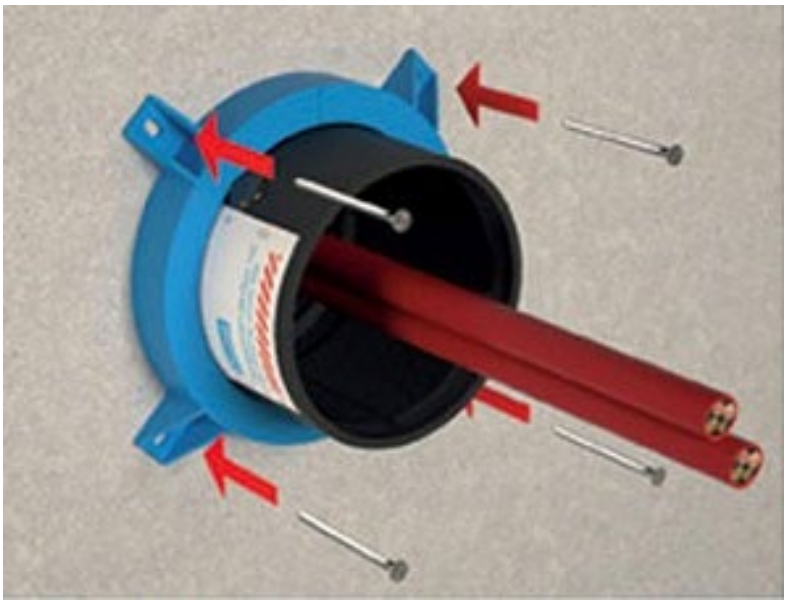

Figure 5 Promastop® Installation Procedure Step 1

4.5.2. Repeat the install of the two-part collar on the opposite side.

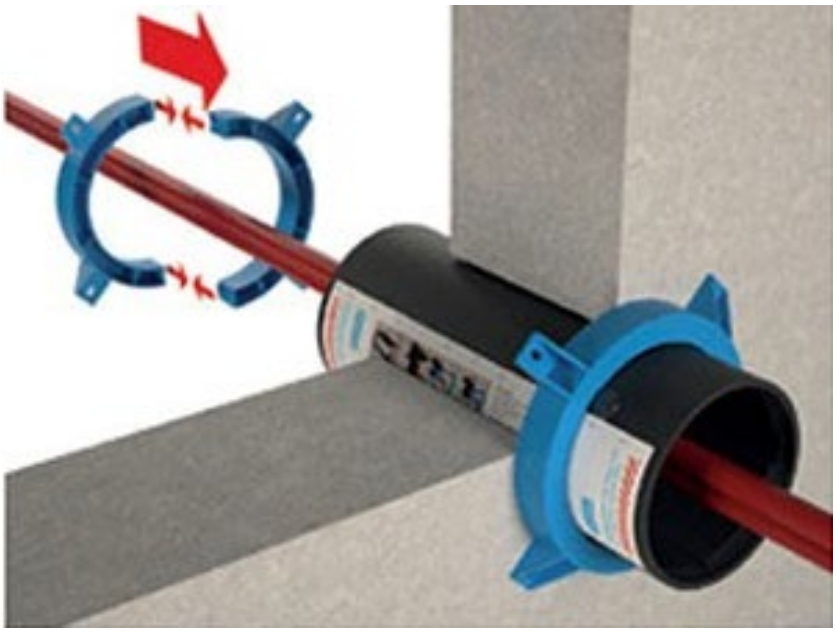

Figure 6 Promat Installation Procedure Step 2

4.5.3. Finally fix the identification label in a suitable location and take a photo as shown below and submit photo labelled with location description to DSD CSI.

Figure 7 Promastop® Installation Procedure Step 3

4.5.4. Example:

Figure 8 Example shows completed installation of Promastop® data, power and security cabling with spare for mechanical.

Appendix A

References

Standards and Compliance

- Any Australian Standards that are relevant to this system.

Glossary of terms

Term	Definition
ACTHD	ACT Health Directorate
AETHER	A messaging Engine
BC	Building Concentrator
BD	Building Distributor
BMCS	Building Management and Control System
C-Cure	An Access Control System
CHS	Canberra Health Services
CSI	Critical Systems Infrastructure
CWC	Clinical Work Device
DO	Double Outlet
DSD	Digital Solutions Division
ECP	Emergency Control Panel
EIS	Emergency Intercommunication System
EWIS	Emergency Warning and Intercommunication System
EWS	Emergency Warning System
FD	Floor Distributor
FIP	Fire Indicator Panel
GSM	Global System for Mobile (communication)
ICT	Information Communications and Technology
IP	Internet Protocol
LLI	Low Level Interface
Lingo	A messaging/chat application used for
MASD	Multi Aspirated Smoke Detection
MECP	Master Emergency Control Panel
MOXA	A serial to IP converter
PA	Public Address
POE	Power over Ethernet
SECP	Secondary Emergency Control Panel
UPS	Uninterruptible Power Supply
VESDA	Very Early Smoke Detection Apparatus
VRF	Virtual Routing and Forwarding (MPLS)
WIP	Warden Intercommunication Phone

Table 1 Glossary

Amendment History

Version	Summary of Changes	Author	Date
2015.0.1	Initial draft	David Richards	27/02/2015
2015.0.2	Updates to several section	David Richards	03/03/2015
2015.0.3	Peer review	Nitin Saxena	04/03/2015
2015.0.4	Minor updates	Nitin Saxena	05/03/2015
2015.0.5	Updates following feedback	Nitin Saxena	10/03/2015
2015.1.0	Final Release version	Nitin Saxena	16/04/2015
2015.1.1	Change 'Edge Device' to 'Endpoint Device' based on feedback	Nitin Saxena	27/04/2015
2018.1.2	New template update	Raj Mohan	09/10/2019
2019.1.2	Update 'Compliance Requirements' page. Review the document and update as necessary.	Nitin Saxena	18/09/2019
2019.2.0	Sent to the Technology Strategy Committee for approval to release	Mark Moerman	30/09/2019
2020.1.1	Updated VESDA isolation switch details	Raj Mohan	06/08/2020
2020.1.0	Infrastructure Hub approval	Mark Moerman	24/03/2020
2020.1.2	Review made doc consistent with PO's Comments	Alkesh Hemrajani	16/12/2020
2021.0.1	Content changes and inclusion of fire penetrations	Raj Mohan	30/03/2021
2021.1.0	Document final review	Mitchell Jamieson-Curran	30/03/2021
2021.1.0	Document updates and final review	David Richards & Mitchell Jamieson-Curran	01/04/2021

Appendix B- Details of Changes

Version	Last Modified date	Author Name	Summary of changes	Section No.	Section Details	Page. No.	Revision/Changes Made
2020.1.1	06/08/2020	Raj Mohan	Update		For Approval		Updated VESDA Isolation switch details
2020.1.2	16/12/2020	Alkesh Hemrajani	Reviewed as per PO		Review		Reviewed the docs per PO's comments
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Main Page with picture	1	Removed page footer words
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Blank page removed	2	Blank page has been removed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Please Read	3 & 4	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Review Control	5	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Document Reference	5	This heading has been cancelled.
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Document Next Review	5	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments		Document Owner	5	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	1.1	Context and Background	8	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	1.3	Key Stakeholders	8	Heading has been removed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	2	Enterprise Architecture	9 & 10	Non-Technical words and Font formats has been changed

2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	3.1.2	Budling Infrastructure	12	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	3.2.1	FIP Hardware	12 &14	Technical words and Figure name has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	3.3	Smoke/Fire Detection	15	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	3.4	Labelling	16	Non-Technical words and Font formats has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	3.5	Fire Suppression Systems	16	Heading name has been changed
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	4.1	Installation Support	17	New heading has been added
2020.1.2	16/12/2020	Alkesh Hemrajani	PO's Comments	Appendix	Appendix A	18	Non-Technical words and Font formats has been changed
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update		Enterprise Architecture		Heading and Picture has been removed
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	2	Fire System and Requirements	7	Technical words have been changed
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	2.2	FIP and MASDS Architecture	8	Old architecture has removed and added new architecture
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	2.3	FIP System and Requirements	9	Technical words have been changed and updated the drawing
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	2.4	Smoke/Fire Detection, MASD Design	12	Technical words have been changed and new picture has been added
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	4	Cable Penetration Sealing	17	New heading, Technical explanation and new pictures has been added
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update	Appendix	Appendix A	21	Technical words have been changed
2021.1.0	01/04/2021	Mitchell Jamieson-Curran	Technical Update		Amendment history	22	Updated the history