CODE OF PRACTICE
FOR THE
AUTOMATIC FIRE ALARM SYSTEM

Date	29 March 2019
Version	1.9
Status	Final
Permission	Unclassified

1 CONTENTS

2 DOCUMENT CONTROL

2.1 REVISION HISTORY

The main versions of the document and associated changes are listed in the table.

Version	Date	Amendment
1.0	March 2005	Final
1.1	April 2005	Final
1.2	April 2005	Final
1.3	January 2014	Code edited and updated to be in line with current processes
1.4	March 2014	Code reviewed and updated from FENZ SME and industry consultation
1.5	June 2015	Code edited and updated to be in line with current processes
1.6	July 2015	Code edited and updated to be in line with current processes
1.7	July 2017	Code revised to new statutory basis - Fire and Emergency New Zealand Act 2017. Fire Service Act and Forest and Rural Fires Act superseded.
1.8	November 2018	Code reviewed and updated to current state environments
1.9	March 2019	Code reviewed and updated to current state environments from FENZ SME and industry consultation

2.2 COPYRIGHT

80 The Terrace
PO Box 2133
Wellington
New Zealand
Phone: (04) 496 3600

Document owner and contact:
Stuart Waring
FENZ System Owner
Information, Communications and Technology Services

3 PURPOSE OF THIS DOCUMENT

The purpose of this Code of Practice is to:

- Establish Fire and Emergency New Zealand (FENZ) objectives and principles for the national Automatic Fire Alarm System (AFAS) and monitoring fire alarms
- Establish the roles and responsibilities for the governance and operation of the AFAS
- Specify the practice and standards of compliance underpinning the operation of the AFAS
- Describe the architecture, technical specification and support for each domain of the AFAS

The requirements of this Code are mandatory and compliance is a condition for supplying services related to the Automatic Fire Alarm System (AFAS) and to Fire and Emergency New Zealand (FENZ).

4 OBJECTIVES

4.1 FIRE AND EMERGENCY NEW ZEALAND PRINCIPAL OBJECTIVES

Fire and Emergency New Zealand (FENZ) is a New Zealand Crown Entity enacted by the Fire and Emergency New Zealand Act 2017, and section 7 of the Crown Entities Act 2004. The principal objectives of FENZ are:

(a) to reduce the incidence of unwanted fire and the associated risk to life and property:
(b) in relation to the main functions of FENZ under section 11 of the Fire and Emergency New Zealand Act 2017 (and the additional functions of FENZ under section 12):
  (i) to protect and preserve life; and
  (ii) to prevent or limit injury; and
  (iii) to prevent or limit damage to property and land; and
  (iv) to prevent or limit damage to the environment.

FENZ employs approximately 1700+ career firefighters, 600+ management and support personnel, and 11000+ urban and rural volunteer firefighters throughout New Zealand. Organisational assets include over 630 fire stations, area offices, regional and national headquarters, and communications/operations centres. FENZ manages a national fleet of appliances, support vehicles, specialist incident command and hazardous substances vehicles, and operational equipment and assets, along with Information, Communications and Technology (ICT) equipment, infrastructure and telecommunications networks.

Over 6000 commercial and industrial buildings are connected to the AFAS, including over 24,000 fire alarm sensors across various sensor networks, telecommunication networks and multi-domain technologies and infrastructures. The AFAS also connects to a multitude of manual call points and sprinkler actuators, traverses 6 multi-tenanted domains with varying ICT infrastructure and information systems, and is supported by this Code of Practice (CoP) and various policies, standards and specifications.

4.2 AUTOMATIC FIRE ALARM SYSTEM (AFAS) OBJECTIVES

FENZ operational objectives for the AFAS are to:

(a) Provide a national AFAS that supports its obligations under the Fire and Emergency New Zealand Act 2017, and to meet strategic goals and outcomes.
(b) Provide Fire Alarm (FA) signal transportation and message handling as an integrated part of the AFAS that meets or exceeds AFAS performance standards set out in this CoP.
(c) Enable the FENZ Communication Centres to receive messages related to fire alarm events via the service provider interface of the Signal Transport System Message Handling System (STSMHS) to support FENZ operational response and achievement of service levels. These messages will conform to the 'Automatic Fire Alarm Service Provider Computer Interface Specification' (AFASPCIS).
(d) Provide end-to-end building owner and AFASP customer information provisioning to FENZ systems to support False Alarm administration, reduction, and assurance
(e) Obtain intelligence from fire alarms to support and enhance FENZ operational response.
(f) Provide for all connected fire alarms to be monitored and service agents notified of defects
(g) Encourage fire alarm owners to connect their fire alarms directly to FENZ
(h) Limit FENZ response to fire calls only
(i) Promote reduced incidence of False Alarms from connected systems

(j) Actively innovate to enable FENZ to gain more information from intelligent fire alarm and environmental monitoring systems than just 'fire', 'defect', 'isolate', and 'normal' messages (where the fire alarms and environmental sensor networks have the capacity to provide that additional information).

5 INTRODUCTION

The FENZ National Automatic Fire Alarm System (AFAS) consists of five interconnected operating domains as described in Section 4 (in this context a system domain is an area of control delegated to, or contracted by FENZ to, a specific system actor). AFAS system domains include:

1. Built Environment Domain – Fire Alarm (FA) infrastructure and sensor networks domain
    - The built environment domain system actor is either the building owner or delegated representative, which may include a fire alarm service agent
2. AFASP Domain - provides interconnection to the built environment sensors, transforms incoming sensor signals to system-standard format messages and forwards the resulting messages to the FENZ STSMHS Domain and to the relevant service agent
    - The AFASP Domain system actor is the AFASP contractor
3. FENZ STSMHS Domain - receives the messages from the AFASP Domain system, correlates incoming messages to eliminate duplicates transmitted over multiple paths and forwards the messages to FENZ communications centres in the Police Domain
    - The FENZ STSMHS domain system actor is the IaaS contractor
4. NZ Police Domain – FENZ Communications Centre which dispatches responders or takes other appropriate actions
    - The NZ Police Domain system actor is Police ICT technical support
5. FENZ Domain - maintains configuration records, incident histories and billing records
    - The FENZ Domain system actors are the Comcen Communicators, ICT technical support and false alarm administrators

6 PRINCIPLES OF OPERATION

The AFAS is a life critical system. The system will meet FENZ Service Criticality definitions (Appendix 1) and performance standards prescribed in this CoP. The following operating principles apply:

1. The primary purpose of the AFAS is to transmit signals from fire alarm sensors (and other built environment sensors) to the appropriate responders. Responders may include FENZ brigade units dispatched by the Communications Centres (Comcens), or service agents dispatched directly by the AFASP or by a parent service company.
2. The AFAS will be used by FENZ Comcen personnel on a 24 x 7 basis, 365 days per year
3. The AFAS is deemed a life critical system to provide services on a 24 x 7 basis, 365 days per year – where human lives and property may be endangered if the production system is unavailable to users
4. FENZ Comcen personnel will access the system from terminals in the Comcen (i.e. from the shared FENZ/NZP Communications and Resource Deployment environment), which include the Computer Aided Dispatch (CAD) terminal and the AFAS Customer Alarm Terminal (CAT).
5. The STSMHS will also be accessed from terminals in the STSMHS Domain and FENZ Domain for technical support purposes
6. Development and Test instances of the STSMHS will be supported by the same resources and under the same strategy as the production instance.
7. FENZ ICTS will manage support agreements with external technology suppliers in support of the services identified in the AFAS support strategy.
8. Services and resources deployed within the NZP CARD environment will be supported in accordance with the STSMHS Agreement, and the FENZ/NZP Shared Information Technology Environment (SITE) Agreement.
9. NZ Police Domain CARD infrastructure and systems (excluding the STSMHS) are supported by Hexagon and NZ Police ICT Group.
10. The FENZ STSMHS domain is supported by the STSMHS Supplier (Unisys NZ) in accordance with the STSMHS Agreement
11. FENZ Domain infrastructure and systems (excluding the STSMHS) are supported by FENZ ICT and other various Suppliers.

12. AFASP Domain infrastructure and systems (excluding the STSMHS) are supported by AFASP ICT specialists other various Suppliers, and in accordance with the AFASP Agreements.
13. The STSMHS will be supported by full service desks for each domain, manned on a 24 x 7, 365 days per year basis as described in the AFASP, STSMHS and SITE Agreements and Services Schedules.
14. The AFAS will align with best practice guidelines outlined in the Information Technology Information Library (ITIL v3) Service Design framework, and various mandatory and recommended NZ Government ICT standards including the NZ Information Security Manual.

7 ROLES AND RESPONSIBILITIES (PRIMARY)

7.1 FIRE AND EMERGENCY NEW ZEALAND

Fire and Emergency New Zealand (FENZ) has overall responsibility for the management and operation of the Automatic Fire Alarm System (AFAS). In meeting its responsibilities, FENZ may appoint agents and/or representatives with authority to act on its behalf and delegate certain specific roles and activities to be performed by those agents or representatives.

The responsibilities and functions of FENZ with respect to the AFAS encompass the following functions and/or activities:

1. Monitor incoming fire alarm messages and respond with appropriate actions and resources to these messages
2. Maintain and operate the AFAS to permit direct or indirect exchange of data with Automatic Fire Alarms (AFAs) as specified in the AFASPCIS and in this document
3. Collect and store information about events handled by the AFAS as necessary to support its internal operations and to effectively and efficiently manage the system. This may include information about fire events, and non-normal system and device state information including defects, test, isolate and return-to-normal events as specified in appropriate internal documents
4. Undertake the direct responsibility for the following aspects of the AFAS system(s):
    a. all software, systems and communications links between the Service Provider Interface of the STSMHS and the Communications Centre dispatch system(s)
    b. all software, systems and communications links between the Signal Transport System Message Handling System (STSMHS) and FENZ 'back-end' systems
5. Maintain and distribute FENZ AFASPCIS and 'Protocol Specification' documents
6. Maintain and distribute interface software modules for installation on the AFASP communications gateway/concentrator to allow the AFASP software to connect to and interoperate with the STSMHS
7. Maintain and distribute fire alarm routing table specifications and information to the STSMHS Service Provider
8. Maintain and publish the standards and procedures for certification of Automatic Fire Alarm Service Providers (AFASPs) in the 'Certification of Automatic Fire Alarm Service Providers' or other designated documents as revised and published from time to time
9. Appoint and certify AFASPs and AFASP systems and system configurations to operate and monitor the alarm signal event collection, forwarding and monitoring processes as set out in this Code of Practice, the 'Certification of Automatic Fire Alarm Service Providers' document and other applicable specification and standards documents
10. Review and authorise significant changes to those systems, system configurations, processes and procedures.
11. Audit the operation of the AFAS and the management, operation of AFASPs with respect to the standards and practices set out in the 'Certification of Automatic Fire Alarm Service Providers' document and this Code of Practice. For more information, see Section 9: AFAS Processes, Policies, Procedures and Standards
12. Invoice the AFASPs for the fees payable by the AFASP to FENZ in accordance with the applicable 'Contract for Service' between FENZ and the AFASP.

7.1.1 FIRE ALARM CONNECTIONS AND DISCONNECTIONS

With respect to fire alarm connections and disconnections, FENZ will maintain and publish standards, practices and specifications for:

1. Alarm device connections to and disconnections from FENZ AFAS
2. All processes related to the AFAS
3. Procedures, standards and processes for query of data about AFA unit status and AFA unit status updates.

In addition, FENZ will provide a Fire Alarm Identification Number (FAID) for each device connected to the AFAS.

See Section 9.2: Fire Alarm installation and connection standards.

7.1.2 TELECOMMUNICATIONS AND TELECOMMUNICATIONS LINKS

With respect to telecommunications links maintained and operated by FENZ or its agent/designee, FENZ will:

1. Develop standards and procedures for notification to AFASPs and to the Signal Transport System Message Handling System Service Provider (STSMHSSP) of faults and service outages concerning FENZ-operated communications links and/or associated services
2. Provide timely notification to affected parties in accordance with the standards and procedures set out in point 1
3. Work with the AFASPs and the STSMHSSP as appropriate to ensure the efficient and effective operation of the AFAS and related functions
4. Designate and provide a point of contact and a means of contact for the AFASPs and the STSMHSSP to contact appropriate FENZ staff or agents at all times - 24 hours per day, 7 days per week.

7.1.3 UNWANTED AND FALSE FIRE ALARMS

FENZ or its agent/designee will:

1. Develop and publish standards, practices and procedures for notifying AFASPS of unwanted/false alarm events originating from AFA devices connected to the AFAS through the AFASP
2. Notify the AFASP of unwanted/false alarm events in accordance with the standards and procedures set out in point 1
3. Provide a method and electronic interface for the AFASP to enter data concerning unwanted/false alarms in accordance with the standards and procedures set out in point 1
4. Undertake processes and procedures to follow-up unwanted/false alarm incidents as necessary to ensure efficient and effective operation of the system, including, but not limited to providing notice to responsible parties of infractions, sending warning letters, assessing and billing for applicable penalties, handling queries and settling disputes related to unwanted/false alarm incidents and any assessed penalties.

7.2 AUTOMATIC FIRE ALARM SERVICE PROVIDERS

Automatic Fire Alarm Service Providers (AFASPs) are appointed and certified by FENZ to manage the:

1. Operation of Fire Alarm (FA) units
2. Operation of the telecommunications links between those FA units and the AFASP domain system
3. Transmission of event notification messages from the AFASP domain system to the STSMHS
4. Dispatch of Service Agents to attend to alarm and fault incidents
5. Management of installation and testing of new or replacement FA monitoring equipment
6. Operation and monitoring of the overall system to ensure that all performance standards and other requirements are met.

7.2.1 COMPLIANCE TO STANDARDS AND PRACTICES

The AFASP is responsible for ensuring that:

1. At all times they comply with all standards, requirements and codes of practice for the AFAS and that they maintain a current certification in accordance with the standards and procedures set out in the 'Certification of Automatic Fire Alarm Service Providers' document and in this Code of Practice
2. All connected fire alarms meet applicable standards (NZS 4512:2010: Fire detection and alarm systems in buildings) and that they are fitted with access devices that are either separate or integrated with the alarm unit, which:
    a. immediately transmit alarm and state change event data to the AFASP communication gateway for onward transmission to FENZ STSMHS
    b. are powered from monitored un-interruptible energy (power) supplies having sufficient capacity to sustain operation of the equipment, communications device interface and any transmission devices powered by them, for a minimum of 24 hours in the event of mains power supply failure
    c. incorporate an automatic testing facility to test the energy supply and detect failure of batteries and power supply devices at intervals not exceeding 48 hours. Batteries must have the capability to provide immediate notification of failure of the charging circuitry or of the battery itself. Notification

of the failure should be provided by way of the state indicators/state notification capabilities of the fire alarm

d. provide capability to generate test signals complying with the AFASPCIS
e. provide the capability to provide a 'test correct' or successful test indication at the originating FIRE ALARM device on receipt of a successful test indication from the STSMHS/AFASP communications gateway.

7.2.2 FIRE ALARM CONNECTIONS AND DISCONNECTIONS

AFASPs will provision and commission fire alarm connections and disconnections in Accordance with the CoP processes, standards, procedures and specifications for:

2. Fire alarm connections to and disconnections from the FENZ AFAS
4. All processes related to the AFAS
5. Procedures, standards and processes for query of data about FA unit status and FA unit status updates.

See Section 9: AFAS Processes, Policies, Procedures and Standards.

7.2.3 FIRE ALARM SIGNALS AND SIGNAL HANDLING

The AFASP must process all fire alarm and state change event signals from FIRE ALARM units connected to their communication gateway/concentrator in accordance with the performance standards set out Section 9: AFAS Processes, Policies, Procedures and Standards. The AFASP must ensure that:

1. all signals from attached alarm units are transmitted to FENZ without delay
2. transmission of messages are monitored and that when fire alarm messages are not acknowledged by the STSMHS within the time interval specified in applicable standards, manually transmit notice of the fire alarm event to FENZ by way of the 111 emergency contact system using specified procedures
3. signals indicating device faults or defects are forwarded to the appropriate Service Agent without delay and that the Service Agent responds to the incident and that the unit is returned to normal state as soon as practicable
4. they maintain awareness of the status of all incidents and follow-up as necessary to ensure prompt attention to all events
5. they maintain and operate the elements of the Automatic Fire Alarm System within its responsibility to ensure that operations comply with applicable standards and procedures and that performance meets the standards set out in Section 9: AFAS Processes, Policies, Procedures and Standards
6. where operation of facilities are delegated to third parties, including owners of monitored premises, they must ensure that delegated operations meet the applicable performance standards set out in Section 9: AFAS Processes, Policies, Procedures and Standards
7. they report to FENZ on a six monthly basis, as set out in the Contract of Service between FENZ and the AFASP or supplementary instructions from the FENZ, the performance of all facilities against the standards set out in the "Policies. Practices and Standards" section of this Code of Practice
8. malfunctioning fire alarms are isolated as soon as reasonably practical and the appropriate Service Agent is dispatched to attend to the fault
9. attached devices do not remain in test or isolated mode after the completion of service and tests, including follow-up with the responsible Service Agent during normal business hours and at the end of each working day where devices remain in isolate or test status
10. they escalate service incidents which are not resolved within time frames set in applicable service standards as appropriate in compliance with incident handling procedures
11. they respond to query or control messages from FENZ via the STSMHS as specified in the AFASPCIS
12. all parties to tests are aware that testing is in progress and of the result of the testing.

7.2.4 MANAGEMENT OF THE SYSTEM

The AFASP must provide and manage the provision of service to customers of the AFAS system whose alarm equipment is monitored and managed by way of its systems.

The AFASP must ensure that:

1. installation of all fire alarms to be connected to FENZ AFAS meets the relevant New Zealand Standards(s) and that a Certificate of Completion has been provided by an independent, accredited inspector when available immediately after connection

2. connections and disconnections of equipment to AFAS are carried out in accordance with applicable standards and FENZ processes outlined in Section 9.2: Fire Alarm installation and connection standards as revised and published by FENZ from time to time
3. each installed device or device configuration passes the tests set out in Section 9.3: Fire Alarm Commissioning Process as revised and published by FENZ from time to time
4. they maintain required records and electronic data regarding the connected devices, the premises at which they are installed, the premise owner or owner's agent and the responsible Service Agent. The AFASP must maintain appropriate information within its internal systems and ensure that FENZ systems are updated as set out by FENZ in applicable operating procedures and updated from time to time
5. they complete the tasks designated for them in the transfer of alarm monitoring service to a different AFASP on a timely basis and in compliance with standards and practices set out by FENZ and revised and published from time to time
6. response to all incidents related to the service or equipment within their management responsibility meet the service standards as set out in Section 9: AFAS Processes, Policies, Procedures and Standards as revised and published by FENZ from time to time
7. they provide timely notice to FENZ and to the owner of the premises with installed fire alarm equipment of any failure within the AFASP system which may affect transmission of signals indicating fire events from the FIRE ALARM to FENZ STSMHS. This notice should set out information known about the cause and/or impact of the failure and actions being taken to restore normal operations
8. they provide periodic updates concerning failures as set out in point 7 above
9. they establish a contact point and contact procedures and that FENZ and the STSMHS Service Provider have current contact and contact information allowing contact at any time, 24 hours per day, 7 days per week.

7.2.5 COMMUNICATIONS AND MONITORING SYSTEMS

The AFASP maintains and operates communications and networking systems that receive signals from FIRE ALARM units on customer premises, transform incoming signals into standard alarm data format messages and transmit those messages to FENZ by way of the STSMHS.
Those systems used for monitoring and transmission of signals for the AFAS must comply with the requirements set out in this Code of Practice and the AFASP must ensure that:

1. they maintain and operate its certified monitoring and management systems in accordance with the information provided to FENZ during the certification process
2. they notify FENZ in advance and gains FENZ approval for any changes to the configuration or operation of its certified monitoring centres or infrastructure or any connected equipment or associated processes. Significant changes may require re-certification of the configuration.

7.2.6 REPORTING

The AFASP must provide reporting to FENZ regarding the management, operation and performance of its facilities providing service to the AFAS. In addition, the AFASP must provide to FENZ specified information regarding the equipment, premises, premise owner or owner's agent and Service Agent and must ensure that the information held by FENZ is at least as current as that held by the AFASP i.e. they must provide updates to FENZ information to reflect changes in their own records.
The AFASP must:

1. Collect and forward to FENZ in the manner specified in the information set out in Section 9: AFAS Processes, Policies, Procedures and Standards for each installed fire alarm device
2. Update, in the manner specified, the records held by the FENZ
3. Maintain file copies of all contracts and correspondence between the AFASP and the premise owner, its agent and/or the responsible Service Agent regarding the fire alarm devices, device installation, and monitoring and service arrangements
4. Maintain records of all faults and service incidents for a period of not less than 12 months from the completion of the incident response
5. Maintain system logs of all communications between the attached FIRE ALARM devices and the AFASP communications gateway/concentrator, and between the AFASP communications gateway/concentrator or server and FENZ STSMHS for a period of 18 months

6. Provide a report, on a six monthly basis, to FENZ of its performance against the performance standards set out in Section 9: AFAS Processes, Policies, Procedures and Standards and as set out in the 'Contract of Service' between FENZ and the AFASP and in supplementary instructions issued from time to time to the AFASP by FENZ under the terms of that contract.

7.2.7 UNWANTED AND FALSE FIRE ALARMS

Reducing the number and the cost of unwanted and false alarms is a key ongoing focus for the FENZ. To assist in this effort, the AFASP must:

1. determine, as soon as reasonably practicable, the cause of false alarm events originating from FIRE ALARM units connected by way of the AFASP facility
2. collect and forward to FENZ as soon as reasonably practicable all information available to the AFASP related to the cause of unwanted and false alarm events
3. provide updated information regarding unwanted and false alarm events as soon as it becomes available to the AFASP.

7.3 SIGNAL TRANSPORT SYSTEM MESSAGE HANDLING SYSTEM (STSMHS) DOMAIN SERVICE PROVIDER

The Signal Transport System Message Handling System Service Provider (STSMHSSP) manages operation of FENZ message handling gateway, the STSMHS infrastructure-as-a-service (IaaS) and the downstream FENZ AFAS components installed in the FENZ Communications Centres. The STSMHSSP is contracted to FENZ under a Master Services Agreement and is subject to the performance standards and service criticality definitions prescribed in this Code of Practice. The STSMHSSP must:

1. operate and maintain the Message Handling System (MHS) in accordance with the STSMHS performance standards as defined and published by FENZ and as specified in the agreement or 'Contract for Service' between FENZ and the STSMHS Service Provider
2. process all fire alarm connections and disconnections to the Automatic Fire Alarm System (AFAS) in accordance with FENZ processes, as provided by FENZ and updated from time to time
3. immediately inform FENZ of any system failures that may affect the transmission of fire events to FENZ response and dispatching system
4. liaise with FENZ and the AFASPs as required to facilitate the efficient operation of the signal transport system and associated functions
5. establish a contact point and contact procedures and ensure that FENZ and the AFASPs have current contact and contact information allowing contact at any time, 24 hours per day, 7 days per week.

7.4 ROLES AND RESPONSIBILITIES (DOMAIN SPECIFIC)

Further domain and actor roles and responsibilities are specified in the each of the AFAS Domain descriptions in subsequent sections of this CoP.

8 AFAS ARCHITECTURE

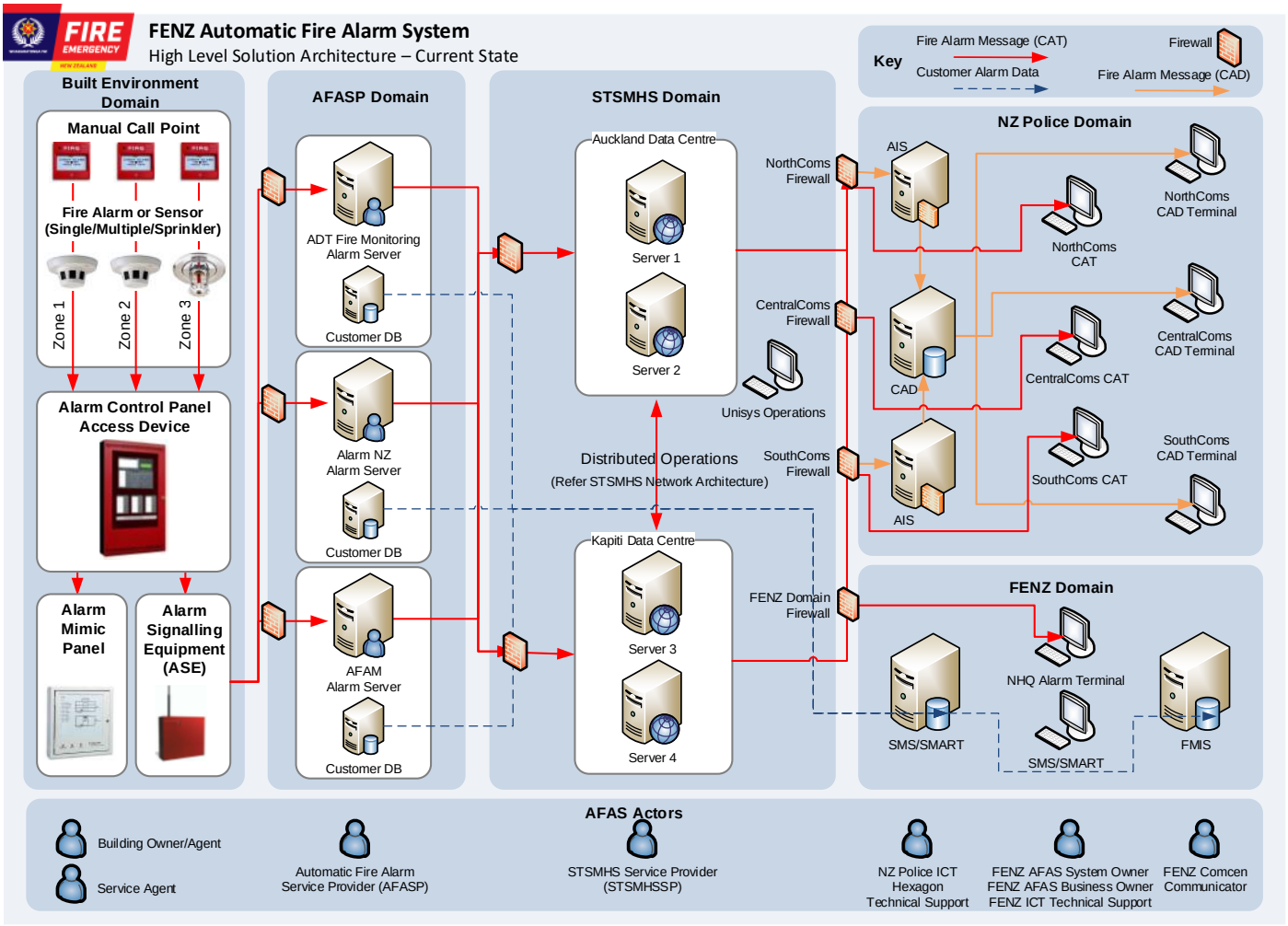


Figure 1: AFAS High Level Solution Architecture

9 AFAS DOMAINS

9.1 BUILT ENVIRONMENT DOMAIN

9.1.1 FIRE SAFETY AND WARNING SYSTEMS

Fire safety and warning systems installed in buildings are determined in accordance with the NZ Building Act 2004 and Regulations Specified Systems, NZ Building Code (NZBC) C1–C6 Protection from fire, other verification methods or alternative designs. Fire Alarm Systems are determined in accordance with NZBC Acceptable Solutions and Verification Methods F7/AS1/VM1, C/AS1-7, NZ Standards 4510/4512/4515/4541, and the acceptable risk of the relevant building as defined in the NZBC.

All of the Acceptable Solutions and Verification Methods relating to F7 (Warning Systems) are contained in F7/AS1, which provides a design solution for different types of warning systems: fire, sprinkler, smoke alarm, and the automatic alerting of FENZ. F7/AS1 also provides specific information on domestic smoke alarm systems, and those for hotels, motels or multi-unit residential accommodation in retirement villages. It sets out the location of alarms with reference to Acceptable Solutions C/AS1-7 and for every space to have at least one fire alarm sensor.

This CoP specifies and describes the current state built environment domain fire alarm systems in use and connected to the AFAS. FENZ also recognise and specify future state emerging technologies in the built environment (including the extended alarm protocol (XAP)), and this CoP will continue to be amended to include new technologies, standards and specifications when implemented and deployed by FENZ.

In general terms, all fire safety and warning systems are included in a Warrant of Fitness Compliance Schedule for a building. The building owner (or agent) is legally responsible for ensuring compliance and maintaining a current building Warrant of Fitness.

9.1.2 FIRE ALARM SYSTEMS

Fire alarm systems will be designed, installed and maintained in accordance with specific requirements of Acceptable Solution F7/AS1, with Acceptable Solutions C/AS1 to C/AS7 specifying the fire alarm system to be installed in each risk group as required by NZS 4512:2010. Fire alarm sensors will be installed throughout the firecells of each risk group as required by NZ 4512:2010. The following sections provides specific details on each fire alarm system type and the AFAS specifications required for compliance and connection to FENZ to achieve AFAS objectives:

9.1.2.1 TYPE 1 – DOMESTIC SMOKE ALARM SYSTEM

A Type 1 system is based on one or more domestic type smoke alarms with integral alerting devices. Coverage shall be limited to selected parts of a single firecell, and manufactured to at least one of: AS 3786, ISO 12239 or BS EN 14604.

SUPPORT QUALIFICATION: Type 1 domestic smoke alarms are excluded from the AFAS Code of Practice and are not covered by NZS 4512:2010.

9.1.2.2 TYPE 2 – MANUAL FIRE ALARM SYSTEM

A single or multiple zone system with an alarm panel to provide defect warning, zone index diagram, with automatic signalling to a remote receiving centre and suitable for connection to the AFAS. The system is installed in accordance with NZS 4512:2010 Fire detection and alarm systems in buildings. The manual call points are typically located close to final exits.

9.1.2.3 TYPE 3 – AUTOMATIC FIRE ALARM SYSTEM ACTIVATED BY HEAT DETECTORS AND MANUAL CALL POINTS

An automatic fire alarm system activated by heat detection (usually point-type sensors) and manual call points with automatic signalling to a remote receiving centre. Sprinkler coverage to NZS 4541 or NZS 4515 may be allowed to be substituted for all or part of the heat detection. The system is designed and installed in accordance with NZS 4512:2010.

9.1.2.4 TYPE 4 – AUTOMATIC FIRE ALARM SYSTEM ACTIVATED BY SMOKE DETECTORS AND MANUAL CALL POINTS

An automatic fire alarm system activated by smoke detectors and manual call points as per a Type 2 system. Where such a system is required but the environment is such that unwanted alarms are likely, the smoke detectors may be replaced with heat detection, up to a set maximum area of heat detection coverage. The system must be designed and installed to NZS 4512:2010.

9.1.2.5 TYPE 5 – AUTOMATIC FIRE ALARM SYSTEM WITH MODIFIED SMOKE DETECTION AND MANUAL CALL POINTS

Type 5 is a variation of the Type 4 and Type 7 alarm systems requiring part of the smoke detection component to comprise only a local alarm. The local alarm system, activated by the presence of smoke, shall have audible alerting devices to warn only the firecell occupants and the building management, where such management exists.

Comment: Examples of management situations are motels, hotels or multi-unit residential accommodation in retirement villages.

The local alarm component of a Type 5 system:

a) Shall be restricted to single firecells containing sleeping accommodation, being household units or individual suites in risk group SM. The local alarm system shall not be extended to other areas such as exitways or common spaces. These shall retain a Type 4 smoke detection system, and
b) Shall have the facility to be silenced (muted) by a 'hush' switch located at a level readily able to be reached in accordance with Acceptable Solution D1/AS1. The hush switch shall mute the alarm for a time not exceeding 2 minutes, and
c) Shall be permitted only where an automatic fire detection and alarm system activated by heat detectors (part of the main alarm system) is also installed in sleeping firecells which do not already have an automatic fire sprinkler system.

Where a Type 5 system is installed, mechanical ventilation in accordance with Acceptable Solution G4/AS1 shall be provided in the kitchen area of the household unit or suite.

In exitways and common spaces the required Type 4 or Type 7 system shall not be modified. The system installation for Type 3 and Type 4 components shall comply with NZS 4512:2010.

The system installation for the local smoke alarm component shall also comply with NZS 4512:2010.

9.1.2.6 TYPE 6 – AUTOMATIC FIRE SPRINKLER SYSTEM WITH MANUAL CALL POINTS

An automatic fire sprinkler system with automatic signalling to a remote receiving centre installed throughout the building in accordance with NZS 4541:2013 Automatic fire sprinkler systems or NZS 4515:2009 Fire sprinkler systems for life safety in sleeping occupancies (up to 2000 square metres). Type 6 system is a combined automatic fire sprinkler system and Type 2 alarm. Activation of the sprinklers shall automatically activate the audible alerting devices of the alarm system.

9.1.2.7 TYPE 7 – AUTOMATIC FIRE SPRINKLER SYSTEM WITH SMOKE DETECTORS AND MANUAL CALL POINTS

An automatic fire sprinkler system with automatic signalling to a remote receiving centre plus a Type 4 smoke detection and manual call point system (including a Type 2 system). Sprinkler installation shall comply with the requirements of a Type 6 system.

9.1.2.8 TYPE 9 – SMOKE DETECTION IN AIR-HANDLING SYSTEMS

Smoke detection is used to shut down the heating, ventilation and air-conditioning (HVAC) system and close any mechanical smoke dampers to reduce the spread of smoke through the building via ducting.

9.1.2.9 TYPE 18 – FIRE HYDRANT SYSTEMS FOR BUILDINGS

These systems, complying with NZS 4510:2008 Fire hydrant systems for buildings, are required where the size or geometry of the building requires that firefighters would be required to carry or lay out more than 75 m of hose to reach all parts of a building.

9.1.3 MANUAL CALL POINTS

A fire alarm manual call point (or pull station) is an active fire protection device, usually wall-mounted with break glass/Perspex and a switch, that, when activated, initiates an alarm on a fire alarm system. In its simplest form, the user activates the alarm switch, which completes a circuit and locks the handle in the activated position, sending an alarm to the fire alarm control panel. Built environment manual call points (single or multiple) installed in commercial and industrial buildings are connected to the AFAS via hard-line infrastructure.
SUPPORT QUALIFICATION: Support for Manual Call points is the responsibility of the Building Owner or Agent.

9.1.4 FIRE ALARM

Built environment fire alarms and other sensors, including sprinklers, activate automatically and trigger an alarm message to the AFAS via the building Alarm Signalling Equipment. Signals are generally sent via wireless networks to the AFASP alarm monitoring infrastructure, with secondary communications network connectivity to ensure compliant network diversity and resilience.
SUPPORT QUALIFICATION: Support for fire alarms is the responsibility of the Building Owner, Service Agent and/or AFASP.

9.1.5 FIRE ALARM SYSTEM ALARM SIGNALS AND MESSAGING[1]

Fire alarm systems generate alarm signals and messaging that include:

1. fire or fire alarm signals originating from primary or secondary fire alarms, zone sensors, manual call points and/or automatic sprinkler systems
2. fault or defect signals indicating actual or potential sensor unit failures and which require the attendance of a service agent
3. device polls or handshaking which assure both the monitoring centre and the sensor (or sensor concentrator)

[1] Refer to AFASPCIS

device of the integrity and availability of the transmission path between the sensor field concentration point (alarm panel/ASE/CTU/NAD) and the alarm monitoring centre

4. miscellaneous signals and responses to state queries from the monitoring centre including test signals, fire alarm state, etc.

9.1.5.1 FIRE ALARM SYSTEM TYPES

Fire alarm system or related system types described in fire alarm messaging may include:

Type of System[2]	System Description
01	Domestic smoke alarm system, not suitable for connection to the AFAS
02	Manual fire alarm system
02f	Type 2 call point alarm system, not required to be connected to the AFAS
03	Automatic fire alarm system activated by heat detectors and manual call points
03b	Type 3 fire alarm system where firecells with only a single escape route require a Type 4 or Type 6 alarm
03f	Type 3 heat detection system, not required to be connected to the AFAS
04	Automatic fire alarm system activated by smoke detectors and manual call points
04a	Type 4 fire alarm with smoke detectors (battery powered)
04b	Type 4 fire alarm with smoke detectors (hardwired 12-24v)
04f	Type 4 fire detection and alarm system, not required to be connected to the AFAS
05	Automatic fire alarm system with modified smoke detection and manual call points
06	Automatic fire sprinkler system with manual call points
06f	Type 6 automatic sprinkler system plus manual fire alarm system, not required to be connected to the AFAS
07	Automatic fire sprinkler system with smoke detectors and manual call points
07f	Type 7 automatic sprinkler system plus Type 4 fire detection and alarm system, not required to be connected to the AFAS
08	Emergency warning and intercommunication voice communication system (EWIS) and emergency telephone system complying with AS 2220.1
09	Smoke detection in air-handing systems
10	Natural smoke venting
11	Mechanical smoke extraction
12	Hold open device
13	Pressurisation of safe paths
14	Fire hose reels
15	Fire Service lift control
16	Emergency lighting in exit ways
17	Emergency electrical power supply
18	Fire hydrant systems for buildings
19	Refuge areas
20	Fire systems centre
21	Gas flooding
22	Gas Detection
23	Security system – Heat / Smoke
24	Portable fire extinguishers
Unknown	AFASP database has not determined the equipment type

9.1.5.2 FIRE ALARM MODE, STATUS AND MESSAGE PRIORITY[3]

[2] The suffix "f" indicates a direct connection to the AFAS is not required provided a telephone is installed and freely available at all times to enable 111 calls to be made

[3] Refer to AFASP Computer Interface Specification

Fire alarm signals originate from individual sensors or within sensor management/concentrator units embedded in the fire alarm. Each fire alarm signal includes and specifies the mode and status of the alarm unit, along with specifying the priority of fire alarm messages forwarded to the AFAS as specified in the AFASP computer interface specification (AFASPCIS):

1. NORMAL indicator reflects the current state of the monitored environment
2. ALARM indicator reflects the current state of the monitored environment
3. PRE-ALARM indicator reflects the future state of the monitored environment
4. DEFECT indicator reflects the current state or 'health' of the monitored environment
5. TEST indicator reflects the current state of the monitored environment fire system via the 'Test' switch
6. ISOLATE indicator reflects the current state of the monitored environment fire system via the 'Isolate' switch and that signals are to be disregarded by all downstream devices and processes. In particular, this indicates to the services within the monitoring centre domain that the messages originating from this device must not be on-transmitted to the STSMHS. Note that signals from an FA unit can be programmatically isolated by way of the monitoring system as well as by way of the on-device isolate switch.

9.1.5.2.1 MODES

Select text	Description
Normal	Equipment is operating normally
Test	Equipment is being tested by service agent or AFASP
Isolate	Equipment is isolated by service agent or AFASP
Evacuate	Building is being evacuated
Shunt	Equipment is shunted by FENZ
Unknown	AFASP database has not determined the mode
Water off	Sprinkler system is disconnected from water supply.

9.1.5.2.2 STATUS

Select text	Description
Normal	Normal status
Alarm	Fire has been detected
Defect	Fire alarm equipment self-monitoring has determined that it is defective
Trouble	Fire alarm equipment has been tampered with
PreAlarm	Fire alarm equipment has detected that a fire alarm may be issued shortly
Unknown	AFASP database has not determined the current status

9.1.5.2.3 PRIORITY ALLOCATION

Fire alarm messages will include a message consisting of one of the following Priority No.s:

Priority	Description	
97–99	Verified (approved) automatic fire call	Fire
94–96	Unverified (approved) automatic fire call	
93	Verified (non approved) automatic fire call	
92	Verified manual fire call	
91	Unverified (non approved) automatic fire call	
90	Unverified manual fire call	
80–89	Hazardous materials or environments	Non-fire
70–79	Evacuations	
60–69	Equipment defects	
50–59	Equipment isolates	
40–49	Equipment troubles	
30–39	Database queries, changes and commands	
20–29	Operator logs and actions	
10–19	Equipment tests	
2–9	Normal events	

9.1.6 ALARM CONTROL PANEL (ACCESS DEVICE)

A Fire Alarm Control Panel (FACP), or Fire Alarm Control Unit (FACU), is the controlling component of a Built Environment Domain Fire Alarm System. The panel receives information from environmental sensors designed to detect changes associated with fire, monitors their operational integrity and provides for automatic control of equipment, and transmission of alarm messages to the AFAS, also necessary to prepare the facility for fire based on a predetermined sequence.

The panel may also supply electrical energy to operate any associated sensor, control, transmitter, or relay. There are four basic types of panels: coded panels, conventional panels, addressable panels, and multiplex systems.

SUPPORT QUALIFICATION: Support for Alarm Control Panels is the responsibility of the Building Owner, Service Agent and/or AFASP. Further FENZ approvals are required for Alarm Control Panels with territorial authorities and building owners under the Building Act.

9.1.7 ALARM MIMIC PANEL

A Fire Alarm Control Panel Repeater (or Mimic) Panel is a remotely located panel which gives access to main panel controls. It normally has only a communication cable connecting it to the main panel (RS-485 or IEEE) but allows you to see all the same information as the main panel and perform all the same functions from a remote location.

It is common to find a repeater panel placed near a reception or security area for easy access. While the actual fire panel would be out of sight in a utility room due to the large number of wires that must be run to the actual main panel.

A mimic panel means there is a graphic representation of the building and zones on the face of the main panel and indicator lights showing the status of the sensors within the graphic representation.

SUPPORT QUALIFICATION: Support for Alarm Mimic Panels is the responsibility of the Building Owner, Service Agent and/or AFASP.

9.1.8 ALARM SIGNALLING EQUIPMENT (ASE)

Alarm Signalling Equipment (ASE) allows for an alarm signal generated by the fire alarm and FACP to be automatically and wirelessly transmitted to the AFASP.

Multiple fire alarm panels or sprinkler systems can be operated independently on the same ASE connection, up to a maximum of 16.

Generally, ASE combines fire alarm signalling with its own status and sends it to the AFASP domain system using an in-built cellular radio modem as the primary telecommunications network connection. AFAS communications network business continuity requires all ASE connections to the AFASP domain system to meet the Availability and Performance Standards prescribed in section 9.1 of this CoP. To ensure communications network business continuity, a secondary (backup) communications network connection[4] to the AFASP domain system must be available should the primary communications network connection become unavailable, unless the AFASP can demonstrate that:

1. each primary connection from the ASE to the AFASP domain system has achieved persistent connection availability above 99.7% for each reporting period; or
2. the AFASP has entered into a Waiver with their Customer where it is recognised that the communications network cannot achieve the minimum AFAS Availability and Performance Standards

SUPPORT QUALIFICATION: Support for ASE is the responsibility of the Building Owner, Service Agent and/or AFASP.

9.1.9 ROLES AND RESPONSIBILITIES

9.1.9.1 BUILDING OWNER – FIRE ALARM OWNER

Within the AFAS Built Environment domain, Building Owners and/or fire alarm owners are responsible for:

1) carrying out all fire alarm connections and disconnections to the AFAS in accordance with FENZ processes (as outlined in the Code of Practice), as provided by FENZ and updated from time to time.

[4] Secondary communications will be either an enduring hard-line communications network (e.g. Fibre), or a separate wireless communications network to ensure diversity (e.g. with the CTU having dual SIM)

2) verifying that the installation of the fire alarm to be connected to the AFAS meets the relevant New Zealand Standard(s), and a Certificate of Completion has been provided by an accredited inspection body or IQP when available immediately after connection to the AFAS. If not required in the relevant standards, each completed fire alarm system must also pass the test(s) described in this Code of Practice and relevant FENZ test and certification processes prior to the connection to the AFAS.
3) carrying out all changes to data related to fire alarms connected to the AFAS and their owners' details in accordance with FENZ processes, as provided by FENZ and updated from time to time.
4) carrying out the migration of a fire alarm owner to a different service provider in accordance with FENZ processes, as provided by FENZ and updated from time to time.

9.1.9.2 SERVICE AGENT

Service Agents provide installation, maintenance and servicing for fire alarm equipment. Service Agents are responsible for:

1) installation of all fire alarms to be connected to FENZ AFAS meeting the relevant New Zealand Standards and that a 'Certificate of Completion' has been provided by an accredited inspection body or Independent Qualified Person (IPQ)[5] Inspector when available immediately after connection.
2) ensuring connections and disconnections of equipment to the AFAS are carried out in accordance with applicable standards and FENZ processes outlined in Section 4: Policies, practices and standards as revised and published by FENZ from time to time
3) ensuring each installed device or device configuration passing the tests set out in Section 9.3: Fire Alarm Commissioning Process prior to connection to the AFAS as revised and published by FENZ from time to time;
4) attending to fire alarm premises for post alarm actuation services as soon as reasonably practicable, for example, for fires or false alarms.
5) ensuring fire alarm tests are satisfactory and if not, appropriate corrective action is taken.
6) reduction in the number and the cost of unwanted and false alarms, and must:
    a. determine, as soon as reasonably practicable, the cause of false alarm events originating from the fire alarm for which they provide maintenance and service
    b. collect and forward to FENZ or its designated agent, as soon as reasonably practicable all information available to the Service Agent related to the cause of unwanted and false alarm events
    c. provide updated information regarding unwanted and false alarm events to FENZ or its designated agent as soon as it becomes available to them.

Role	Responsibility
Building Owner	Alarm Ownership, Installation
Service Agent	Alarm Installation and Servicing
AFASP	Alarm Monitoring and Transmission

9.1.10 DEMARCATIONS

Demarcation	Component	Responsibility
Built Environment Domain	Manual Call Points	Owner
	Fire Alarm	Owner
	Alarm Control Panel	Owner
	Alarm Mimic Panel	Owner
Fire Alarm Infrastructure	Manual Call Points	Servicing and support
	Fire Alarm	Servicing and support
	Alarm Control Panel	Servicing and support
	Alarm Mimic Panel	Servicing and support
AFASP Domain system	Alarm Signaling Equipment	Owner, Servicing and support

[5] An IQP is a person (or firm) approved by the territorial authority as qualified to inspect certain specified fire alarm systems and ensure that necessary maintenance occurs. "Independent" means they have no financial interest in the building.

9.1.11 FIRE ALARM COMMISSIONING

SUPPORT QUALIFICATION: Fire Alarm Commissioning procedures are described in Section 9.3: Fire Alarm Commissioning Process and FENZ national procedure PMPP07_Commissioning Private Fire Alarms process.

9.1.12 SUPPORTING DOCUMENTS, POLICIES, PROCEDURES, STANDARDS

Refer to:

- FENZ RCC-2 12b Fixed Systems Commercial Study Guide
- FENZ F2 Fixed fire protection systems NCI
- FENZ G1-2 - Private Fire Alarms (NCI 24)
- FENZ National Procedure PMPP07 - Commissioning Private Fire Alarms
- FENZ National Procedure – Fire Alarm Panel Approvals
- FENZ AFASP Computer Interface Specification (AFASPCIS)
- FENZ AFASP Computer Interface Specification (AFASPCIS) Extended Alarm Protocol (XAP)
- NZ Standard 4512
- NZ Standard 4515
- NZ Standard 4541
- NZ Building Act 2004 and regulations
- NZ Building Code - Acceptable Solutions C/AS1 to C/AS6; Acceptable Solution D1/AS1

9.2 AFASP DOMAIN

9.2.1 AUTOMATIC FIRE ALARM SERVICE PROVIDERS SYSTEMS

AFASP Systems provide monitoring facilities and interconnection between the Built Environment Domain and the STSMHS Domain. FENZ does not specify the system architecture of each AFASP system, however each AFASP system is subject to minimum AFAS performance standards described in Section 9.1: Availability and Performance Standards for AFASP systems and facilities, must comply with the AFASPCIS and meet the following minimum criteria for monitoring facilities and services for connecting fire alarms to the AFAS:

1. AFASPs must ensure that Access Devices (alarm control panels) meet the following requirements, if the Access Device is not integrated in the fire alarm:
    a. The Access Device must be powered from monitored uninterruptible energy supply having sufficient capacity to sustain operation of the Access Device for a minimum of 24 hours in the event of a mains failure; and
    b. The Access Device must incorporate an automatic testing facility where at intervals not exceeding 48 hours the energy supply is tested in a way that will detect failure of the battery. If this test fails a message indicating this failure must be forwarded to FENZ and the AFASP.
    c. The Access Device must incorporate a facility to verify the current state of any Fire Alarm connected to the panel.
2. The AFASP must provide and maintain primary and secondary network connections to the STSMHS Domain as specified in this CoP and the AFASPCIS.
3. The AFASP's equipment must allow for FENZ to automatically poll the AFASP's database in respect to all fire alarm mode and status, and date/time of the last mode and status change.
4. The AFASP must monitor the performance standards contained in the AFASP Agreements, and report as required by FENZ.
5. The AFASP must forward messages indicating fire alarm fire-events to the relevant Service Agent, and follow up return of the fire alarm to normal. For avoidance of doubt, the AFASP must send fire alarm related messages to a particular Service Agent only if that Service Agent is recorded as the Service Agent for that particular fire alarm. The AFASP must not send messages related to a particular fire alarm to any other party than FENZ, the Service Agent recorded as the Service Agent for that fire alarm, or the owner of that fire alarm.
6. The AFASP must forward messages indicating fire alarm defects to the relevant Service Agent, and follow up the return of these defect fire alarms to status 'normal' (as defined in the AFASPCIS). This includes the AFASP advising Service Agents at the beginning and end of each working day of all respective fire alarms with status 'defect'.

7. The AFASP must forward messages indicating a fire alarm is tested to the relevant Service Agent, and follow up the return of these fire alarms to mode 'normal' (as defined in the AFASPCIS). This includes the AFASP advising the Service Agents at the start and end of each working day of all respective fire alarms with mode 'test'.
8. The AFASP must forward messages indicating a fire alarm is isolated to the relevant Service Agent, and follow up the return of these fire alarms to mode 'normal' (as defined in the AFASPCIS). This includes the AFASP advising the Service Agents at the beginning and end of each working day of all respective fire alarms with mode 'isolate'.
9. AFASP messages to Service Agents must include the following information:
    a. Date and time of the event (year, month, day, hour, minute, second);
    b. fire alarm number (AreaFAID, as defined in the AFASPCIS);
    c. Mode and Status of the fire alarm (as defined in the AFASPCIS);
    d. Name of the Protected Premises that houses the fire alarm; and
    e. AFASP identifier (AFASPID, as defined in the AFASPCIS).
10. The time period for forwarding messages from the AFASP Domain system to the FENZ STSMHS is:
    a. 10 seconds for 90% of all messages, and
    b. 15 seconds for all messages from the receipt of such a message from a fire alarm by the AFASP Domain system.
    c. For avoidance of doubt the time periods specified above do not include the time the message is travelling from a fire alarm to the AFASP Domain, or the time the message is travelling from the AFASP Domain to the Service Agent's message receiving equipment.

9.2.2 CERTIFICATION

Annual AFASP certification demonstrates that AFASPs:

1) Have a formal commitment to FENZ through a structured management system;
2) Consistently manage processes;
3) Possess a structured quality management system to continually improve their processes and service to the general public and FENZ; and
4) Operate within a Grade C2 premises as detailed in Australian Standard AS 2201.2-2004.

AFASP certification has been developed by FENZ to provide Service Providers with a model for their management system. It is based upon a variety of standards such as ISO9001:2000 and the Telarc Q-Base Code. It also references other documents, specifically the Australian Standard AS 2201.2-2004. It recognises the need for a management system to have formalised structures and systems in place meeting the needs of FENZ and Service Providers.

9.2.3 ARCHITECTURE

AFASP System Architectures are Commercial-in-Confidence and not prescribed in this Code of Practice. Refer to each AFASP for system architectures.

9.2.4 ROLES AND RESPONSIBILITIES

Role	Responsibility
Operations Manager	ADT
Technical Operations	ADT
Operations Manager	Alarm NZ
Technical Operations	Alarm NZ
CEO	AFAM
Technical Operations	AFAM

9.2.5 DEMARCATIONS

In general, demarcations points for AFASP systems are consistent. Each AFASP network architecture includes a primary telecommunications network channel for all fire alarm messaging, with secondary telecommunications network channel for redundancy and business continuity.

Demarcation points are set as follows:

Demarcation Point	Component	Responsibility
Built Environment Domain	Alarm Signaling Equipment	AFASP
FENZ STSMHS Domain	STSMHS Domain Router	Unisys

9.2.6 SUPPORTING DOCUMENTS, POLICIES, PROCEDURES, STANDARDS

Refer to:

- FENZ Certification for Automatic Fire Alarm Service Providers
- FENZ AFASP Computer Interface Specification (AFASPCIS)
- FENZ AFASP Computer Interface Specification (AFASPCIS) Extended Alarm Protocol (XAP)
- AS 2201.2-2004
- ISO 9001:2000
- Telarc Q-Base Code

9.3 SIGNAL TRANSPORT SYSTEM MESSAGE HANDLING SYSTEM (STSMHS) DOMAIN

9.3.1 FENZ STSMHS DOMAIN

The STSMHS solution is deployed on standard off-the-shelf DELL servers running Windows Server 2012 R2 Standard Edition. It utilises industry standard network equipment.

The Auckland Data Centre (ADC) and Kapiti Data Centre (KDC) sites are configured to permit independent operation should the other site fail.

All external organisations are connected to the STSMHS at both ADC and KDC. FENZ NHQ connectivity to ADC is not essential for fire alarm transmission under DR conditions, but will need to be connected to ADC should there be a failure of the KDC site for more than a few days.

Telco diversity was established by using both Spark and Vodafone for WAN connectivity to the Comcens. Each AFASP also uses at least two different telco providers for WAN connectivity to the STSMHS.

9.3.2 ARCHITECTURE

The STSMHS Domain Architecture is a distributed operations architecture and infrastructure-as-a-service deployed across the two Unisys data centres located in Auckland and Kapiti, interconnecting the AFASP Domain with the NZ Police and FENZ Domains. The STSMHS acts as an enterprise service bus (ESB), transporting fire alarm messages within life critical service levels.

Due to the security classification of the STSMHS Architecture, this is restricted to applicable FENZ ICT technical support and STSMHS Domain Supplier personnel. The STSMHS is fully described in the STSMHS Solution Architecture Description (SAD) document, Schedule 5 annexed to the STSMHS Agreement. Please contact the FENZ AFAS system owner for further information.

9.3.3 ROLES AND RESPONSIBILITIES

Role	Responsibility
Systems Architect	STSMHS Level 2 Technical Support
Architecture Specialist	STSMHS Operations Management
Kapiti Data Centre	IaaS Support and Service
Auckland Data Centre	IaaS Support and Service
FENZ System Owner	AFAS system administration and custodianship

9.3.4 DEMARCATIONS OF SUPPORT RESPONSIBILITY

Demarcation Points of the STSMHS are set as follows:

Demarcation Point	Component	Responsibility
STSMHS Domain	STSMHS Router 1, 2, 3	Unisys
	AFASP Domain System	AFASP
FENZ Domain	FENZ Firewall	FENZ
	FENZ Firewall Network Connection	Unisys

Demarcation Point	Component	Responsibility
NZ Police Domain	FENZ Firewall	NZ Police
	Spark WAN	Unisys
	Vodafone WAN	Unisys
	CAT Terminal	Unisys

9.3.5 SUPPORTING DOCUMENTS, POLICIES, PROCEDURES, STANDARDS

Refer to:

- STSMHS Solution Architecture Description
- STSMHS Master Services Agreement
- FENZ AFASP Computer Interface Specification (AFASPCIS)
- FENZ AFASP Computer Interface Specification (AFASPCIS) Extended Alarm Protocol (XAP)

9.4 FENZ DOMAIN

9.4.1 STATION MANAGEMENT SYSTEM (SMS)

The FENZ Station Management System supports fire alarm customer and asset information. AFASPs access SMS to enter details of fire alarms, false alarms and completion of alarm and Incident reports. The following fire alarm related data is entered by AFASPs:

Data Field
Building name
Building town / city
Building suburb
Building street name
Building street number
Building daytime contact phone number
Building daytime contact designation
Building owner name
Building owner town / city
Building owner suburb
Building owner street
Building owner street number
Building Owner PO Box
Building owner contact phone number
Building owner representative name
Building owner representative town / city
Building owner representative suburb
Building owner representative street
Building owner representative street number
Building Owner Representative PO Box
Building owner representative contact phone number
Fire alarm area ID (PFA number)
Fire alarm manufacturer / make / model
Fire alarm manufacturer type number or panel DBA
Fire alarm FENZ letter of approval date
Fire alarm certifier name
Fire alarm certification number
Fire alarm system type
Fire alarm connection type
Fire alarm service area
Fire alarm location descriptor
Fire alarm date of last test

Data Field
Fire alarm date of last survey
Fire alarm owner name
Fire alarm owner town / city
Fire alarm owner suburb
Fire alarm owner street
Fire alarm owner street number
Fire alarm owner PO Box
Fire alarm owner contact phone number
Fire alarm service agent company name
Fire alarm service agent contact phone number
Key holder name (up to 5 key holders)
Key holder contact phone number (up to 2 contact phone numbers for each key holder)
Key holder contact phone number remark
Contractor Data 1
Contractor Data 2

Subsets of the above data are regularly transferred to CAD and FENZ Standard Operating Procedures (SOP) software to support commissioning of fire alarms and locate/verify functions in the Communications Centres. Following connection of a fire alarm to the AFAS, the AFASP must also provide the following fire alarm related data to FENZ:

Data Field
Connection Date
Disconnection Date

For SMS procedures and documentation, refer to the AFAS System Owner.

9.4.1.1 FALSE ALARM RELATED DATA

Each AFASP must input the following False Alarm related data into the Station Management System within 2 working days to complete the incident report. This supports identification of False Alarms, and subsequent cost recovery actions by FENZ.

Data Field
False Alarm cause classification
False Alarm cause description

9.4.2 ENTERPRISE GIS (EGIS) AND SMART APPLICATIONS (SMART MAP, SMART CHANGE)

The FENZ enterprise Geographic Information System (eGIS) and SMART Applications supports fire alarm asset location information. AFASPs access SMART to enter details of (Private) Fire Alarms (PFA), Common Place Names (CPN) and other ancillary location data to verify and associate fire alarms. Data entered into SMART is regularly transferred to CAD to support Commissioning of fire alarms and locate/verify functions in the Communications Centres.

For SMART procedures and documentation, refer to the AFAS System Owner.

9.4.3 FMIS

Fire Alarm and False Alarm related Data is replicated to the FENZ Financial Management Information System (FMIS) to support the AFAS cost recovery model, including fire alarm Connection Fees and other ancillary cost recoveries.

For FMIS procedures and documentation refer to the Financial Controller or Funding and Procurement Manager, FENZ National Headquarters.

9.4.4 ROLES AND RESPONSIBILITIES

Role	Responsibility
FENZ SMS and Business Planning Manager	SMS Business Owner

Role	Responsibility
FENZ Team Leader Spatial Intelligence	SMART Applications System Owner
FENZ Manager Revenue and Assurance	FMIS – AFAS cost recovery model
FENZ Financial Controller	FMIS Business Owner

9.4.5 DEMARCATIONS

Demarcation Point	Component	Responsibility
FENZ STSMHS Domain	FENZ Firewall	FENZ
	FENZ Firewall Network Connection	Unisys
NZ Police Domain	CAD	NZ Police
	CAD Transfer Server	FENZ
FENZ Domain	FENZ Firewall	FENZ
	FENZ Firewall Network Connection	Unisys
	SMS Web Interface	FENZ
	SMART Web Interface	FENZ
	FMIS Web Interface	FENZ

9.4.6 SUPPORTING DOCUMENTS, POLICIES, PROCEDURES, STANDARDS

Refer to:

- FENZ Station Management System support strategy
- SMART Applications support strategy
- FENZ National Procedure PMPP03 - Data Management of Common Place Names
- FENZ National Procedure PMPP07 - Commissioning Private Fire Alarms
- FENZ National Procedure - G1-2 Private fire alarms (NCI 24)
- FENZ National Procedure - Specialist Knowledge Private Fire Alarms (G1-2)
- FENZ False Alarm Best Practice Guide
- AFASP Fire Alarm Data Management in SMS guide
- FENZ AFASP STSMHS Certification Test Scripts Part 2 guide

9.5 NZ POLICE DOMAIN

9.5.1 AIS

The AFAS Alarm Interface Server (AIS) is deployed in the NZ Police Domain and acts as proxy for the STSMHS network connection and firewalls into the FENZ Comcen environment and CAD in all 3 Communications Centres.

For AIS Support, refer to the SITE Agreement, NZ Police ICT group and Hexagon.

9.5.2 CARD AND CAD

The NZ Police and FENZ Communications And Resource Deployment (CARD) environment is governed by NZ Police and FENZ through the Shared Information Technology Environment Agreement. Change Management for CARD is governed through the NZP/FENZ Joint Operations Group (JOG).
The Computer Aided Dispatch (CAD) system is governed by NZ Police and FENZ through the Shared Information Technology Environment Agreement. Change Management for CAD is governed through the NZP/FENZ Joint Operations Group (JOG).
The Master CAD infrastructure resides in the Revera Auckland Data Centre with supporting virtual CAD infrastructure located in the Revera Wellington Data Centre. CAD is provisioned into all 3 NZP/FENZ Communications Centres in the virtualised CARD environment, and is supported by NZ Police ICT group and Hexagon.

For CAD system architecture, procedures and documentation and support, refer to the SITE Agreement, NZ Police ICT group and Hexagon.

9.5.2.1 CAD AFAS FIRE ALARM DATA MANAGEMENT

CAD receives all AFAS/STSMHS fire alarm messages and locates and verifies the location of the fire alarm to support FENZ response.

The SITE Agreement describes the Operational, mapping and location data used in the Comcens environment to locate/verify fire alarm activations, and respond to emergency and non-emergency events. Data to support locate/verify functions in CAD is sourced from a variety of providers including Corelogic, NZ Post, Hexagon, NZ Transport Agency, Department of Conservation, Land Information NZ, FENZ, NZ Police, Central and Local Government.

There is a regular maintenance regime for this data, which is tested before deploying into the live environment. Urgent data updates are completed in all environments as necessary under the NZ Police/FENZ Data Change Policy.

This data is available in a number of environments including CAD, InterCAD, STSMHS, NZ Police and FENZ specific applications.

FENZ CAD Operational Data related to the AFAS and supporting commissioning of fire alarms includes the following and is supported and maintained by FENZ ICT directorate:

Data Set	Provided by	Update Frequency	Responsibility
Common Place Name (CPN)	FENZ	FENZ provides data updates as scheduled on the mapping update plan, but on average every three weeks.	FENZ is the steward for this data and manages and maintains the data, with appropriate maintenance fees charged, on behalf of FENZ, Police and Ambulance. The data contains sensitive and secure data that is not available for release into the Public Domain.
FENZ Alarm, pager, call-sign, deployment data.	FENZ	Requirement to frequently update.	FENZ operational data. Agreed update process outlined in the FENZ Priority Update Policy which is reviewed and updated annually by all parties.
Private Fire Alarm (PFA) data	FENZ	Required to update frequently	FENZ operational data. Automatic Fire Alarm Service Providers maintain data in FENZ SMS. PFA details updated in CAD either with CPNs or via the FENZ Priority Update Policy. This data may contain Fire Alarm built environment owner data, keyholder information and other ancillary access information.

SUPPORT QUALIFICATION: Other AFASP, building owner and fire alarm data supporting fire alarm locate/verify functions in CAD are described in Section 8.4: FENZ Domain.

9.5.3 CUSTOMER ALARM TERMINAL

A STSMHS Customer Alarm Terminal (CAT) has been provisioned into each FENZ Communications Centre as a separate computer terminal to the main CAD terminals. The CAT terminal and software provides an independent portal for viewing fire alarm messages that have been sent from the AFAS and STSMHS to the AIS.

SUPPORT QUALIFICATION: For CAT Terminal support, refer to the STSMHS Master Services Agreement.

9.5.3.1 FUNCTIONS OF THE CAT TERMINAL

- Fire alarm messages sent from the AFAS to the AIS are independently sent to the CAT Terminal for the Communications Centre Communicator.
- Details of the physical fire alarm such as building name, building address are displayed.
- Key holder details are displayed by clicking on the row of interest.
- Once started the CAT terminal will automatically maintain a connection with the STSMHS servers. The table below describes the data displayed on the screen.

Field / Button Name	Description
STSMHS Connected	Shows the status of the connection between the STSMHS and the CAT terminal.
Primary Connected	Shows the status of the Primary AIS/CAD server.
Secondary Connected	Shows the Status of the Secondary AIS/CAD server.

Evacuate Comcen	When button is pressed, STSMHS will not route any traffic to the Comcen. See section 7.3.3 for more details on this function.
Date	Date that the fire event was received.
Time	Time that the fire event was received.
FAID	The unique fire alarm Identification Number as assigned by FENZ.
Com	The communications centre that the alarm has been routed to.
Address	Displays the building name, address, Service Agent and AFASP name information. *Note to display the key holder information of an Alarm simply click on the alarm row of interest.
Status	Displays the current state of the record this can take the following value: New — New Fire has been received but is not acknowledged. Accept — Fire has been accepted by CAD. Archive — Old record fetched from local store displayed when CAT is restarted if old records exist.

9.5.4 ROLES AND RESPONSIBILITIES

Role	Responsibility
STSMHS Systems Architect (Unisys)	CAT Terminal STSMHS Domain
FENZ Communications Centre Manager	Centralcoms CARD/CAD
FENZ Communications Centre Manager	Northcoms CARD/CAD
FENZ Communications Centre Manager	Southcoms CARD/CAD
FENZ ICT Architect	AFAS System Owner
NZP Communications Centres National Manager	CARD/CAD
NZP Service Delivery Manager	CARD/CAD
NZ Police Network Administrator	CARD/CAD Networks
CAD Technical Support	CAD

9.5.5 DEMARCATIONS

Demarcation Point	Component	Responsibility
STSMHS Domain	FENZ Firewall	Unisys
	FENZ Firewall Network Connection	Unisys
NZ Police Domain	Northcom FENZ Firewall	FENZ
	Centralcom FENZ Firewall	FENZ
	Southcom FENZ Firewall	FENZ
	Northcom AIS	NZ Police
	Centralcom AIS	NZ Police
	Southcom AIS	NZ Police
	Revera Auckland Data Centre	NZ Police
	Revera Wellington Data Centre	NZ Police
	Northcom CAT Terminal	Unisys
	Centralcom CAT Terminal	Unisys
	Southcom CAT Terminal	Unisys

9.5.6 SUPPORTING DOCUMENTS, POLICIES, PROCEDURES, STANDARDS

Refer to:

- SITE Agreement
- FENZ Data Change Policy
- STSMHS Master Services Agreement

10 AFAS PROCESSES, POLICIES, PROCEDURES AND STANDARDS

This section sets out the processes, policies, procedures and standards for the AFAS and for certified AFASPs. AFASP operations must meet the requirements set out in previous sections and comply with the policies, practices and standards set out in this section.

10.1 AVAILABILITY AND PERFORMANCE STANDARDS FOR AFASP SYSTEMS AND FACILITIES

AFASP monitoring and communications systems and processes must comply with the following availability and performance standards:

1. There must be no single point of failure in the pathway between the AFASP communications gateway/concentrator and FENZ STSMHS domain
2. All services must be provided by way of redundant sites and facilities located far apart enough to avoid the possibility that a single event or series of events will disable both facilities
3. Fail over or fall back from the primary transmission route/facility to any backup must occur automatically without the need for manual intervention and without loss of in-transit messages
4. Fail over or fall back must result in the delivery of messages within the times specified in the performance standards set out below
5. The AFASP communications gateway/concentrator facilities must support device-initiated selection of, and fall back to, an available gateway address/port by the remote (FA) device using a list of available addresses/ports maintained on the device
6. Failure of any section of the telecommunications link between the fire alarm and FENZ STSMHS must not cause a message indicating a fire-event
7. The telecommunications link between a fire alarm and the FENZ STSMHS Domain must comply with the following standards at all times:
    a. A signal from a fire alarm must travel to the FENZ STSMHS domain in no more than:
        i. 10 seconds for 97% of all messages; and
        ii. 15 seconds for all messages
    b. The telecommunications link between a fire alarm and the FENZ STSMHS domain must be available for 99.7% in any period of 12 months
    c. In calculating the availability of the link in 7b, the following formula is to be used:
        i. Total Minutes (b) = Total Number of minutes in the 12 months up to and including Month X
        ii. Down-Time (c) = Total number of minutes of downtime in the 12 months up to and including Month X
        iii. For the 11 months before the connection of a fire alarm to the AFAS the monthly availability is deemed to be 100%
        iv. For each month X, the following formula is used to calculate and chart the availability: Availability % (a) = 100 times (b – c) / b.
    d. The AFASP must demonstrate to, and have approved by, FENZ how the Down-Time (item (c) in the availability formula above) of any link between a fire alarm and FENZ STSMHS Domain is determined.
    e. No more than one in 1,000,000 messages received by FENZ STSMHS domain from the AFASP Domain system are to be unintelligible;
    f. The single failure maximum outage time for the telecommunications link between the fire alarm and FENZ STSMHS domain is 6 hours; and
    g. The disruption of the telecommunications link between the fire alarm and FENZ STSMHS domain must be detected in less than 10 minutes.
8. The following exclusions are to be taken into account for calculating the availability of the link between the fire alarm and the FENZ STSMHS domain:
    a. Force Majeure
    b. Faults that have been carried over to the next day with agreement of FENZ will have the corresponding delay subtracted from the outage time
    c. Where access to end-user sites is not available, the corresponding delay will be subtracted from the outage time
    d. Faults that are caused by the end-user, and
    e. Faults that are caused by FA Service Agents servicing the fire alarms.

10.2 FIRE ALARM INSTALLATION AND CONNECTION STANDARDS

10.2.1 INSTALLATION OF AUTOMATIC FIRE ALARM (AFA) DEVICES AND SYSTEMS

Equipment and installations of equipment to be connected to the AFAS must meet the following standards:

1. All equipment connected to the AFAS must meet the following requirements:
    a. Complies with the requirements set out in New Zealand Standard NZS 4512:2010: Fire detection and alarm systems in buildings, or later versions as may be published from time to time
    b. Complies with AS/NZS CISPR 22:2004 (for radiated and conducted emissions) and respectively the new compliance requirements (RCM and R-NZ) issued by the Ministry of Business, Innovation and Employment (MBIE – Radio Spectrum Management). The RCM consolidated the three previous marks (C –tick, RCM and A – tick (Australia). The R-NZ is a New Zealand only radio label for radio products not harmonised with Australia; and
    c. Has an energy supply compliant with NZS 4512:2010 and NZS 3100:2017.
2. Fire Alarm (FA) units installed for connection to the AFAS must have declared functional requirements per Section 105 (a), (b), (g) and (h) of NZS 4512:2010.

10.2.2 CONNECTION AND DISCONNECTION OF FIRE ALARM DEVICES AND SYSTEMS

10.2.2.1 CONNECTIONS TO AFAS

1. FENZ will authorise connection of only certified fire alarm equipment to the AFAS. At its sole discretion, FENZ may authorise connection of non-certified equipment where circumstances warrant. Such authorisation must be obtained in writing from the FENZ.
2. FENZ will authorise connection of fire alarm equipment to the AFAS only where the equipment is installed, maintained and tested by a suitably qualified person who is registered as an independently qualified person with the appropriate Local Building Consent Authority or Territorial Local Authority.
3. The AFASP must ensure that all equipment connected to the AFAS is authorised by FENZ and:
    a. is installed, maintained and tested by a suitably qualified person as set out above
    b. is certified to the standards prescribed by the version of NZS 4512 that is current at the time of installation
    c. has had a current annual survey and has up-to-date monthly test records if the alarm was previously installed and in use whether previously connected to the AFAS or not
    d. has passed the tests as described in Section 9.3: Fire Alarm Commissioning Process
    e. has a device connecting the fire alarm to the telecommunications network that:
        i. complies with AS/NZS CISPR 22:2004 (for radiated and conducted emissions) and respectively the new compliance requirements (RCM and R-NZ) issued by the Ministry of Business, Innovation and Employment (MBIE – Radio Spectrum Management). The RCM consolidated the three previous marks (C –tick, RCM and A – tick (Australia). The R-NZ is a New Zealand only radio label for radio products not harmonised with Australia; and
        ii. has an energy supply compliant with NZS 4512:2010 and NZS 3100:2017
4. Before the equipment is installed, the AFASP must provide FENZ with:
    a. data as per Section 9.3: Fire Alarm Commissioning Process , and
    b. the contact details of a contact person to arrange building inspection for the purpose of preparing operational plans, including access in the event of fire calls.

10.2.2.2 DISCONNECTIONS FROM AFAS

1. The AFASP will, on instruction from FENZ, disconnect a fire alarm from the AFAS.
2. The AFASP may, with agreement from FENZ, disconnect a fire alarm from the AFAS for:
    a. non-payment of service fees
    b. a breach of the Certificate of Compliance
    c. failure to comply with relevant NZ Standards for more than 6 months
    d. failure to comply with requirements set out in the agreement between the AFASP and the fire alarm owner
    e. occurrences of false alarm incidents whose number exceeds the maximum permissible number of false alarm incidents within any 12-month period as set and revised from time to time by the FENZ.

3. Provided FENZ approval has been given to disconnect a fire alarm, the AFASP must issue to the customer a 10 days final notice, in writing, of the impending authorised disconnection.
4. The FA Service Agent or AFASP performing the disconnection and/or removal of a fire alarm must ensure that all disconnection actions meet the requirements of Part 7 of NZS 4512:2010 including the notification requirements in Section 702.
5. The Service Agent or AFASP performing the disconnection must obtain a signed notification form signed by the owner of the premises or their authorised agent before the service is disconnected.
6. On disconnection, a notice similar in form to that in Figure K2 of NZS 4512:2010 must be affixed to the outside of the main control or indication panel as specified.

10.3 FIRE ALARM COMMISSIONING

As described in the summary business processes below, the FENZ AFAS Fire Alarm System Commissioning process is logically separated into four Phases:

1. Phase 1 – Initiation: Phase 1 describes three stages of initiating a fire alarm connection to the AFAS:
    a. Stage 1 is the Design stage completed by the building owner, territorial local authority and the FENZ fire engineering/design review unit. Prescribed Firefighting Facilities Process is completed by AFAS system actors with initial fire alarm system designs assessed for compliance
    b. Stage 2 is the Building Consent Process, completed by the building owner and assessed by the local building consent authority
    c. Stage 3 is the Building Construction and Fire Alarm Installation stage, and includes the Fire Alarm System Assessment Process completed by the building owner, fire alarm service agent, AFASP and FENZ fire engineering/design review unit.

    From successful completion of Phase 1 Built Environment stages and processes, installed and certified Fire Alarm Systems then enter Phase 2 to connect and commission fire alarms into service.
2. Phase 2 – Fire Alarm System Data: Phase 2 describes the process for creation of supporting Fire Alarm System data required by to be entered into the FENZ Domain system by AFASPs and FA Service Agents in order to initialise and connect fire alarms to the AFAS. Fire Alarm System Data is specified in section 8.4 (FENZ Domain) of this CoP. From successful completion, loading and validation of required Fire Alarm System data, the commissioning process then move to Phase 3 to deploy and authorise fire alarm connection to the AFAS.
3. Phase 3 – Deploy and Authorise: Phase 3 describes the Alarm Signalling Equipment (ASE) installation and connection completed by the AFASP and FA Service Agent in the built environment, along with the required extract/transform/load (ETL) fire alarm data process between FENZ and Police domains, required to initialise the FENZ Communications Centres computer-aided dispatch (CAD) systems in preparation for Phase 4 testing and commissioning of fire alarms.
4. Phase 4 - Test and Commission: Phase 4 is completed collaboratively between various AFAS system actors to test the new fire alarm connection and commission the fire alarm into service. The tests described below must be passed before the Contractor connects a Fire Alarm to the AFAS. These tests are in addition to any tests mandated by the relevant standards for a Certificate of Completion. The test procedure is that:
    a. The Service Agent contacts the Contractor to request a time to conduct a commissioning test.
    b. The Contractor requests an available time from the relevant Communications Centre to conduct the test, and informs the Service Agent.
    c. The Contractor establishes a conference call between the Contractor, the Service Agent and the Communications Centre.
    d. The Service Agent originates a message from the fire panel indicating a live fire event from the Fire Alarm to the Contractor and FENZ.
    e. Communications Centre staff inform the Contractor whether the Communications Centre staff received a message indicating a fire event from the Fire Alarm.
    f. The Contractor informs the Service Agent whether both FENZ and the Contractor received a message indicating a fire event from the Fire Alarm.
    g. The Service Agent verifies to the Contractor whether the Service Agent received a page message indicating a fire event from the Fire Alarm.

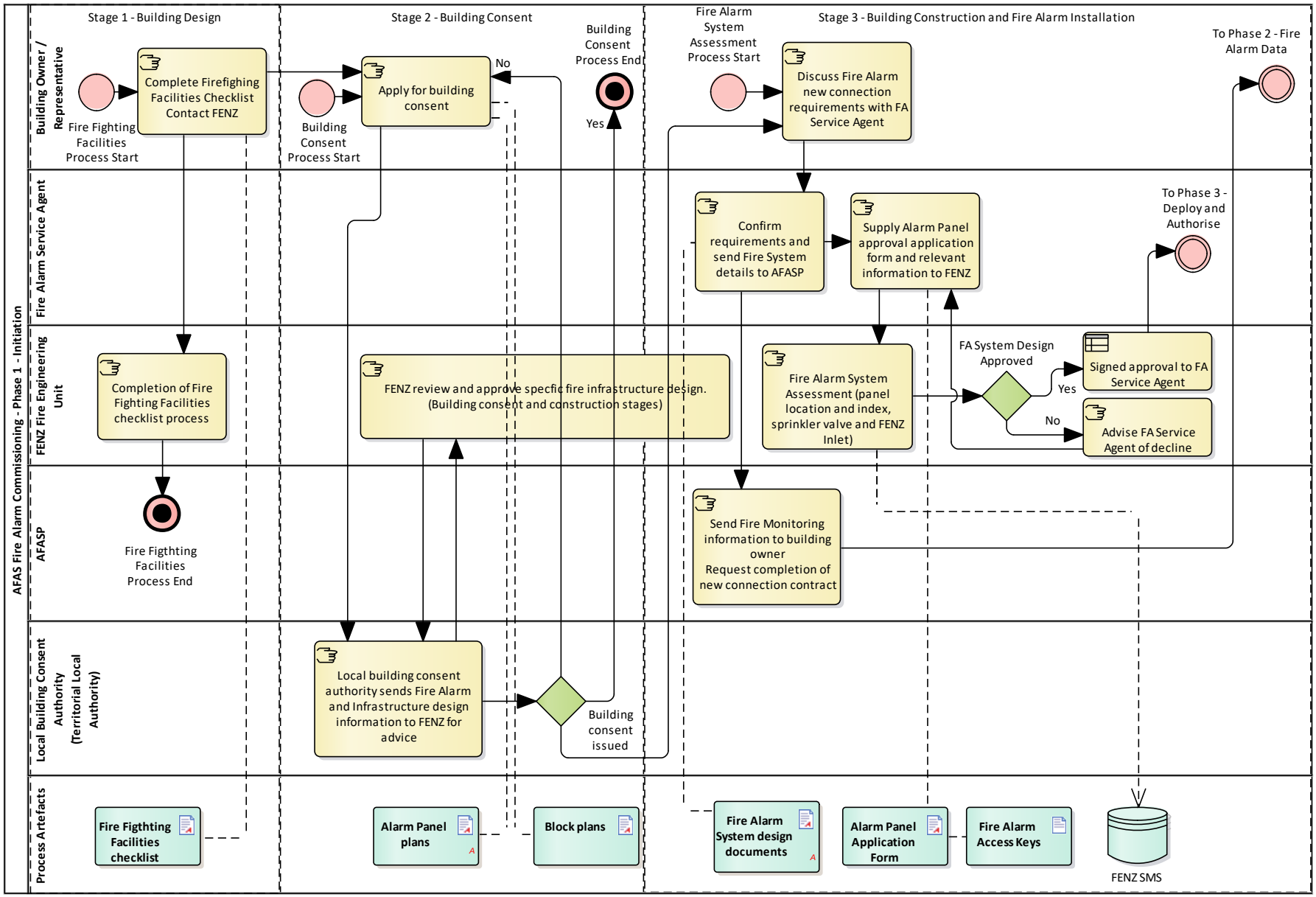
h. The Contractor will provide to the Service Agent a copy of the Fire Alarm history report showing evidence of the live fire event used in the commissioning test, including date and time when that fire event message was sent to FENZ and acknowledged by FENZ.

The test will be regarded as being passed if the Contractor, the Service Agent and FENZ each received all messages outlined above.

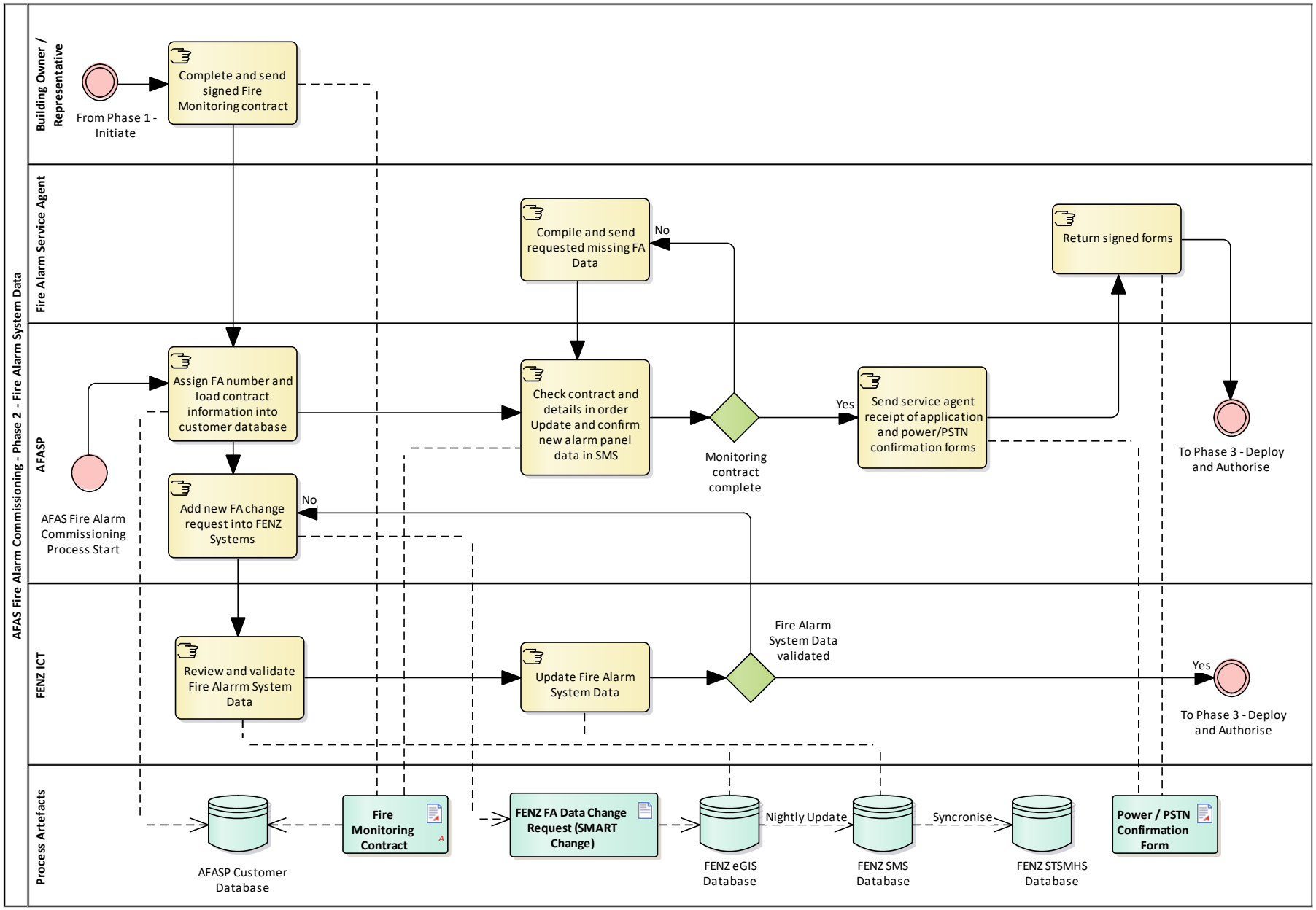
The Contractor must record the test results and forward them to FENZ in accordance with FENZ processes as advised from time to time.

Detailed descriptions of the AFAS fire alarm commissioning process are available on request from FENZ.

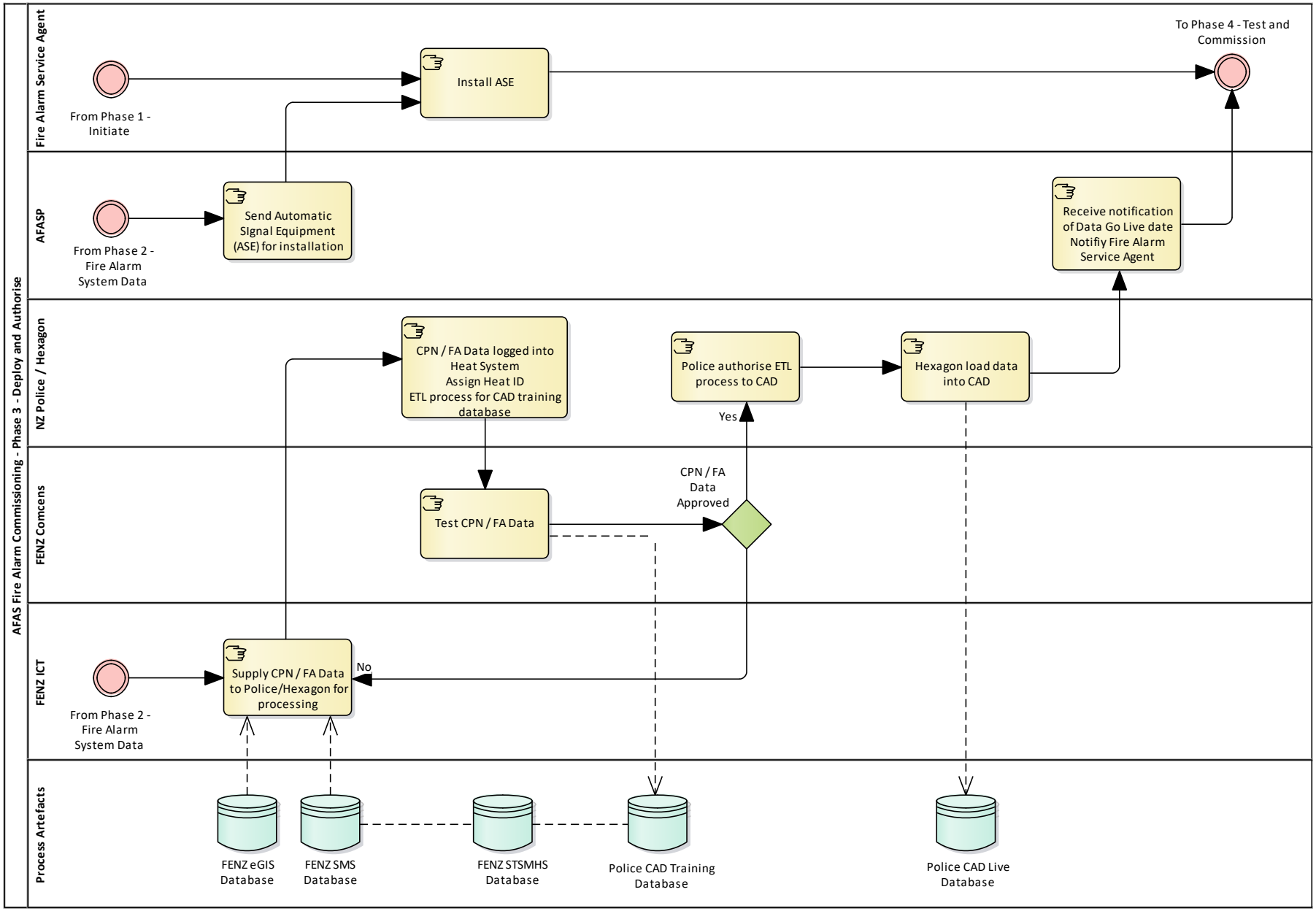
10.3.1 PHASE 1 – INITIATION



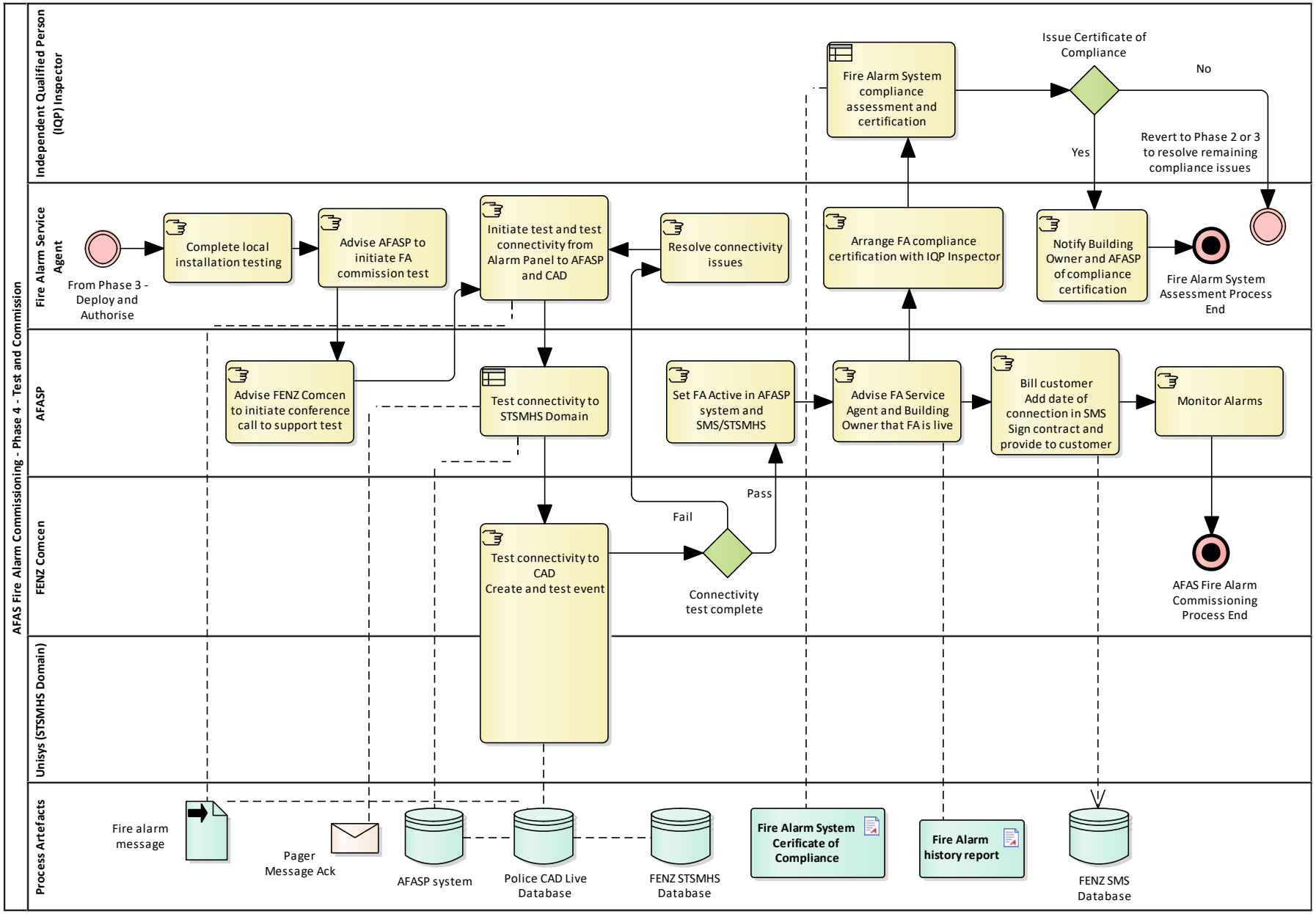
10.3.2 PHASE 2 – FIRE ALARM SYSTEM DATA



10.3.3 PHASE 3 – DEPLOY AND AUTHORISE



10.3.4 PHASE 4 – TEST AND COMMISSION



10.4 FIRE ALARM MESSAGE HANDLING

10.4.1 ALARM PANEL/NETWORK INTERFACE OPERATION

A typical sensor installation consists of sensor units connected by way of a signal bus (generally an RS-485 bus) to an alarm panel/concentrator unit. The panel periodically pools the attached sensor devices for state. The devices respond with the current state of their (usually four) indicators. When the state of the indicators changes, the alarm panel formats a message to be transmitted to the monitoring service concentrator. The message generally consists of a set of ASCII characters which provide information concerning the identifier or number of the fire alarm associated with the sensor and the state of the sensor indicators.

The interface between the panel, concentrator unit and the network is provided by a network interface device called variously an ASE (Alarm Signalling Equipment), a CTU (Communicating Terminal Unit) or a NAD (Network Access Device). Each AFASP provides and maintains a service-specific unit designed to inter-operate with its monitoring equipment.

In normal operation, the network interface unit periodically polls the communications port at the monitoring centre. If the poll fails (the monitoring centre concentrator does not respond), the device will select the next port/address in its internal list and attempt connection using that port. Note that for our purposes, ports are hardware connections (e.g. an Ethernet network port or an RS-232 port with attached modem or dialler-modem) rather than TCP-oriented software ports.[6]

The network interface device will cycle through its list of connection ports/protocols until it gets a response. If the device has become isolated, i.e. none of the ports respond, the device will continue to cycle through its list of ports/addresses until connection is successful or the device is manually reset.

It is critical to the correct operation of the system that the network interface device selects the mode/address for connection and that each of the multiple connection addresses connect to different concentrator gateways at the monitoring centre or backup site.

The connection protocol sets the following implied ‘contract’ between the device and the gateway:

> *When a gateway makes a positive response (ACK) to a poll or to a message transmission it is guaranteeing that it has an operational pathway to the MHS device or alternatively that none of the port/addresses in the Network Interface Device connection list has an operational connection to the MHS, but that this gateway has an operational connection to a responsive monitoring centre console to allow it to pass the message for manual handling.*

If the gateway is unable to fulfil this contract, it must make a negative acknowledgement (NAK) even if its internal operation is intact and functioning normally. In simpler terms, a gateway must not accept a message it cannot guarantee it will be successfully delivered to the STSMHS within the interval allowed by the performance standard (currently 15 seconds). It may, however, accept and handle a message if there is no other gateway able to directly forward the message within the specified time interval and if it has a working connection to a responsive operator workstation which will deliver the signal message to the operator within the specified timeframe to allow manual handling of the event.

If these standards are not met, messages may be isolated or ‘black holed’ and never delivered to the responder. The alarm network interface unit device will cease trying to forward the message, believing it to have been successfully processed.

10.4.2 AFASP MONITORING SYSTEM OPERATION

The AFASP monitoring system performs three key operations:

1. It accepts incoming signals from the FIRE ALARM units, reformats them into a standardised form and forwards the messages, including alarm messages, to FENZ by way of the STSMHS.
2. For signals that reflect fault or alarm status, it forwards notification and dispatch information to the appropriate Service Agent.
3. It monitors the delivery of fire alarm messages and, if a message is not successfully delivered to the intended

[6] Note that the address will be a selector appropriate for the port type e.g. an IP/Port address for an Ethernet port, a telephone number for a dialler unit, etc.

recipient, it alerts the recipient (FENZ Comcen and/or the Service Agent) by way of a manual contact procedure.

In addition, the AFASP provides customer and equipment management services including management of service contracts, registration of AFAs, sites and key contacts, and bills customers for fire alarm services. For more information, see Section 9.5: AFASP Premises, Computer and Telecommunications Facilities Standards.

10.4.3 STSMHS AND FENZ OPERATIONS

The STSMHS system is a message handling gateway which accepts incoming messages from the AFASPs and forwards them on to the appropriate destinations within FENZ and the Communications Centres.

The STSMHS provides guaranteed delivery to all required recipients for messages which it accepts and acknowledges.

10.4.4 MESSAGE FLOW

A fire alarm sends messages (signals) indicating events detected by the fire alarm units. These event signals represent changes in the state of the fire alarm. These changes may include the detection of fire conditions (fire alarms) and/or detection of faults within the fire alarm units.

Messages are transmitted to the AFASP communications gateway/concentrator which translates the messages into a standard format for handling by the AFAS and forwards them automatically to FENZ by way of the STSMHS. The AFASP also sends dispatch notices to or dispatches the Service Agent responsible for maintenance and servicing of the affected alarm equipment.

The signal path between the fire alarm and the STSMHS, and also between the STSMHS and the FENZ's dispatching system, is an electronic path that does not require human intervention.

Messages to FENZ are transmitted electronically via the Service Provider Interface of the STSMHS. These messages must conform to the AFASPCIS. The technical interface between the AFASP internal programming and the NFS Communications Interface must conform to the STSMHS - AFASP Application Programming Interface Design Specification, which is available on request from the FENZ.

Messages between the fire alarm units and the AFASP are sent in a semi-standard format with possible proprietary extensions/elements specific to the type of equipment installed on site. The AFASP is responsible for ensuring that the connection interface (electrical and logical) and the protocol standards for these connections are clearly and completely specified in available documentation and that connected units conform to these specifications.

FENZ does not currently set a specification for the structure and format of these messages, but does set requirements for the reliability and performance of the communications link(s) used to transmit signals from the fire alarm units to the AFASP communications gateway/concentrator. In addition, FENZ maintains a list of commercial networks and network providers which have been tested and determined to comply with these standards.

All messages received from the fire alarm units are transformed and formatted to comply with FENZ Protocol Standard and forwarded by the AFASP to FENZ by way of the STSMHS. The STSMHS then routes these messages to appropriate destinations within FENZ including FENZ Communications Centres and various databases maintained by FENZ.

FENZ databases maintain information concerning the type and location of the fire alarm units as well as the parties responsible for the fire alarm and for providing service and maintenance of the fire alarm. FENZ databases also include information about the performance of fire alarm installations including information about faults and false alarms. The underlying database information is maintained by FENZ staff and external parties.

From a systems standpoint, Communications Centre staff initiate and manage response actions appropriate to the messages indicating fire events. For fire events, supplementary data related to the fire alarm unit – historical performance, past non-normal events, false alarms, other fire alarm-related data, is also forwarded to the Communications Centres by the STSMHS.

Using the same communications links, FENZ may also query the Service Provider for fire alarm-related data, as specified in the AFASPCIS. Examples of this include FA-mode and FA-status ('Site FA Mode Summary' and 'Site FA Status Summary', as specified in the AFASPCIS), and date/time of the last FA-mode and FA-status changes.

Note that because of operational constraints built in to many fire alarm devices, the information to respond to these queries will be returned by the AFASP from its database of the current state of the devices rather than directly from the device itself. Depending on the timing, this information will reflect the last response to the connect poll from the

device to the AFASP gateway or the last information transmitted by the device in response to an event. In either case, the response will reflect the latest available information from the device.

10.4.5 FUNCTIONAL OPERATION

For reliability and performance, the computer traffic between FENZ and the AFASP must be delivered on at least two independent communications links with the signals carried via independent telecommunications services and infrastructure.

10.4.5.1 TRANSPORT

The connections between the AFASP and the STSMHS must be by way of an approved, fully redundant, links utilising Internet Protocol (IP); the links may be dedicated point-to-point links carrying IP traffic or they may be approved IP-based Virtual Private Network (VPN) connections. On shared transport, a VPN connection between the AFASP and the STSMHS must be used to ensure that there is no unauthorised access to the monitoring network or the traffic across the network.

FENZ requires that all AFASPs will keep this IP network physically and logically separate from all other internal networks, including networks for monitoring other devices. The only links permitted between this IP network and the AFASP's internal networks is to be the AFASP's dedicated communications gateway/concentrator servers.

10.4.5.2 NETWORK PROTOCOL

At both the STSMHS and AFASP end-points, the link must accept connectionless Universal Datagram Protocol (UDP) broadcasts on a single-fixed UDP port, and transmit those broadcasts to servers at the remote connection point. It is permissible to convert broadcasts to messages that are forwarded to specific server IP addresses, but it is preferable to maintain connectionless (and thus address-less) broadcasting, as this ensures that changes in IP addresses or number of servers at either end will not impact router or VPN configuration.

Each AFASP is assigned a unique UDP port number for data transmission. Messages containing that UDP port number are transported across the link. STSMHS operations staff ensure this port number is registered at the STSMHS and in the configuration of the AFASP API module that is supplied to the AFASP. It is the responsibility of the AFASP to ensure that this UDP port number is configured in the VPN or router. No other network protocols or TCP/IP ports are to be allowed across the connection.

10.4.5.3 MESSAGES AND SESSION CONTROL

The application data is communicated using three distinct and separately implemented protocols. Details on each of these are specified in FENZ 'STSMHS - AFASP Application Programming Interface Design Specification', which is available on request from the FENZ. All message-handling and monitoring applications must comply with this specification.

10.4.5.4 AFASP COMMUNICATIONS AND MONITORING CENTRES

Each AFASP must maintain at least two physically and logically separate sites to provide fully-redundant computing and communications infrastructure.

The facilities should be in separate locations with sufficient separation to ensure that an event or series of events in one location is unlikely to interfere with the operation of both facilities.

Facilities must meet the relevant portions of AS/NZS 2201.2-2004: Intruder alarm systems – Monitoring centres, for a Level C, Grade 2 monitoring centre.

These should relate to building construction, access control, fire protection, backup power, etc. Elements of the standard regarding premises ownership and the details of internal monitoring systems, staffing and operation should be excluded as they are set out in the Certification Requirements for AFASPs and related documents.

To ensure there is no single point of failure in the FENZ/AFASP communication system, at least two hosts are required at each AFASP, with at least two connections from each host to two distinct FENZ STSMHS servers. The communications paths must connect over at least two physically and logically separate networks.

The following diagram illustrates this implementation architecture and is used to illustrate how the protocols are implemented over diverse communications links. Considerations such as geographic separation between sites will determine the actual configuration and implementation at each AFASP.

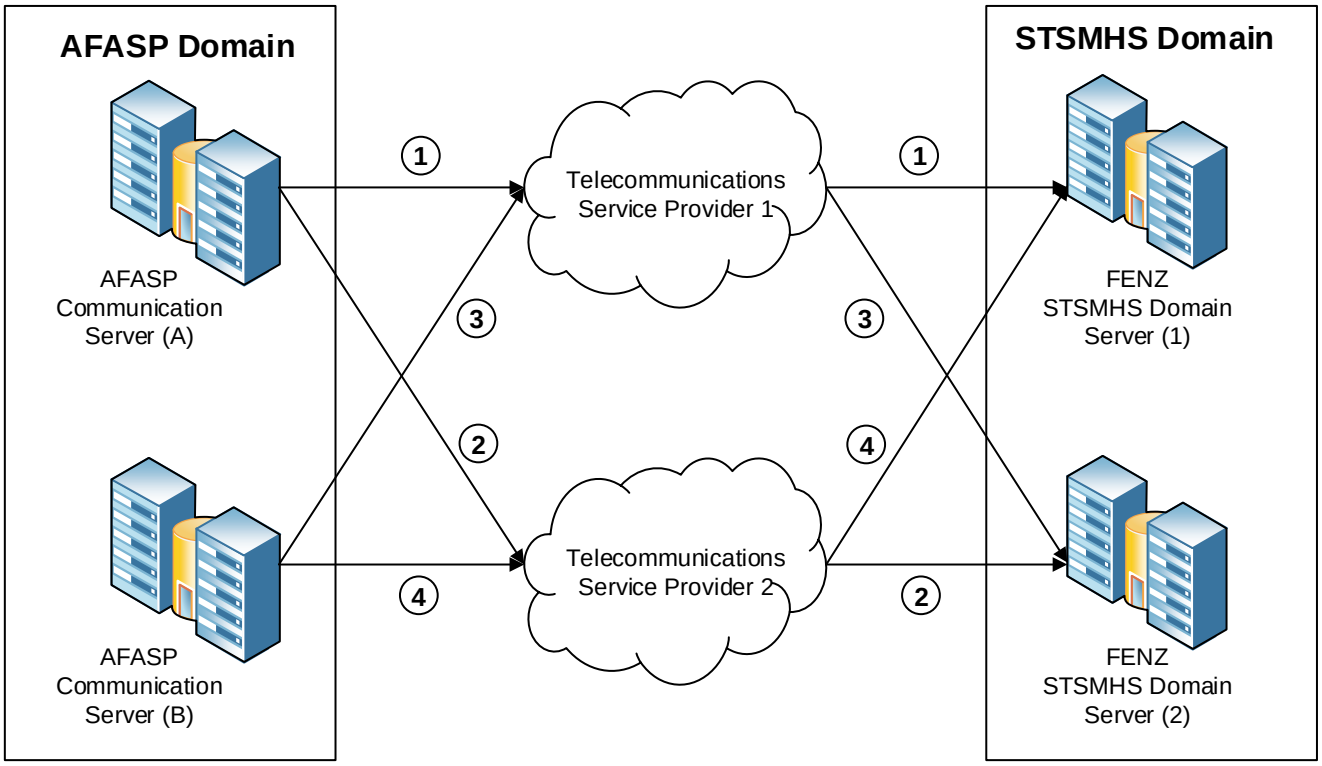


Figure 2: Communication paths for single AFASP implementation

Figure 2 illustrates the communication paths required for a single AFASP implementation. Each of the AFASP communication servers and FENZ MHS Servers is connected via two links to the other servers. Each link utilises FENZ AFASP protocol and connection interface.

10.5 AFASP PREMISES, COMPUTER AND TELECOMMUNICATIONS FACILITIES STANDARDS

10.5.1 PREMISES AND FACILITIES

1. AFASP facilities must comply with the applicable sections of the Australian Standard AS 2201.2-2004: Intruder Alarm Systems, Part 2: Monitoring Centres, with respect to building services, construction, facilities and equipment. Building services and construction must meet the requirements of Grade C; and all facilities and equipment must meet the requirements of Grade 2.
2. The Service Provider must provide suitable evidence that their facilities and equipment meet these requirements.

10.5.2 SYSTEMS AND OPERATIONS

AFASP systems to monitor fire alarms must:

1. be technically robust and be able to transmit fire alarm signals from fire alarms to FENZ Communication Centres rapidly, reliably and unambiguously in compliance with the standards as set out in this section
2. provide for new fire alarms to connect in a straightforward manner, no matter where they are in the country
3. provide for all connected fire alarms to be monitored and Service Agents notified of non-normal events
4. promote reduced incidence of false alarms from connected fire alarms
5. not constrain the type or nature of information available to FENZ from installed fire alarm devices provided that such information is available from the devices.

10.5.3 ALARM SIGNAL HANDLING AND MONITORING SYSTEMS

AFASPs must provide, maintain and operate all equipment and software required to provide the automatic fire alarm management and transmission services for fire alarms in accordance with the performance standards described in this section and in accordance with the representations set out in its application for certification or re-certification and associated documentation.

1. In maintaining the equipment or software the AFASP must not do anything which alters FENZ STSMHS Domain or interferes with or affects its operation.

2. The AFASP must protect the AFASP's equipment and software, and the connected FENZ STSMHS Domain from unauthorised access and viruses.
3. The AFASP must carry out connections, disconnections and changes related to fire alarms in accordance with FENZ processes as advised in writing from time to time.
4. The AFASP must provide computer and telecommunications facilities to enable data and information to be passed between FENZ and the AFASP's premises as required at no cost to FENZ. The AFASP must obtain approval and certification from FENZ for the computer and telecommunications facilities to be provided under this clause.
5. The AFASP must notify the FENZ, in advance, of any planned changes to its computer and telecommunications facilities and obtain prior written approval of FENZ for any changes. The AFASP must provide plans and other documentation necessary for FENZ to evaluate the impact of the changes and must provide implementation and back-out/recovery plans for all changes.
6. FENZ may, at its sole discretion, withhold approval or may require re-testing and re-certification of the facilities where they determine that testing and re-certification are required to demonstrate correct, compliant operation. Changes to systems, equipment or facilities without the prior, written approval of FENZ will void the AFASP certification.

10.5.3.1 FIRE ALARM-RELATED DATA

All data regarding the AFAS held by the AFASP is the property of FENZ and must not be used for any purpose not related to the AFAS without the written permission of the FENZ. The AFASP must carry out:

1. all changes to data related to fire alarms and the fire alarm owners' details in accordance with FENZ standards, as notified by FENZ and updated from time to time
2. the migration of a fire alarm owner to a different AFASP in accordance with FENZ standards as provided by FENZ and updated from time to time.

10.5.3.2 FIRE ALARM EVENT DATA

Fire alarm and related event data and the correct handling of event data are critical to the correct operation of the AFAS. In handling event data, the AFASP must meet the following requirements:

1. The AFASP must provide event data from the fire alarms in accordance with the AFASPCIS
2. The AFASP must provide FENZ with event data from zones or points from fire alarms that are able to provide that information from zones or points, in accordance with the AFASPCIS
3. The AFASP must forward alarm-event data to FENZ electronically immediately after that data becomes available at the input to its monitoring and event handling system
4. In case the AFASP cannot forward alarm-event data to FENZ electronically, or the Service Provider does not receive an acknowledgement from FENZ STSMHS Domain of the message containing the alarm-event data within 20 seconds, then the AFASP must call FENZ (111 call) and notify FENZ Communications Centre of the alarm event verbally.

10.5.4 OPERATIONAL SUPPORT SYSTEMS

10.5.4.1 CUSTOMER MANAGEMENT, BILLING AND COLLECTIONS SYSTEMS

1. The AFASP must establish and maintain a system for storage and management of data concerning customers, contracts with customers, customer sites, premises and facilities, and AFA equipment installed at those sites.
2. The system must, at a minimum, contain the information set out in the AFASP Agreement and further described in Section 8.4: FENZ Domain.
3. In addition, the AFASP must establish and maintain separately or in conjunction with the above, a system to calculating the periodic charges due, including any amounts due to the FENZ, and to produce and deliver to the customer an invoice for the charges due.
4. The AFASP must establish and maintain a system for:
    a. recording the periodic charges due to FENZ for each of the AFA connections and any other amounts collected by the AFASP on behalf of FENZ
    b. reporting the amounts due to FENZ in a form prescribed by FENZ, and
    c. remitting the amounts due to FENZ on a timely basis.

10.5.4.2 INCIDENT MANAGEMENT SYSTEMS

1. The AFASP must have a procedure for investigating any incidence or complaints of substandard service, and other quality or system failures, to determine the root cause of the problems and failures and to take action to ensure that similar problems will not recur. The effectiveness of the corrective action must be evaluated to ensure that it has rectified the root cause of the problem.
2. The AFASP must establish and maintain a system for recording all customer contacts and for tracking and reporting progress of all customer requests, faults and complaints.
3. This AFASP system must provide a register of incidents of substandard service, complaints and other quality or system failures as well as customer queries and issues. The register must maintain a record of the incidents, actions taken and the resolution of the incidents. The register must be made available to FENZ upon request.

10.5.5 TELECOMMUNICATIONS FACILITIES

The AFASP must ensure that they provide telecommunications facilities which fully comply with the requirements set out in Section 6.1.2: Automatic Fire Alarm Service Providers and in this section. They must:

1. Fully document the telecommunications path(s) and other facilities for handling signals between the network-interface of a fire alarm and the AFASP interface of the Signal Transport System Message Handling System (STSMHS)
2. Maintain the documentation set out in point 1 so that the information contained therein is current at all times
3. Make the documentation available to FENZ or its authorised agent(s) on request
4. Ensure that the telecommunications network and other systems and facilities described in point 1 is capable of forwarding fire alarm event messages to the STSMHS
5. Demonstrate that the telecommunications path(s) and other systems and facilities described in point 1 will operate successfully end-to-end and meet the performance standards set out in Section 9.1: Availability and performance standards for AFASP systems and facilities
6. Ensure that the telecommunications path(s) between the network-interface of a fire alarm and the SP-interface of the STSMHS and other systems and facilities described in point 1 offers protection against unauthorised access to:
    a. the STSMHS
    b. the AFASP's equipment
    c. fire alarms
7. Ensure that the telecommunications path(s) between the network-interface of a fire alarm and the SP-interface of the STSMHS described in point 1 offers protection against viruses and other malicious and unwanted software
8. Ensure that the telecommunications network described in point 1 provides adequate means for network traffic management and control of network loading
9. Identify single points of failure in its corporate telecommunications network that could affect forwarding messages from a fire alarm to the STSMHS, and the means in place to ensure continuity in the event the corporate network is compromised
10. Ensure that the network is physically and logically separate from all other internal networks, including networks for monitoring other devices. The only link permitted between the network and the AFASP's internal networks is the AFASP's dedicated communications gateway/concentrator servers
11. Identify and describe the method used for assigning Internet Protocol (IP) addresses to the devices within its internal networks and within the systems and facilities used for transmission of AFA messages
12. Maintain a record, available for inspection by FENZ and its authorised agent(s), of assigned IP addresses within its internal networks and within the sub-network utilised to transport AFA messages
13. Ensure that all equipment and software used in the facilities described in point 1 and used to provide service for the AFAS (e.g. telecommunications equipment, hardware, application software) are suitably supported (e.g. have a maintenance contract) so they will consistently fulfil the performance requirements set out in this section
14. Ensure that monitoring and reporting facilities are in place to monitor and report on the performance parameters set out in this section.

10.6 AFASP MANAGEMENT AND QUALITY SYSTEMS

10.6.1 MANAGEMENT AND QUALITY ASSURANCE

1. The AFASP must appoint one of its staff (the Systems Coordinator) to have overall responsibility for compliance with the requirements of this Code of Practice in the day-to-day work of the organisation. This must be a senior person with sufficient authority in the organisation to ensure that all other staff follow the management system at all times.
2. The responsibility and authority of this Systems Coordinator must be defined in a written job description or similar document approved by the Chief Executive of the company or an officer of the company appointed to act in their place. The AFASP must establish either a business procedure and/or quality manual that includes the requirements of this document.
3. The AFASP must document, authorise and advise staff of the following policies:
    a. health and safety policy
    b. quality policy
    c. environmental policy.
4. The AFASP must conduct management reviews at 6-monthly intervals to monitor the management system and ensure its effectiveness.
5. The AFASP must conduct monthly internal reviews to reinforce agreed best practices and to continually improve the system.
6. Records of the management reviews and internal audits must be maintained and, upon request, be made available to FENZ for inspection.

10.6.2 BUSINESS CONTINUITY

1. The AFASP must establish and maintain a business continuity plan (BCP).
2. The BCP should clearly state the procedures that would be followed in the event of:
    a. malfunction of individual items of equipment
    b. malfunction of the configuration as a whole in the normal working environment
    c. any activity, unrelated to malfunctioning equipment, that results in an interruption or denial of the service contracted to be provided by the staff and equipment at the normal premises, e.g. staff disruptions, loss of access to premises, etc.
    d. Failover procedures, processes and capability
    e. Fall back procedures, processes and capability.
3. The business continuity/business recovery document should include information concerning the:
    a. critical resources
    b. business and related risks
    c. risk assessments (including business impact analysis)
    d. risk management plans
    e. risk monitoring plans.
4. Systems and facilities to minimise impacts and ensure business continuity should be detailed in the plan e.g. automatic fire suppression systems at the AFASP's premises.
5. The BCP must establish a plan to ensure the continuation of service and, in the case of an interruption to the service, how and how soon the contracted service would be provided using backup or alternative facilities in the event of any of the above or similar occurrences. The AFASP must demonstrate the ability to meet the requirements of this plan in practice.

10.6.3 STAFF TRAINING AND QUALITY MANAGEMENT

1. The AFASP must ensure that all staff are fully trained for the work that they do. Staff must be provided with written work instructions/procedures setting out how the AFASP requires critical jobs or tasks to be carried out.
2. The AFASP practices must comply with reference standard(s)/code(s), and regulations where applicable.
3. Records of staff training must be kept and staff competence must be reviewed 6-monthly to ensure continuing competence and to determine whether retraining is required.

10.6.4 RECORDS AND RECORDS MANAGEMENT

1. The AFASP must have a system for uniquely identifying and controlling all its documents to facilitate location of key documents and to ensure that only the current editions are in use and that no unauthorised changes are made.
2. Documents included within this requirement are those that are essential for ensuring the quality of the service and the proper operation of the AFASP's management system. Documents include:
    a. drawings
    b. material specifications
    c. work instructions
    d. risk assessments
    e. equipment and specifications
    f. operation manuals (the current version and one previous version must be retained)
    g. reference manuals
    h. procedure manuals
    i. job descriptions
    j. regulations.
3. The term 'document' includes any method of recording or displaying information. Documents may be in the form of paper, computer files, wall charts, posters, videos, photographs, Codes of Practice and so on. Whatever the format, documents should be authorised and kept up-to-date to allow them to be used as a permanent reference.
4. The document control system must also ensure that copies of documents are available to everyone who needs them so that they do not have to rely on memory for information.
5. Records must be sufficient to demonstrate that all essential processes have been carried out, and that all essential inspections or tests have been undertaken in compliance with the management system and the requirements of this Code of Practice.
6. Records must be retained for an appropriate period. This period will depend upon the nature of the record. The following table lists several types of records and their retention periods:

Record type	Retention period
Customer & contract records	7 years
Computer system logs	18 months
Staff records	5–7 years*
Premise inspections & NZSA Certificate	12 months after expiry of certificate
Customer contact & complaint records	Approx. 2 years
Incident reports & actions records**	Minimum of 18 months

* Dependent on the organisation's policies.

** Records of serious incidents must be retained in the event of claims or litigation.

11 APPENDICES

11.1 APPENDIX 1 - FENZ SERVICE CRITICALITY DEFINITIONS

Name	Impact	Description	Implication	RPO + RTO

Life critical	If these systems fail, lives are at risk.
	
	People Die.
		• Tightly focused and integrated IT/Ops with business ownership
		• Clearly defined and articulated Definitions, Standards, Principles and Procedures. With ownership and review procedures in place.
		• Rigorous business requirement evaluation and alignment process with service definitions. Defined exceptions processes.
		• Operational standards: highly managed, actively reviewed monitored Operation, Development, Release and Change mgmt.
		• SDLC is highly rigorous and extensively managed
		• Development and testing is to extensively controlled, and synchronised environments with regulated engineering criteria
		• Full-redundant continuous-running systems:
		  ○ active-active application clustering mode
		  ○ redundant network and pathways
		  ○ hot-swap hardware, with duplicated data-streaming
		  ○ redundant data-store
		  ○ resilient transactional commit
		  ○ geographically split locations
		  ○ No single points of failure
		  ○ Non-Blocking
		• Rotate service centre with patching windows
		• In-house specialists and operational management
		• Extensive contingent partnerships and close-contractual arrangements
		• Ops support: dedicated specialised skills and infrastructure
		• Maintenance window active rolling service, with hot-standby (emergency) service
			Complexity
			Extreme
			
			Cost
			Significant
				RTO < 10 Min
				
				RPO < 30 Min
				
				Up Time
				99.999%
				
				Downtime Tolerable
				5.26mins per year

Mission Critical	If these fail, will impact safe deployment of services, delay access to time-critical outcomes. Can have Legal impact.
	
	People face Legal Action
		• Operational standards: managed, actively monitored with improvement processes in place
		• Effective and proven operation, development, release and Change mgmt. procedures – with specific owners and business alignment
		• SDLC is rigorous, with managed lifecycle and feedback loops.
		• Development work directly with Operations and business.
		• Have jointly agreed development and health profile criteria, as well as move to introduce standards based criterion.
		• Insourced or outsourced facilities – dedicated operations staff
		• Multiple cloned environments, systems and data replication
		  ○ hot standby (dedicated) systems;
		  ○ active clusters and data-routing
		  ○ alternative pathways available to core services
		  ○ resilient data management from Disk up to application
		• rigorous operational support model
		• 24x7 operational monitoring
		• Maintenance window Quarterly Window [4 hrs.], with monthly rolling environment fail-over
		• Maintenance window is applied to fail-over environment, ready for monthly cut-over
		• Development and testing is to controlled, using an automated test and release toolset, as well as dedicated standardised environments
			Complexity
			High
			
			Cost
			High
				RTO: 4 Hours
				
				RPO: 4 Hours
				
				Up Time
				99.99%
				
				Downtime Tolerable
				52.56mins per year

11.2 APPENDIX 2: GLOSSARY OF TERMS

Term	Definition
Access Device	A device that connects a fire alarm to the AFAS
Acceptable Solution	Acceptable Solutions for NZBC clauses C/AS1-7 Protection from fire. The scope of each Acceptable Solution is limited to a certain group of buildings: • C/AS1 is for typical houses, small multi-unit dwellings and outbuildings. • C/AS2 is for other multiple-unit accommodation buildings such as apartments, hotels, motels and hostels. • C/AS3 is for buildings where care or detention is provided – i.e. where there is a delay to evacuation (excluding prisons). • C/AS4 is for public access buildings such as schools and other educational facilities and places where people gather – halls and recreation centres, cinemas, shops, restaurants and cafés, hairdressers and so on. • C/AS5 is for many workplaces such as offices, laboratories, workshops, most factories and low-level storage facilities. • C/AS6 is for high-level storage areas in buildings such as warehouses, temperature-controlled storage, trading and bulk retail. • C/AS7 is for vehicle parking and storage, including car parks, truck and bus parks, stacked boat storage and light aircraft hangars.
AFA	Automatic Fire Alarm. Refer to Fire Alarm.
AFAID	Automatic Fire Alarm (unique) IDentification number
AFAS	Automatic Fire Alarm System. Includes the collection of equipment, software, transmission links, standards, specifications, protocols and processes necessary to transport messages between fire alarms and the Communications Centres
AFASP	A FENZ certified Automatic Fire Alarm Service Provider, providing Fire Alarm monitoring and transmission services as specified in this AFAS 'Code of Practice' and the FENZ 'Certification for Automatic Fire Alarm Service Providers' procedure
AFASP Domain system	System under control of the AFASP that exchanges messages between the Fire Alarm and FENZ STSMHS domain in accordance with the AFASPCIS
AFASPCIS	Automatic Fire Alarm Service Provider Computer Interface Specification means the protocol specification, including the extended alarm protocol specification (XAP) and associated application programming interface specification, for the computer interface between the FENZ STSMHS domain and the AFASP Domain system, as available on the FENZ public internet page, as amended from time to time
AFASPCIS XAP	Automatic Fire Alarm Service Provider Computer Interface Specification Extended Alarm Protocol
Annual availability	The annual proportion of time during which a unit or a system is able to perform its required function within the scheduled service hours (service hours are: 24 hours per day, 7 days per week)
API	Application Programming Interface
AS	Australian Standard
ASE	Alarm Signalling Equipment
BCP	Business Continuity Plan
CAD	Computer-Aided Dispatch
CAT	Customer Alarm Terminal
Certificate of Compliance	Fire alarm or sprinkler installation certificate issued by a body accredited for fire alarm installation in accordance with the relevant New Zealand standard
Certification	The meaning set out in the FENZ 'Certification for Automatic Fire Alarm Service Providers' procedure available on FENZ public internet page, as amended from time to time
Certified fire alarm	Fire alarm that has a Certificate of Compliance issued by a body accredited for fire alarm installation certification or a letter from an FENZ Area Manager authorising the connection of the fire alarm to the AFAS

Term	Definition
Code of Practice	This document including all appendices - the Code of Practice for Automatic Fire Alarm System document available on the FENZ public internet page, as amended from time to time
Comcen	Communications Centre. FENZ personnel who are responsible for dispatching fire appliances to fire alarm alarm-events and 111 calls. FENZ operates three Communications Centres, located in Auckland, Wellington and Christchurch
Computer Interface Specification (CIS or AFASPCIS)	The protocol specification, including the extended alarm protocol specification (XAP) and associated application programming interface specification, for the computer interface between FENZ STSMHS domain and the AFASP Domain system, as available on FENZ public internet page, as amended from time to time
Contact point	Accept and act on calls in accordance with performance standards. Contact points as defined in agreements between the agreement parties
CPN	Common place name. A CPN represents the location of a named, recognisable and definable feature, built object or geographic place. CPNs include: • names of towns, cities and localities • geographic features, such as bridges, lakes, streams, and landmarks • statues and memorials • buildings
CTU	Communicating terminal unit
Customer	Owner or occupier of protected premises who has entered into an agreement with the AFASP
Direct connection	Telecommunications connection where messages are sent electronically without human intervention
Emergency	Emergency means (within the Fire and Emergency New Zealand Act 2017) an event requiring an immediate action to protect and preserve life, prevent injury, or avoid damage to property and includes— a) a fire (including an alarm of fire); and b) a hazardous substance emergency; and c) a state of emergency declared under the Civil Defence Emergency Management Act 2002; and d) any other substance emergency; and e) an incident attended by emergency services (including the New Zealand Police, FENZ, and hospital and health services)
FA	Fire alarm. An apparatus that performs specified fire-related functions in response to the operation of a sprinkler, detector, manual call point or other input, as defined in the relevant Standards New Zealand standard, as amended from time to time, that is connected to the AFAS by the AFASP
FACP	Fire Alarm Control Panel
FACU	Fire Alarm Control Unit
False alarm	False alarm (as defined under FENZ False Alarms Policy (POLFA 7.5) as amended from time to time
FENZ	Fire and Emergency New Zealand or its appointed agent, as described in the Fire and Emergency New Zealand Act 2017: 1) FENZ is a Crown entity for the purposes of section 7 of the Crown Entities Act 2004. 2) The Crown Entities Act 2004 applies to FENZ except to the extent that this Act expressly provides otherwise. 3) FENZ is the same body as the New Zealand Fire Service Commission constituted under section 4 of the Fire Service Act 1975.
Fire message	Message from a fire alarm showing that one or more of the fire alarm's detectors are in a fire condition

Term	Definition
Force Majeure	Any cause reasonably beyond a party's control. A Force Majeure event is an event reasonably beyond the control of the affected party (including, without limitation, a directive to FENZ by someone so empowered) but does not include financial difficulties or delay caused by or in connection with relations between the Contractor and the Contractor's employees, agents or contractors.
IP	Internet Protocol
IQP	Independent Qualified Person
MBIE	Ministry of Business Innovation and Employment
MHS	Message Handling System
NAD	Network Access Device
NAK	Negative acknowledgement
NZBC	New Zealand Building Code
NZS	New Zealand Standard
PFA	Private Fire Alarm. Refer to Fire Alarm.
Protected premises	A building or part of a building that is: a) fitted with one or more fire alarms; and b) physically separate from other buildings at a given location (provided that, in determining whether or not a building is physically separate, common walls, walk ways and service tunnels must be ignored)
Relevant Building	A building or part of a building used for 1 or more of the following purposes: a) the gathering together, for any purpose, of 100 or more persons: b) providing employment facilities for 10 or more persons: c) providing accommodation for 6 or more persons (other than in 3 or fewer household units): d) a place where hazardous substances are present in quantities exceeding the prescribed minimum amounts, whatever the purpose for which the building is used: e) providing an early childhood education and care centre (other than in a household unit): f) providing nursing, medical, or geriatric care (other than in a household unit): g) providing specialised care for persons with disabilities (other than in a household unit): h) providing accommodation for persons under lawful detention (not being persons serving a sentence of home detention or community detention, or serving a sentence of imprisonment on home detention, or on parole subject to residential restrictions imposed under section 15 of the Parole Act 2002): i) any other prescribed purpose.
Service Agent	A person engaged by the owner of Protected Premises or Relevant Building to maintain and repair the Fire Alarm
Services	Fire alarm monitoring and transmission services provided by the AFASP in accordance with this Code of Practice and Agreement for Automatic Fire Alarm Monitoring and Transmission Services
SITE	NZ Police/FENZ Shared Information Technology Environment
SMART	The FENZ Spatial Mapping and Reporting Tools database and applications environment associated with the Station Management System, which manages data and information supporting FENZ AFAS Fire Alarm System Commissioning process as described in Section 9.3: Fire Alarm Commissioning
SMS	The FENZ Station Management System - the FENZ database and application environment that manages data and information supporting FENZ AFAS Fire Alarm System Commissioning process as described in Section 9.3: Fire Alarm Commissioning

Term	Definition
STS	Signal Transport System. Hardware, software, transmission links, and processes to transport messages between fire alarms and the STSMHS
STSMHS	Signal Transport System Message Handling System. Collection of servers, equipment and transmission links between the AFASP Domain system and the Communications Centres alarm interface servers (which transports messages from FENZ Interconnection Device to the Communications Centres alarm terminals), as contracted to and managed by FENZ STSMHSSP
STSMHSSP	Signal Transport System Message Handling System Service Provider. Provides operation and maintenance services for the STSMHS, as agreed with FENZ
TCP	Transmission control protocol
UDP	Universal datagram protocol
VPN	Virtual private network

11.3 APPENDIX 3: ASSOCIATED DOCUMENTS, LEGISLATION, REGULATION AND STANDARDS

Document/Standard	Description	Author	Publication Version : Year [Classification]
AFASPCIS	Automatic Fire Alarm System Computer Interface Specification	FENZ	1.7 : 2019
AFASPCIS XAP	Automatic Fire Alarm System Computer Interface Specification Extended Alarm Protocol	FENZ	1.7: 2019
AFAS FA Data Management in SMS	Specification for fire alarm data management in the FENZ station management system	FENZ	5.0 : 2014
STSMHS – AFASP Application Programming Interface Design Specification	Specification for FENZ STSMHS Domain to AFASP Domain API integration	FENZ	1.3c : 2007; or 1.7 : 2005 [In-Confidence]
Certification for Automatic Fire Alarm Service Providers	Fire and Emergency New Zealand (FENZ) requirements for Automatic Fire Alarm Service Providers (Service Providers) becoming and remaining certified to provide services in respect of Automatic Fire Alarm Systems	FENZ	1.8 : 2017
AFASP Certification Test Scripts Parts 1 and 2	STSMHS – AFASP Application System Tests	FENZ	4.6 : 2010 [In-Confidence]
AFAS Signal Transport System Message Handling System [STSMHS] Solution Architecture Description	Specification for the current state build, architecture, software licensing and components of the NZFS Automatic Fire Alarm System Signal Transport System Message Handling System (STSMHS)	FENZ	1.0 : 2015 [Commercial-In-Confidence]
PMFRM01_Alarm Panel and Inlet Approvals	FENZ national process for fire alarm panel installation approvals	FENZ	2014
F2 - Fixed fire protection systems (NCI 25)	FENZ national procedure for safe and effective operations at calls to complexes protected by sprinkler, drencher, or other fixed fire protection systems	FENZ	2008
G1-2 - Private Fire Alarms (NCI 24)	FENZ national procedure for efficient operations at calls to complexes monitored by private fire alarm systems	FENZ	2008
FENZ National Procedure PMPP07 - Commissioning Private Fire Alarms	FENZ national process for commissioning of Fire Alarms to the AFAS	FENZ	2014
Fire and Emergency New Zealand Act	Statutory basis for FENZ to operate	NZ Government	17 : 2017
Crown Entities Act	Statutory basis for FENZ to operate	NZ Government	115 : 2004

Document/Standard	Description	Author	Publication Version : Year [Classification]
Building Act	Statutory basis for FENZ to operate and contains the provisions for regulating building work	NZ Government	72 : 2004
Building Regulations	Various Building Regulations, which contain prescribed forms, list specified systems, define 'change the use' and 'moderate earthquake', and set out the rate of levy and fees for determinations	NZ Government	Various
Building Code (NZBC) and Acceptable Solutions C/ASx	The Building Code, contained in Schedule 1 of the Building Regulations 1992, which sets performance standards all new building work must meet, and covers aspects such as stability, protection from fire, access, moisture, safety of users, services and facilities, and energy efficiency	NZ Government	1992
Compliance Document for New Zealand Building Code Clause F7 Warning Systems	Compliance Document prepared by the Department of Building and Housing in accordance with section 22 of the Building Act 2004, and the New Zealand Building Code Acceptable Solution F7/AS1.	Department of Building and Housing	04 : 2012
BRANZ Guide to the Acceptable Solutions : Protection from Fire	Guide to Acceptable Solutions C/AS1–7 : Protection from Fire produced by BRANZ in summary from NZBC compliance documents published by MBIE	BRANZ	2015
FENZ False Alarms Policy (POLFA 7.5)	FENZ Policy for false alarm management	FENZ	POLFA 7.5
Goods and Services Tax Act	Goods and services tax payable	NZ Government	141 : 1985
Parole Act	Statutory basis defining Relevant Building providing accommodation for persons under lawful detention	NZ Government	10 : 2022
Companies Act	Statutory basis defining related company	NZ Government	105 : 1993
Arbitration Act	Statutory basis for contract disputes and arbitration	NZ Government	99 : 1996
AS/NZS CISPR	NZ Standards for radiated and conducted emissions and respectively the new compliance requirements (RCM and R-NZ)	Ministry of Business, Innovation and Employment	22 : 2004
NZS 4512:2010	NZ Standard for Fire Detection and Alarm Systems in Buildings	Standards NZ	2010
NZS 4541:2013	NZ Standard for Automatic fire sprinkler systems	Standards NZ	2013
NZS 4515:2009	NZ Standard for Fire sprinkler systems for life safety in sleeping occupancies (up to 2000 m2)	Standards NZ	2009
NZS 4517:2010	NZ Standard for Fire sprinkler systems for houses	Standards NZ	2010

Document/Standard	Description	Author	Publication Version : Year [Classification]
NZS 3100:2017	Approval and Test Specification – General requirements for electrical equipment	Standards NZ	2017
AS/NZS 2201.2:2004	AS/NZS 2201.2:2004: Intruder alarm systems – Monitoring centres	Standards NZ	2004
Open systems interconnection (OSI) 35:100	Standard for AFAS communications interface, the Open Systems Interconnection model (OSI model) partitions the AFAS communications interface system into 7 abstraction layers.	International Standards Organisation (ISO)	35:100

11.4 APPENDIX 4: CHANGE CONTROL

No.	Date	Page, section	Description of change	Owner
1	November 2018	Entire document	Reviewed and updated CoP to reflect current state environments, processes policies, procedures and standards	Stuart Waring
2	March 2019	Entire document	Code reviewed and updated from FENZ SME and industry consultation	Stuart Waring