Digital Solutions Division

ACT Government | ACT Health

St-09 BMCS ICT Specifications

Version 2020.1.0- Approved

This page is left intentionally blank

Please Read

IMPORTANT COMPLIANCE REQUIREMENTS

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

This is a controlled document and is reviewed on an annual basis. The last review was carried out on September 2019. If you are viewing this document after September 2020, you will need to contact the sender to confirm you are working from the latest revision.

It is the responsibility of the contractor/vendor to read and adhere to the procedures, processes and guidelines set out in the following document when quoting for or carrying out work for ACT Health.

If you have questions or require clarification of any of the procedures, processes or guidelines in the following document please contact the sender of the document in writing with your questions so that a formal response can be provided. If any specific requirement is unclear, it is expected that clarification will be sought from the Health DSD - ICT architect(s), rather than a decision made and a design implemented and based on unclarified assumptions.

These standards are applicable to ALL CHS and ACTHD sites or any work funded by ACTHD (e.g. Calvary, ACTHD provided NGO sites) unless specifically exempt.

All Greenfield Health sites are expected to be fully compliant with all appropriate standards.

Brownfield Health sites undergoing refurbishment should be fully compliant unless an exemption is provided by DSD Infrastructure Hub.

In the event of any design non-compliance issues, a Departures document must be completed and submitted to DSD Infrastructure Hub. These issues should be resolved, in consultation with DSD Infrastructure Hub, as soon as possible within the project process and explicitly prior to site handover.

While some test cases have been cited within these documents as examples, the list is not exhaustive, and all appropriate test procedures shall be formulated, approved prior to testing and testing shall be performed by the client system administrators before full acceptance can be signed off by the Director of ICT Infrastructure Hub.

IMPORTANT:

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

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

Document review high level

(to review detailed document updates click here)

Version	Summary of Changes	Author	Date
2020 0.1	Updated EMS content	Raj Mohan	21/02/2020
2020 0.2	Review DBR	David Richards	25/03/2020
2020 1.0	Mark Moerman Approval for release	Mark Moerman	30/03/2020

Document references

Document	Version	Location

Document default review cycle

(to be review every 12 months from the release date)

Date	Version	Comments
Feb 2020	2020 0.1	New format date
Mar 2020	2020.1.0	First Release New Format & incl. EMS
Mar 2021		(Next review date)

Document Owner

Name	Location
Senior Director, ICT Infrastructure Hub	DSD, Future Capability & Governance, ACT Health

Contents

1. Building Management and Control System (BMCS)

1.1 Introduction

This document forms part of a suite of documents that describe ICT specifications for the ACT Health Directorate, Business and Infrastructure support systems. It provides the Building Management and Control System (BMCS) ICT Specification including the Energy Management System (EMS), applicable to the green-field and refurbished brown-field sites.

1.2 Assumed knowledge and document dependencies

Relevant documents are mentioned in Appendix A.

1.3 Key Stakeholders

Stakeholder Title	Authority	Details
Digital Services Division -CTO	Approval	
Director Business & Infrastructure	Approval	
Shared Services ICT (Solutions Architects & NCS)	Approval	

Table 1 - Audience and Stakeholder Positions

1.4 Disclaimer

The following document provides ICT ONLY specifications and requirements for the designated system – Building Management and Control System, and is by no means intended to cover all the comprehensive business requirements for the system. Additional business and user requirements will be presented in project specific documentation such as Business Requirements, Solution and Detailed designs.

2. Executive summary

The specifications provided in this document are based on standardising architecture and integration for the Building Management and Control System and the Energy Management System across all the Health Directorate sites. This architecture will provide the building blocks for a consistent implementation of this system at the Health Directorate sites. Additionally, it provides the benefit of installations that have standardised configurations within the Directorate, enabling reusable patterns and repeatable system implementation. The consistent architecture shall minimise the risks associated with ongoing support for disparate implementations, simplifying the installations whilst reducing the ongoing maintenance costs. The incumbent system is the Siemens Apogee platform.

The Building Management and Control System provides management, control, communication and speedy response to alarm and maintenance events, making buildings more comfortable, safe, productive, efficient… and less costly to operate.

The Building Management and Control System offers the functionality of a BACnet Web-based Application Suite. The BMCS uses the BACnet protocol which performs across multiple systems, providing the necessary foundation for future expansion. BACnet is the Heating, Ventilation and Air Conditioning (HVAC) industry standard protocol, according to its founding and sponsoring organizations, American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE), International Standards Organization (ISO), and American National Standards Institute (ANSI). Its reputation and growing use make it the best choice for a standard protocol across a system, or to use as an interoperability tool to help knit together a cohesive, tightly integrated system despite disparate technologies or vendor systems.

Now and into the future, building operations are driven by higher energy costs, simplification of climate control, and the promise of wireless and digital communications. The BMCS system currently delivers facility management solutions in an expandable and upgradable system. The Siemens System’s backward and forward compatibility allows continual performance improvement, expandable functionality and future proofing, while protecting past investments and OPEX.

The system will comply with the architecture principles such as high level of availability, ability to integrate with other systems, IP-based connectivity and adherence to tiered architectural model.

The network infrastructure implemented to support Health Directorate critical systems is in compliance with the Medical Grade Network (MGN) architecture. The MGN architecture can be summarised as modular, Highly Available (HA) and resilient network which minimises the impact of a network component failure on the Health systems. Additionally, the architecture provisions sufficient capacity to allow for growth in the infrastructure requirements for Health systems.

3. Enterprise Architecture

The architecture presented within this document complies with the Enterprise Architecture Principles outlined in "ICT Enterprise Architecture Principles_v0.2_2013_03_20" document. The architecture principles are as follows:

- Control technical diversity to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple systems;
- Maintaining interoperability between systems to conform to defined standards that promote benefit to the business;
- Commissioning systems to a defined level of availability, recognising increasing demand for services to be provided outside of traditional office hours. The system availability also considers the lack of tolerance for system outage over longer periods of time;
- The systems must be manageable and be monitored;
- Use of common systems for head-end and building concentrator layers throughout the Health Directorate is preferred rather than use of separate vendor systems performing identical tasks;
- The user interface layer of the architecture must provide devices that are supported by the building concentrators; and
- The systems must be able to adapt for change and growth. The architecture modularity allows for individual components to be upgraded without replacing the entire system.

The following technology principles are also applicable:

- Interface between head-end and building concentrator shall be IP over Ethernet (can be a sub protocol of IP e.g. TCP, BACnet, UDP etc); and
- Interface between endpoint devices and the concentrator shall follow known standards; however it can be a mixture of analogue, dry contact, or data protocol compliant cabling (e.g. BACnet over RS485, Zigbee over IEEE 802.15.4 etc).

The preferred architecture model implemented at the Health Directorate uses a three-tiered modular approach. The tiered model is based on the principles of hierarchy, modularity, resiliency and flexibility.

This model consists of three tiers, head-end servers/appliances, building based concentrator and endpoint devices, which support hierarchical and modular approach. The head-end and building concentrator tiers within this model are intended to provide high levels of resiliency and availability. The model also provides the flexibility of leveraging existing infrastructure, where practical, which is expected to be used within various onsite or off-site buildings.

The Building Management and Control System must be compatible with IP networks for the top two tiers of the architecture i.e. at Head-end and building concentrators. Additionally, it should be able to leverage the layer-3 network commissioned by the Shared Services ICT. Additionally, edge devices over time, may become more Ethernet or wireless based as IOT becomes more prevalent

The Shared Services ICT network architecture has been provisioned to comply with the MGN architecture which supports the principles outlined previously, providing a robust and resilient network that supports the Building Management system discussed in this document.

The following diagram, Figure 1, illustrates at a conceptual level the expected architecture for the Building Management and Control System. Each architecture layer is described in the following sections.

The Electrical Metering System is an IP based electrical meter monitoring system and whilst it is a separate standalone system, will work in tandem to provide statistical usage data, to enhance the operational efficiency of the BMCS.

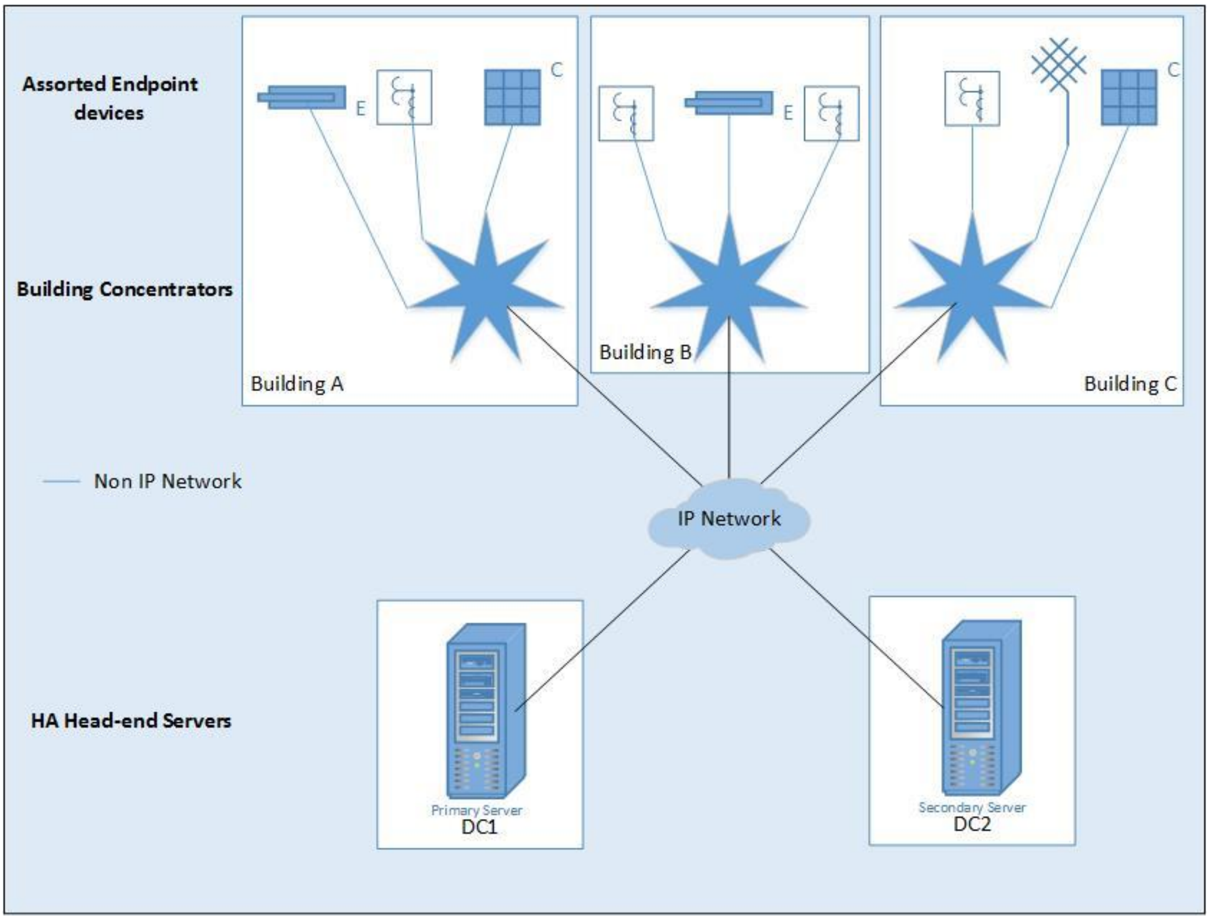


Figure 1 - Three-tiered Architecture model

Alternatively, some systems may not have building-based concentrators. The endpoint devices for these systems connect directly to the Shared Services ICT Ethernet switches, which provide connectivity over the network to the head-end infrastructure. The head-end infrastructure is expected to comply with the standards and specifications previously outlined for the three-tiered architecture.

4. Building Management and Control System

The Building Management and Control System, is expected to comply with the architecture discussed previously. The architecture should be modular enabling any future system to be integrated into the Building Management and Control System so that it can be modified and expanded according to the future requirements of the Health Directorate.

The Head-end and concentrator tiers should be IP compliant and scalable. It should be able to support multiple controllers in different buildings and off campus sites while using the centralised HA head-end server configuration.

The following diagram, Figure 2, illustrates how the three tier Building Management and Control System architecture shall be implemented within the Health Directorate.

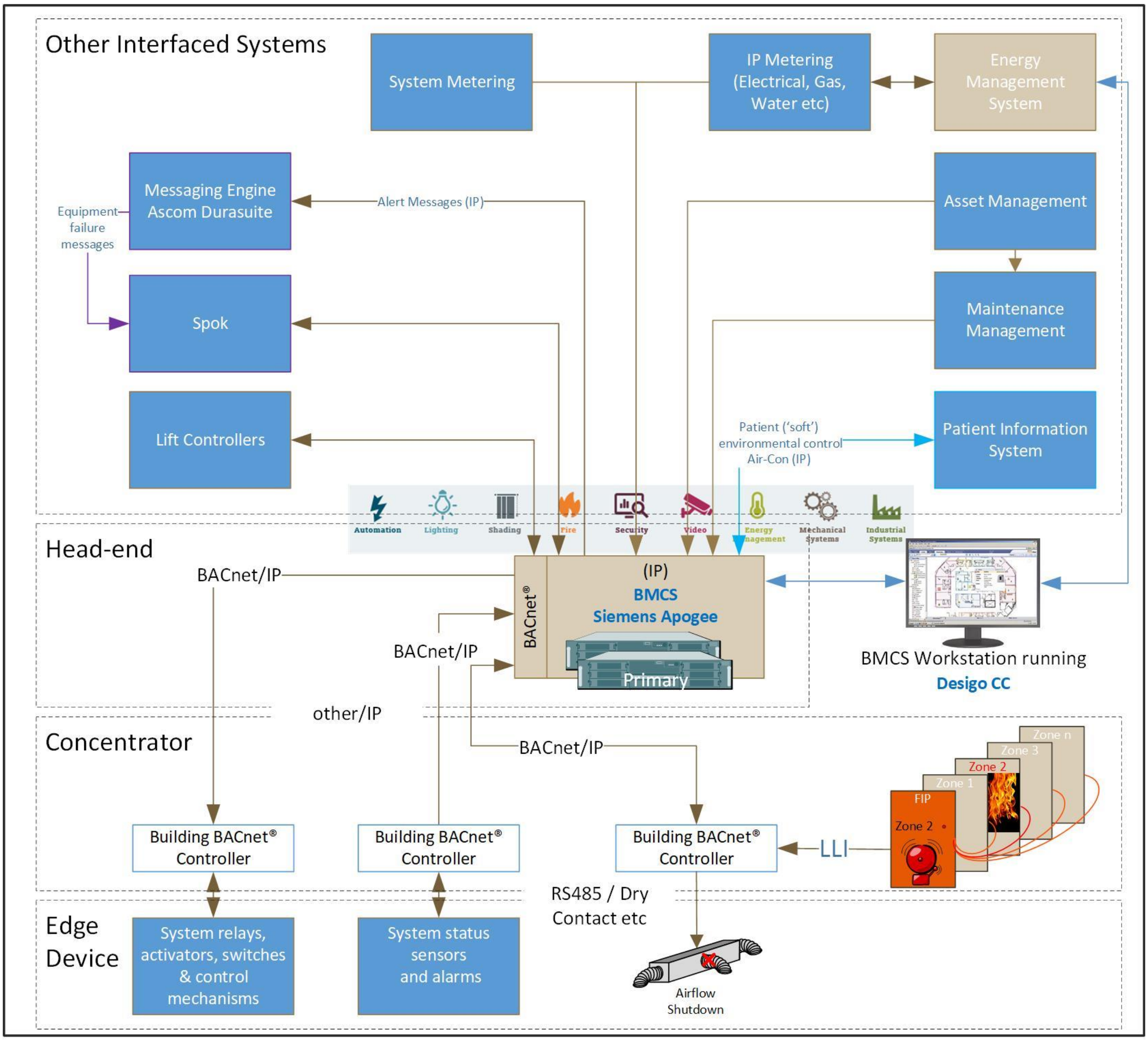


Figure 2 – Building Management and Control System Architecture

The head-end infrastructure is expected to be deployed in a highly available model, whereby primary and secondary servers/appliances will be provisioned for the system. In the HA configuration, the secondary appliance must be ready to assume the primary role in the event of the failure of the primary appliance. The fail-over is expected to be automatic, in order to minimise the impact on the business.

The primary and the secondary systems must consist of the same model appliances and must operate on the same level of software. It is expected a heartbeat will be maintained between the two systems and failover will take place when the secondary system does not receive a configurable number of heartbeats from the primary.

It is preferred that the primary and secondary servers be located in separate data centres. However depending on the system architecture, at a minimum the head-end infrastructure must be located in separate communications rooms in separate buildings.

The servers should be able to leverage the Shared Services ICT layer-3 IP network. Shared Services ICT will allocate the public IP addresses used by the system to communicate with other Health systems. In the event the system has a requirement to use private network, this information should be provided to the project team. The primary and secondary servers will present a Virtual IP (VIP) address to the devices accessing the head-end appliances. The individual IP addresses allocated to the appliances will not be exposed to other devices.

The Apogee system HA Server head-end will support the following capabilities:

- Provide Desigo CC software that will enable: -
    - Manage rapidly changing IT standards
    - Protect your systems from complex cybersecurity threats
    - Tap powerful cloud computing technologies
    - Store large quantities of building data for analysis
    - Use advanced visualization tools
    - See info on-the-go with mobile applications
    - Offer data access to external stakeholders
    - Leverage data from multiple building systems
- Support IP connectivity;
- Capable of supporting Virtual Local Area Network (VLAN) to separate BMCS network traffic from other systems;
- Geographically separate locations or at a minimum location in separate communications rooms;
- Support highly available servers operating in primary and secondary configuration;
- Individually, primary and secondary server infrastructure should be able to support the entire Health Directorate BMCS requirements. In the event the primary server are inoperative, the secondary server should be capable of supporting the functionality and capacity provided by the primary servers;
- The failover from the primary to the secondary should be automatic without any intervention. The vendor should state the length of time taken to failover from primary to secondary system;
- The failback from the secondary to the primary should be configurable to be either manual or automatic;
- The system must be able to send alerts to the nominated personnel when the secondary servers assume the role of primary servers;
- Maintain logs which record system errors and events such as date and time of configuration changes, synchronisation status with the secondary system, primary system fail over to the secondary system etc;
- The primary and secondary appliances must be capable of synchronising configurations when a change is implemented. The synchronisation shall be configurable to be automatic or manual;
- Capable of sending a message to the existing paging system;
- Capable of sending an IP based message to the messaging engine;
- Head-end and concentrator tiers capable of connectivity over Cat6$_A$ Ethernet cabling;
- Shall be capable of monitoring every endpoint device for failure and send alerts to the nominated B&I support personnel. This event shall also be recorded in the system log files;
- The system shall support Simple Network Management Protocol (SNMP);

- Provide reporting feature;
- Must be able to synchronise time with the Health Directorate Network Time protocol (NTP) server; and
- The Management Level Networks (MLN), (Head-end Tier) shall support the following protocols:
  - OPC® over TCP/IP;
  - Browser-based Web Access;
  - Terminal Services;
  - Modbus® TCP/IP;
  - SNMP;
  - SOAP/XML;
  - SMTP Support IP; and
  - BACnet network connectivity.

4.1 Building Infrastructure

The building concentrators will be the conduit between the endpoint devices and the head-end server infrastructure. The Concentrator is defined as a cabinet containing dual powered DIN rails, supporting multiple BACnet/IP controllers. The controllers shall be a gateway between the BACnet network and the ACTGov IP network. These controllers shall provide connectivity to the sensors, controllers, activators, meters and any other BACnet endpoint devices. They will process the functionality locally and/or forward it to the head-end infrastructure.

The building concentrators will support the following functionality:

- Capable of supporting IP VLANs to separate Building Management and Control System traffic from other systems;
- The controllers shall access the head-end infrastructure using the VIP address allocated to these devices. Therefore, failure of the primary appliances should not require the concentrators to access a different IP address for the secondary appliances;
- These controllers must be capable of supporting the endpoint functionality locally in the event the network connection between the building-based appliances and the head-end infrastructure is unavailable for a minimum of 24 hours;
- The controller cabinet should support hardware resiliency by providing dual power supplies to the ;
- Must be able to synchronise time with the Head-end server; and
- The Automation Level Networks (ALN), (Concentrator Tier) shall support the following protocols:
  - OPC® over TCP/IP;
  - Browser-based Web Access;
  - Terminal Services;
  - Modbus® TCP/IP;
  - SNMP;
  - SOAP/XML;
  - SMTP Support IP; and
  - BACnet network connectivity.

The concentrators will have an element of autonomous operation capability. In the event of loss of network connections providing connectivity to head-end servers, the concentrators should be able to support operational requirements and operational logging of the endpoint devices.

4.2 Endpoint Devices

Endpoint devices will be BACnet /Modbus compliant and be compatible with the controllers and the specific head end system.

The endpoint devices will feed (sensor/alarm/metering and other passive input devices) data back to the local building concentrator which will enable operational instruction / adjustment back to other active endpoint devices or communicate with the head-end providing information about current parameters and settings.

4.3 Exceptions and Exemptions

Any departure from the above architecture, shall only be accepted when a full assessment of the system has been completed by Shared Services ICT and been shown to provide an acceptable alternate architecture model after technical, operational and risk assessments have been satisfied.

The existing systems will not be required to undergo an assessment, unless they are not compliant with the architecture principles outlined in this document.

Wherever possible the controller cabinets shall be located within 80m of the nearest Floor Distributor (FD) room. Where this is not possible:

- They should be located in as clean an area as possible;
- Have OM4 (12-fibre core) links installed between the controller cabinet and the two Building Distributors (BDs);
- Be terminated on LC patch panels at either end; and
- Have a suitable location for industrial solid-state Cisco switches.

4.4 System Configuration Requirements

4.4.1 Hardware

There is a requirement within the Shared Services ICT to provision all systems, where available, on virtual systems.

Overall system must comply with standards as indicated in Appendix A.

The head-end appliances shall be capable of running on physical servers or preferably on virtual platforms.

The endpoint devices must be:

- BACnet compatible; and
- Physically robust to be able to withstand the industrial environment in which they will mostly be found.

4.4.2 Software and Licensing

The software and licensing must comply with the requirements specified in sections 7.12 and 7.14.

4.4.3 Power

All the critical Health Directorate systems are provisioned with dual Uninterruptible Power Supply (UPS) support. The controller cabinets should be supplied with this UPS backed power.

The power requirements for each cabinet shall be made available to Shared Services ICT for UPS sizing.

5. Energy Management System (EMS)

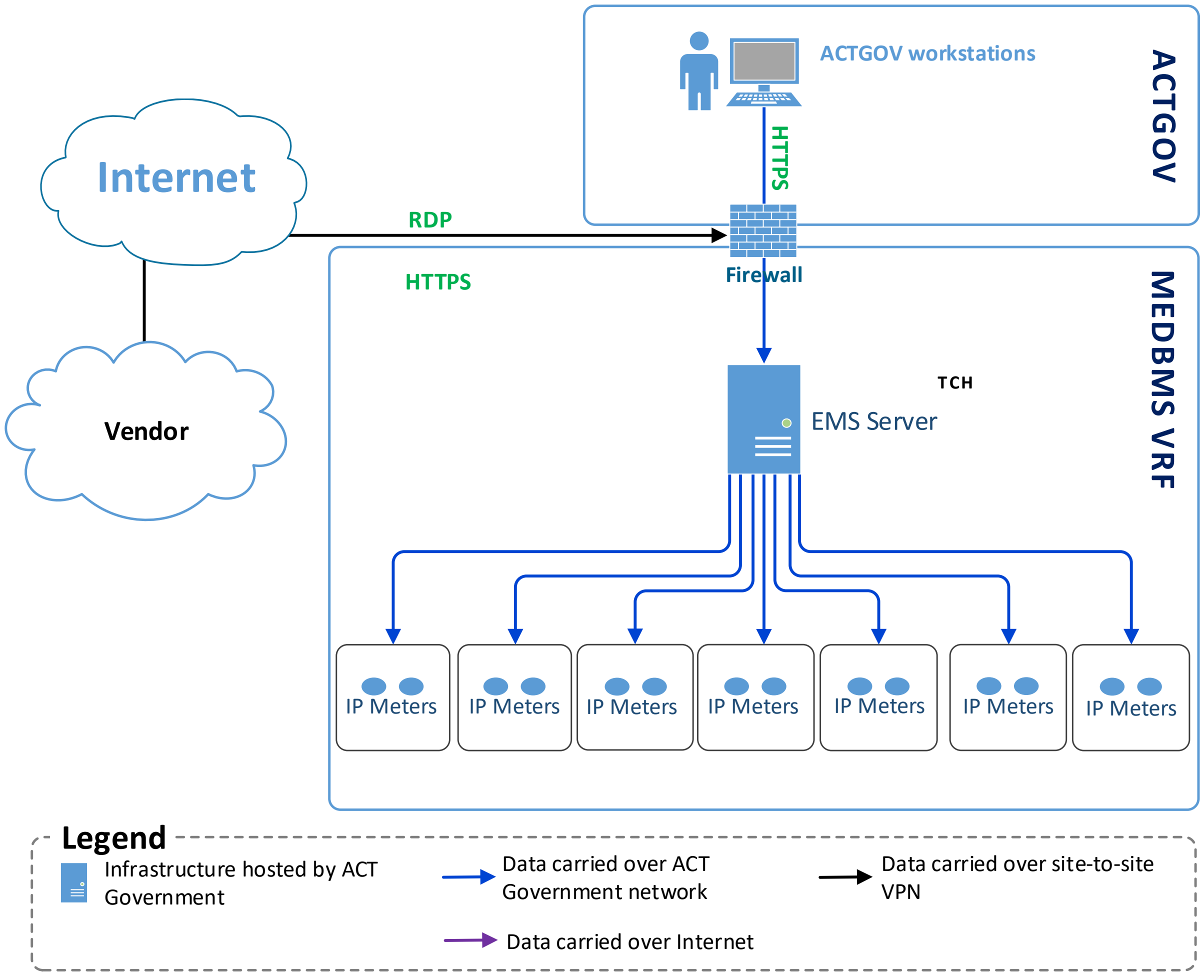
This system is designed to achieve energy efficiency by optimizing processes by analysis and reporting of granular energy use by individual pieces of equipment. EMS server provide the ability to remotely monitor electrical, gas, water and other utility-consuming equipment; gather detailed, real-time data for each piece of equipment via polling of IP based meters; and generate intelligent, specific reporting, enabling real-time guidance on finding and capturing the most compelling savings opportunities.

IP meters send monitoring data captured by controllers and sent to appliance. If the server is not available, the data will be stored by the devices for a pre-configured time and resent to the server when it is back online;

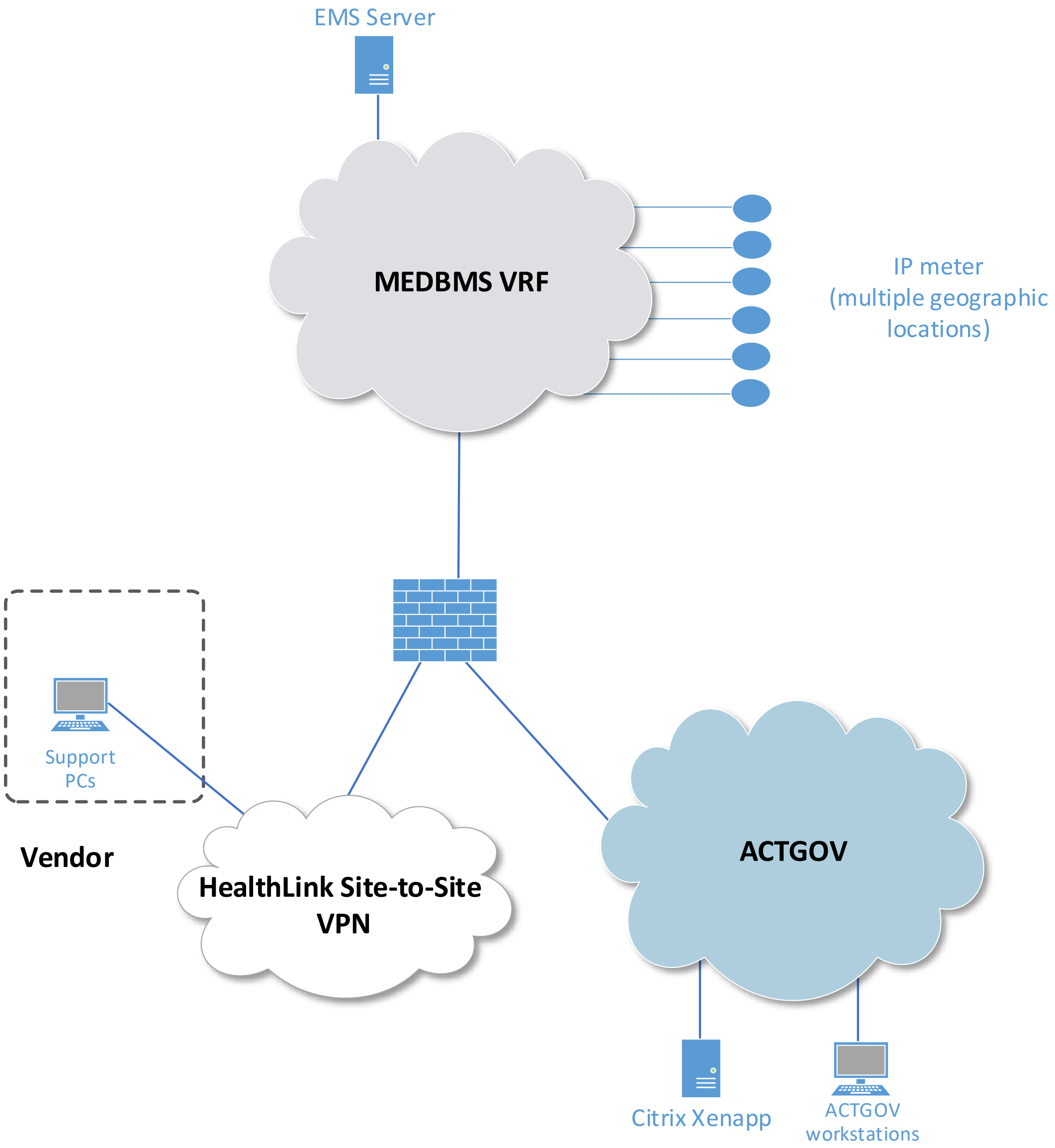
Control & Electric uses a proprietary application to monitor power consumption across TCH;

The IP power meters (e-Meters) will pole once every 15 min this will be sent via BACnet/IP, Modbus/IP to the Control & Electric appliance housed in the TCH data centre. The server will operate within the existing MEDBMS VRF and will be accessed either via workstation within this VRF or via an ACTGOV workstation configured for access through the firewall. Control & Electric will require remote access for administration and maintenance issues via a Citrix XenApp.

5.1 Technology architecture



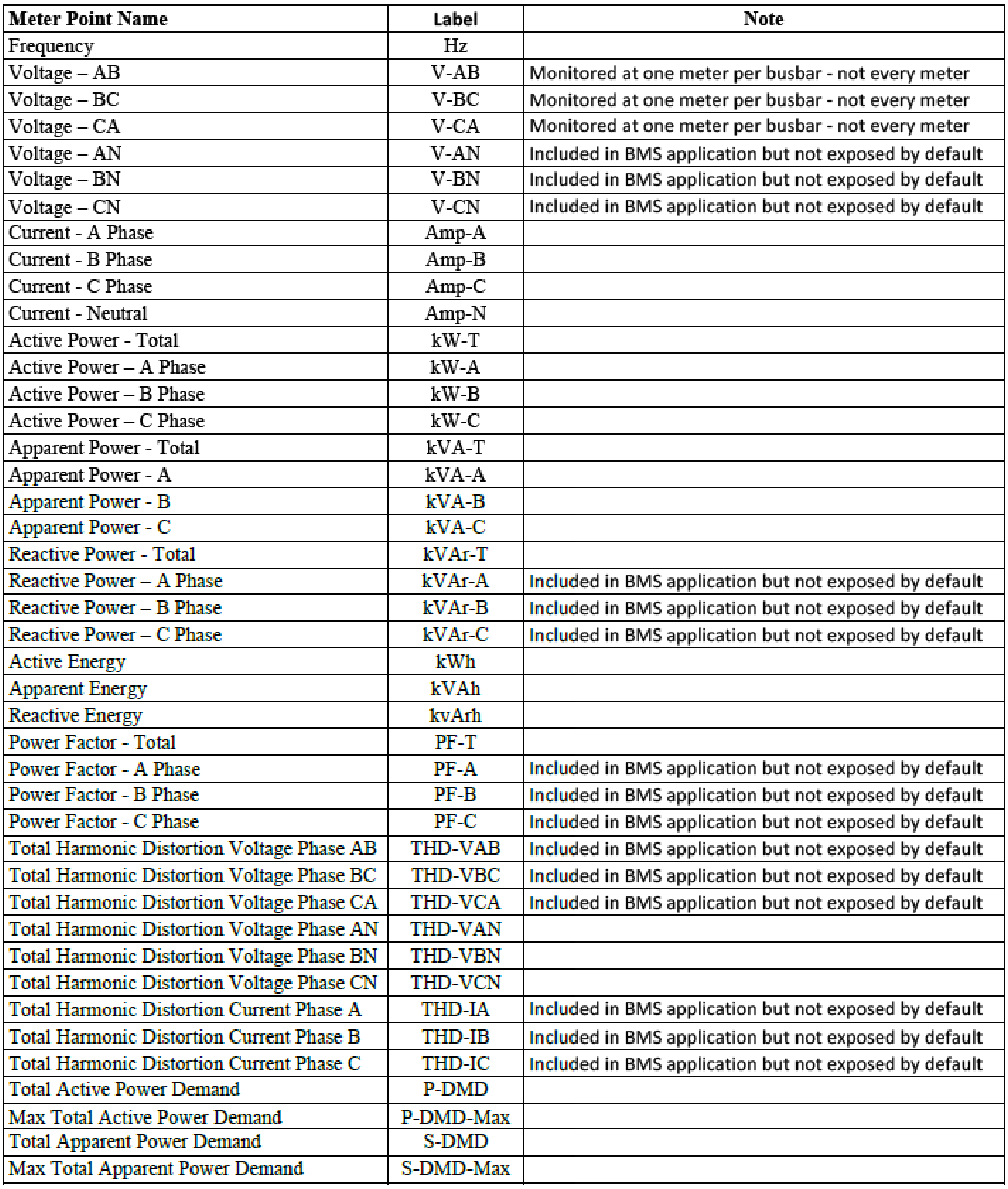
5.2 Network architecture



5.3 Data architecture

The Data stored in the local hard drive within the is capable of capturing the following parameters

Data is copied manually at regular frequency by IMM team. Accessed by ACT Gov pc and stored in the form of text or CSV file and used to IMM



Meter Point Name	Label	Note
Frequency	Hz	
Voltage – AB	V-AB	Monitored at one meter per busbar - not every meter
Voltage – BC	V-BC	Monitored at one meter per busbar - not every meter
Voltage – CA	V-CA	Monitored at one meter per busbar - not every meter
Voltage – AN	V-AN	Included in BMS application but not exposed by default
Voltage – BN	V-BN	Included in BMS application but not exposed by default
Voltage – CN	V-CN	Included in BMS application but not exposed by default
Current - A Phase	Amp-A	
Current - B Phase	Amp-B	
Current - C Phase	Amp-C	
Current - Neutral	Amp-N	
Active Power - Total	kW-T	
Active Power – A Phase	kW-A	
Active Power – B Phase	kW-B	
Active Power – C Phase	kW-C	
Apparent Power - Total	kVA-T	
Apparent Power - A	kVA-A	
Apparent Power - B	kVA-B	
Apparent Power - C	kVA-C	
Reactive Power - Total	kVAr-T	
Reactive Power – A Phase	kVAr-A	Included in BMS application but not exposed by default
Reactive Power – B Phase	kVAr-B	Included in BMS application but not exposed by default
Reactive Power – C Phase	kVAr-C	Included in BMS application but not exposed by default
Active Energy	kWh	
Apparent Energy	kVAh	
Reactive Energy	kvArh	
Power Factor - Total	PF-T	
Power Factor - A Phase	PF-A	Included in BMS application but not exposed by default
Power Factor - B Phase	PF-B	Included in BMS application but not exposed by default
Power Factor - C Phase	PF-C	Included in BMS application but not exposed by default
Total Harmonic Distortion Voltage Phase AB	THD-VAB	Included in BMS application but not exposed by default
Total Harmonic Distortion Voltage Phase BC	THD-VBC	Included in BMS application but not exposed by default
Total Harmonic Distortion Voltage Phase CA	THD-VCA	Included in BMS application but not exposed by default
Total Harmonic Distortion Voltage Phase AN	THD-VAN	
Total Harmonic Distortion Voltage Phase BN	THD-VBN	
Total Harmonic Distortion Voltage Phase CN	THD-VCN	
Total Harmonic Distortion Current Phase A	THD-IA	Included in BMS application but not exposed by default
Total Harmonic Distortion Current Phase B	THD-IB	Included in BMS application but not exposed by default
Total Harmonic Distortion Current Phase C	THD-IC	Included in BMS application but not exposed by default
Total Active Power Demand	P-DMD	
Max Total Active Power Demand	P-DMD-Max	
Total Apparent Power Demand	S-DMD	
Max Total Apparent Power Demand	S-DMD-Max	

5.4 Building Infrastructure

The IP Meters will connect directly to the EMS head-end server infrastructure. The IP Meters shall be located on the controlling distribution boards of the utilities and provide connectivity between the meters and the EMS server via copper ethernet connections to the nearest switch/communications room. They will record data locally and deliver information when polled by the head-end infrastructure.

The IP Meters will support the following functionality:

- Capable of supporting IP VLANs;
- Connect via a copper Cat6$_A$ Ethernet data port; and
- Be compatible for polling by the incumbent EMS server
- Capable of leveraging POE+ where applicable; and
- Shall be designed with components that will support layer-3 IP network and are IP addressable.

6. Network Requirements

6.1 Wired Network

The Health Directorate has been provisioned with a network architecture that is compliant with the MGN to support Health critical systems. The architecture mitigates against the risk of a single network component failure resulting in the loss of connectivity for these Health systems.

The network has been provisioned with 10 Gbps OM4 multimode fibre connections between the access layer Floor Distributor switches and aggregation layer Building Distributor switches. Similarly, 10Gbps or greater OS2 single mode fibre connections are provisioned between BD and Campus Core switches.

Each FD switch is connected to both the BD switches using Multi EtherChannel (MEC) feature. Both the links within a MEC are active with traffic traversing across both the links. In the event of a link failure, the network traffic continues to access the Health systems based in the data centre over the remaining active link.

Any IP based systems shall support the following:

- Capable of connecting to the Ethernet switches over Cat 6_A cabling;
- Capable of leveraging POE+ where applicable; and
- Shall be designed with components that will support layer-3 IP network and are IP addressable.

6.2 Wireless Network

The wireless head-end infrastructure has been implemented to support (802.11ac/ax, Bluetooth & IR beacon) wireless services required in various ACT Health buildings e.g. Wireless Nurse Call handsets. A wireless services block has been created that hosts the head-end wireless network infrastructure in two separate locations, TCH Core Node room A and Core Node room B. Each location includes wireless and security components to support the wireless connectivity required from each site.

Where appropriate the head-end infrastructure currently implemented should be leveraged for the wireless network architecture within Health Directorate buildings.

The site based wireless infrastructure will consist of WAPs, which will be provisioned by the Shared Services ICT. A wireless survey is conducted by an external organisation that specialises in the wireless networks. This survey outlines the location of WAPs within the building. The Health Building Management and Control Systems that require wireless network access are expected to leverage these WAPs.

7. Vendor Requirements

The following requirements are expected to be supported by the BMCS system.

7.1 Installation Support

The Health critical systems have an element of complexity that necessitates suitable planning for the installation, configuration, integration with other systems and testing. These systems also include a number of vendors that need to be coordinated to achieve optimal implementation results and the completion timeframes.

The vendor must identify and document the following:

- Installation and configuration processes;
- Mechanisms for integration with other systems;
- Tools available to verify the approved system implementation;
- Tools available to assist in system fault diagnosis;
- Processes to upgrade the system software;
- Processes to upgrade and/or replace hardware; and
- Willingness to work with the incumbent headend system support vendor to integrate new edge equipment.

7.2 Training

The Health critical systems are implemented with an objective that these systems will assist staff with the quality of care they provide to consumers. This implies that in addition to installing, customising and testing the systems, it will be necessary to have relevant core processes and procedures in place to achieve the expected results. Therefore, staff will need training in the use of the systems that will be installed at the site.

The vendor must identify and document the following:

- Initial user training requirements to effectively use the system;
- Initial system administrator training requirements to effectively manage the system ; and
- The amount of ongoing training for the users and system administrators.

7.3 Backup and Recovery Capability

There is a requirement for having consistent and reliable backups for the systems. The systems shall backup key information for recovery purposes in the event of a catastrophic appliance failure. The scope for the backups includes, but not limited to the following:

- All the folders, files and databases required to recover the system to a state prior to the appliance failure;
- System configuration files;
- System log files; and
- Operating system.

The vendor must identify and document the following:

- The frequency of the backups;
- Whether full backups or incremental backups will be completed;
- How the system will be recovered from the data that has been backed up; and
- The length of time taken to recover the system from the backup data and for the system to be ready for production.

7.4 Logging Capability

The system must have an automatic logging capability (i.e. recording all data), which complies with the Shared Services ICT requirements and good governance. At a minimum, the following logging capabilities must be provided by the system:

- The logs must be available for auditing and problem isolation;
- Access to logs must be restricted to authorised personnel. Access should be logged and must be auditable;
- Logs must include a date and timestamp;
- Logs must record various elements and sufficient detail that explain the event;
- The systems must have adequate storage space for logs; and
- The system must be capable of forwarding logs to a separate central log management server.

7.5 System Monitoring Capacity and Capability

An effective monitoring and event management strategy is crucial to a successful deployment. The existing Health Directorate network infrastructure is monitored by a centralised monitoring system.

The vendor and the Directorate must be able to monitor the systems mentioned in this document. The monitoring strategy must identify and document the following key points:

- Details of how the system will be monitored;
- The components that will be monitored. At a minimum, it is expected the following components will be monitored:
  - Resource utilisation such as CPU and memory utilisation;
  - Disk status including available disk space and other threshold information;
  - Replication activity including status whether or not replication is running and the state of synchronisation; and
  - Security information including access to the system.
- Monitoring and analysis tools available to monitor the system;
- Any diagnostic tools available to assist with problem isolation and resolution;
- Tools available to support system usage statistics to assist with cost allocation to different business units;
- Triggers that will raise an alarm or an event notification when monitoring the system; and
- The personnel responsible for responding and resolving the problem which raised the alarm including the vendor’s escalation process.

7.6 Management Capability

The system management will form a critical aspect for the ongoing optimal operation of the security systems discussed in this document.

The systems must support the following management capabilities:

- Local site management; and
- Remote management as required.

In order to plan for the system management, the following requirements must be identified and documented:

- The ongoing resource requirements for effective system management;
- Post implementation system validation requirements whether manual or automated; and
- The frequencies of ongoing system validation to ensure business units maintain a high level of confidence in the system operation and performance.

Key Performance Indicators (KPI) will need to developed and formally agreed to, ensuring the system is performing in compliance with the expected criteria. These KPIs and associated formulas will be developed collaboratively between Health Directorate and the vendor.

7.7 Capacity Strategy

In order to manage current and future business requirements in a cost-effective manner, capacity management forms a critical component of the system life-cycle. The security systems must provide adequate capacity to meet current anticipated requirements. However, the vendor must identify and document a capacity strategy that provides details of:

- The capacity and scalability of the proposed system including the:
  - Number of concurrent "transactions" supported by the system
  - Amount of CPU, memory and other system parameter utilisation initially expected from the proposed system;
- Strategies to provide additional capacity as the business requirements increase the requirements for the system; and
- Provide a Total Cost of Ownership (TCO) analysis for a 5 year period.

7.8 System Roadmap

The vendors shall provide a technology roadmap that outlines short-term and long-term direction of the technology solution that is being provided. The information will assist Health Directorate in understanding the technology direction a product is expected to take over a period of time.

The roadmap must identify and document the following:

- The product that will be the focus of the roadmap. Each component in the tiered architecture potentially may have a different product cycle;
- The features that will be addressed by the roadmap; and
- The timelines for any technology changes.

7.9 Network Time Protocol

Network Time Protocol is essential for the systems to maintain consistent time with other devices within an enterprise. The consistent time management with other devices assists with event correlation between different machines.

As various systems are integrated at the Health Directorate, in the event of problem resolution, consistent clock on the appliance/server can be crucial. The Health systems shall support NTP to synchronise appliance/server time with the Shared Services ICT NTP server.

7.10 Maintenance & Support

Based on the criticality of the system, a 24 x 7 system vendor support will be required. The support personnel must be based in Canberra. The vendor will identify and document the following:

- The maintenance and support model, including ongoing license costs; and
- Schedule of fees for any other costs that may be applicable.

7.11 System Testing

The Health security systems must undergo extensive testing prior to release into the production environment. The vendor responsible for each system must provide a detailed test and integration plan to Shared Services

ICT for review prior to commencement of testing. The test scenarios must outline the tests that will ensure the system complies with all the functional requirements.

At a high level the test and integration plan must identify and document the following:

- Functionality testing. Provide comprehensive test cases which will verify the functionality provided by the system;
- GUI software testing. In the event the system provides a GUI interface, the test cases must be provided to verify functional aspects of GUI testing;
- Security testing. These test cases must verify compliance with the access restrictions to the system;
- High availability testing. These test cases must verify failover capability of various components of the system;
- Capacity testing. The test cases must outline the capacity testing methodology. Additionally, if any automated tools are available, these must be included in the test cases; and
- Integration testing. These test cases must detail testing that will be conducted to ensure integration with other systems complies with the business requirements.

7.12 Business Unit Validation

In addition to system testing as mentioned in the previous section, there is a requirement for the client to review and validate that the system implementation complies with the business unit’s needs.

The validation by the business unit should include the following:

- Develop and document a test plan to validate the business requirements that have been agreed with the users;
- Review the test results from the vendor system testing and provide feedback to the vendor via the Shared Services ICT project manager;
- Conduct functional and non-functional testing to ensure the system complies with the business needs;
- Perform system performance validation; and
- Provide a report of the test results to the Shared Services ICT project manager.

7.13 Software

The operating software needs to be maintained at no greater than n-1 where n is the latest version.

All software updates shall be performed by the contracted company. The updates should be pre-tested in the Shared Services ICT provided TEST environment, where available.

All updates to the live production environment shall be done strictly under the Shared Services ICT approved change control methodology.

7.14 Licensing

An enterprise approach should be followed for any license requirements. Consideration should be given to the annual licensing requirement, allowing for a single purchase of a larger quantity of licences thereby reducing individual license costs.

A centralised enterprise approach will provide an additional benefit of avoiding any licensing issues during commissioning of a system.

The vendors should provide the Health Directorate with the licensing requirements for their systems.

7.15 Remote Vendor Access

The currently deployed infrastructure forms a conduit on which communication with the external parties will traverse. Remote Vendor Access (RVA) relies on the various elements within the network to facilitate the required communications path. This means access policy alterations i.e. firewall changes, will be required at the inbound access point to the network.

RVA is provided on case-by-case basis to the vendor equipment as required by each project in compliance with the remote vendor access policy.

Any vendor with existing remote access to their head-end infrastructure will not require additional access. However, the vendor will need to request any additional access to new infrastructure.

7.16 Model of Care

The Canberra Hospital and Health Services will rely on various information technology based systems to provide the Model of Care (MoC) to the patients. In order to support the MoC, the business units, in consultation with the vendor, will develop test cases to ensure the system complies with the functionality expected by the user. In addition to the test cases, a compliance check-list must be documented for system vendor compliance.

At a minimum, these test cases should ensure the following criteria are addressed:

- The functional requirements for the system are tested. For example, if a duress button is pressed, what notifications are expected to take place;
- The expected performance of each system is tested. For example, if a duress button is pressed, what is the timeframe for the notifications to be received by the responders; and
- Non-functional requirements are tested.

Appendix A

Reference

Standards and Compliance

- All Australian Standards that are relevant to the Building Management and Control System.

Glossary of terms

Term	Definition
ALN	Automation Level Networks
BACnet	An industrial protocol (typically building control) operating on RS485 or Ethernet
BD	Building Distributor (room)
BMCS	Building Management and Control System
BMS	Building Management System
C&E	Control & Electric - Application reseller / support vendor
FD	Floor Distributer
EMS	Energy Management system
GUI	Graphical User Interface
ICT	Information & Communications Technology
IP	Internet Protocol
KPI	Key Performance Indicator
MLN	Management Level Networks
MEC	Multi Ethernet Channel
Modbus	An Industrial protocol (typically for A/C) operating on RS485 or Ethernet
NTP	Network Time Protocol
OM4	Optical Multimode fibre type 4
OLE	Object Linking and Embedding
OPC	OLE specifications for communicating real-time data from data acquisition devices such as PLCs
OS2	Optical Singlemode fibre type 2
RVA	Remote Vendor Access
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access protocol, is a protocol specification for exchanging structured information in the implementation of web services
TCH	The Canberra Hospital
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAP	Wireless Access Point
XML	eXtended Mark-up Language

Table 2: Glossary

Amendment history

Version	Summary of Changes	Author	Date
2015.0.1	Initial version	David Richards	04/03/2015
2015.0.2	Peer Review	Nitin Saxena	05/03/2015
2015.0.3	Accept review changes & additions to Glossary	David Richards	05/03/2015
2015.0.4	Minor updates to Standards section	Nitin Saxena	05/03/2015
2015.0.5	Incorporate feedback from the business	David Richards	06/03/2015
2015.0.6	Incorporate further feedback	Nitin Saxena	10/03/2015
2015.1.0	Included updated vendor requirements	Nitin Saxena	16/04/2015
2015.1.1	Change ‘Edge Devices’ to ‘Endpoint Devices’ based on feedback	Nitin Saxena	27/04/2015
2020 0.1	Updated EMS content	Raj Mohan	21/02/2020
2020.1.0	Updated and ready for release	David Richards	30/03/2020

Table 3 - Amendment History