Property Services

Design Standard

Volume Eight: Building Management Systems

Issue 1

December 2016

RMIT University

Design Standards – Volume Eight Building Management Systems

December 2016

Version Control

This document will be updated and re-issues to reflect approved change to content, and is subject to version control. The version record and status is documented below

Document Change History [1]:

Version	Date	Author	Comments
1.0	13/12/2016	Property Services	Approved issue of standard

Owner

The overall responsibility for these standards resides with RMIT University Property Services

Review

This Document is reviewed every 12 months.

[1] Printed copies of this document are considered uncontrolled and may not reflect the most recent revision

Table of Contents

1. Introduction

1.1 Background

This document details the minimum RMIT design requirements for electronic security systems. It forms part of the suite of RMIT Design Standards set out below. All volumes of the standards are available on the RMIT Property Services Design Standards web page.

- Volume One Introduction
- Volume Two Architecture and Planning
- Volume Three Electrical Systems
- Volume Four Fire Protection Systems
- Volume Five Hydraulic Systems
- Volume Six Mechanical HVAC Systems
- Volume Seven Vertical Transportation Systems
- Volume Eight Building Management Systems
- Volume Nine Electronic Security
- Volume Ten Communications
- Volume Eleven Audio Visual
- Volume Twelve Landscape
- Design Standards Checklist

This document should be read in conjunction with *Volume One - Introduction*, which provides context on the organisational and governance arrangements that apply to the design and construction of new facilities and describes the key principles that underpin the requirements of the Standards:

- Safety
- Accessibility
- Innovation
- Student Experience
- Maintainability and Serviceability
- Modularity and Standardization
- Reliability
- Compatibility
- Sustainability
- Heritage
- Life Cycle
- Precinct Wide Solutions

Whilst this document provides the design philosophy and minimum RMIT ITS requirements, it is the responsibility of the service provider to ensure any system complies with RMIT ITS Design standards and these can be requested via the relevant RMIT Program Manager. This document is not intended to replace the significant engagement required with both RMIT Facilities & Asset Management team and RMIT ITS via the usual RMIT procedures.

1.2 Purpose

The purpose of this brief is to set out the minimum requirements for design of building management systems (hereafter called BMS) across all RMIT campuses. Furthermore, the brief seeks to recommend open systems standards that will deliver consistency and standardization across all RMIT campuses.

Any design aspects not specifically addressed by this brief shall be identified by the consultant during the design process and shall be brought to RMIT University's attention for resolution.

1.3 Intended Audience

This document is for all those involved with the design, installation, integration and maintenance of building management systems, including:

- Mechanical engineers
- Controls engineers
- Specifying engineers
- Control systems programmers
- System integrators
- Controls technicians
- Architects -provision of location for equipment (now and in future expansion) and cable pathways
- Electrical / Communication consultants -provision of requirements for horizontal and vertical cable pathways, IT field outlet requirements and power

1.4 Demonstrating Compliance with the Standards

Designers and specifiers are required to confirm compliance and to justify any proposed deviations by completing the Design Standards Checklist (see below).

All deviations must be approved by RMIT prior to commencing design. Unless a robust justification is provided for deviations from the standards, it is unlikely that approval will be given. Design Standards compliance is achieved through completion of the Design Standards Checklist and endorsement by RMIT of any proposed non-compliances.

BMS Design Standards Checklist		
Project Name		
Responsible entity		
Engineer		
Date		
Item	**Compliance Description**	**Comply (Initials)**
1	Approved hardware	
2	Approved installers	
3	ITS Requirements	
4	BMS Systems integration with other building services systems	
5	BMS Equipment (ALN/FLN)	
6	BMS Field hardware (Sensors, transmitters, valves etc)	
7	BMS Design documentation	
8	BMS Software & control	
9	BMS & integrated EMS Functions (metering)	
10	BMS UPS Requirements	

1. BMS Design Standards - General

1.1 Definitions of Terms

This document uses a number of terms which may be misinterpreted, the following table defines the use of these terms.

Term/Abbreviation	Description
BMS	Applies to all or part of a control & monitoring system including field controls, sensors, actuators, global integration hardware, computers, servers and associated software. Alternate descriptions include DDC, BAS, BMCS
GUI	Graphical user interface – any software element that enables users to view and/or control elements of a BMS
Tier 1	Products and installers that are considered for use within major projects of high complexity, value and risk. These are generally new large buildings (> 5000 m^2) or buildings with complex mechanical systems and needs.
Tier 2	Products and installers that are considered for use within medium sized projects of medium complexity, value and risk. These are generally small-medium sized buildings (< 5000 m^2 GFA) with simple mechanical systems and needs. This tier also includes extensions to buildings where integration to existing mechanical and control systems is required.
Tier 3	Products and installers that are considered for use within simple projects where small expansions and augmentations are planned to existing mechanical systems within existing buildings. Such projects might include supplementary air-conditioning units or central plant.
Field level network (FLN)	Controllers that are often installed local to the equipment which they control (e.g. fan coil units, variable air volume terminal units).
Automation level network (ALN)	Controllers that are generally (although not exclusively) used to provide integration of sub networks of FLN controllers, and to deploy “global” control strategies.
Field interface devices (FID)	Devices such as sensors, actuators or meters that may be deployed in a network as a means of installation and/or costs efficiency.
BMS PC Server	Computer servers that marshal and monitor a large range of BMS automation and field level hardware, as well as the BMS data points connected to them. (Note, BMS controllers can operate as both both clients and servers so care needs to be exercised when referring to vendor specific servers)
BMS Data Object (point)	Most commonly refers to a hardware “point” physically connected to a BMS field level controller (e.g. temperature sensor, control output etc). Software objects refer to time schedules and other internal functions. Most objects are defined by the BACnet standard and will appear as such within the RMIT BMS system
Telecommunications Outlet (TO)	RJ45 Ethernet outlet that connects to the RMIT data network

2. BMS Design Standards Philosophy

Allows RMIT to determine which products, vendors and installers are qualified to provide systems and installation within the University's built environment.

Defines the technical standards & performance expectations.

Enable integration of all approved BMS products into a common graphical user interface using industry standard protocols.

Provide a framework within which any approved BMS vendor may submit prices and be assured that all clauses and performance expectations remain constant for all manufacturers and installers.

Provide a process through which manufacturers and vendors may have BMS hardware approved for connection to the RMIT IT network.

Encourage innovation and improvements to BMS systems through a defined process of approval overseen by RMIT.

Encourage a dialog between vendors, installers, RMIT management and the student body in regards to building services controls technologies and integration.

2.3 Acceptable Products & System Selection

Designers must only include features and functions that are part of systems or components provided by RMIT's preferred BMS providers. Refer to the RMIT program manager/Facilities team member for details.

2.4 BMS Hardware & Interoperability

The following paragraphs provide a summary of the most important features and functions that must be provided for all systems installed at any RMIT property.

2.4.1 BMS Communications

BMS systems shall be compatible with the BACnet industry standards. Deviations from the standards are not acceptable. Hardware & software that use proprietary communications solutions shall not be deployed.

FLN controllers shall communicate using either BACnet MS/TP or BACnet IP

ALN controllers shall communicate using BACnet IP

FID shall communicate using either BACnet MS/TP or MODbus RTU

GUI devices shall communicate using BACnet IP

2.4.2 Open Systems and Interoperability

BMS hardware shall be deployed by the installer to allow simple integration with other vendors' controls, software and GUI. Refer to section 3 for more detail regarding BACnet integration.

All hardware inputs and output objects shall be exposed for integration by standard industry tools.

Set-points, dead-bands, time schedules, holidays, loops shall have all configurable objects exposed for integration by standard industry tools.

All exposed BACnet objects shall be named (using the “Description” field or similar) in accordance with the RMIT naming conventions to enable simple comprehension by integrators of the location and purpose of the object.

All BACnet objects shall enable both READ and WRITE.

BMS hardware shall not require the use of any proprietary software tools in order to view and integrate the objects within it.

Non-autonomous input/output expansion modules shall only be deployed where every object is fully mapped to its host controller and the same BACnet visibility is available as that provided by an ALN or FLN controller. Such expansion modules may not use proprietary protocols without the prior approval of RMIT Property Services, even when such hardware may have been previously deployed prior to these BMS design standards being published.

3 BMS Field Hardware

3.1 Field Sensors, Transmitters & Actuators

3.1.1 Passive Temperature Sensors

Installers shall deploy passive RTD type temperature sensors that are compatible with the curves preferred by RMIT.

3.1.2 Active Transmitters

Installers shall deploy active transmitters that utilize a standard 24VAC power and 0-10VDC signal. Other variations shall be considered for approval on a project by project basis.

3.1.3 High Level Transmitters (Intelligent)

Where networked devices are used for sensing, installers shall deploy only BACnet MS/TP or MODbus RTU. Other communications methods shall be considered for approval on a project by project basis.

3.1.4 Actuators – Binary

All binary actuators shall be isolated from the BMS controller output by a low voltage, 24VAC relay with appropriately sized contacts to pass at least twice the running current of the driven device.

Where floating control is deployed utilising two binary outputs, wiring may be made directly to the BMS controller outputs provided the switching devices have twice the current capacity of the FLC of the driven device and the inrush current of inductive loads does not exceed the maximum ratings of the control device.

3.1.5 Actuators – Analog

All modulating actuators shall be powered by 24VAC and positioned using a 0-10VDC signal.

All actuators shall be selected such that their force or torque exceeds the project requirement by at least 30%.

Installers shall only deploy those actuators that are specified on the RMIT approved devices list.

3.2 Water Control Valves

3.2.1 Valves

Control valves shall be either plug or rotary, and shall be sized with appropriate actuators to ensure that there is more than sufficient close off to ensure isolation when required.

Valves shall be sized such that the pressure drop and authority ensures good control under all conditions and flows. Authority must not drop below 0.2 or exceed 0.5.

Installers shall deploy only valve brands, models and bodies that are specified on the RMIT approved devices list.

3.3 Valve & Damper Actuators

3.3.1 Actuators

Actuators shall be 24VAC powered and sized to provide more than sufficient torque to drive the valve or damper to which they are attached.

Water control valve close off pressures must be maintained according to the mechanical services specifications in force for the particular project.

Damper actuators must be spring return for all fire control applications unless otherwise specified.

Actuators shall be positioned by a 0-10VDC signal for all major AHU and central plant applications. Where terminal plant is controlled (e.g. VAV or FCU) RMIT accept that floating control of valve actuators is more economically viable.

Where floating control of valve or damper actuators is deployed, installers shall either:

1…Provide a hardware feedback mechanism to guarantee positioning, or

2…Deploy software that provides a regular “Reset” of the positioning calculations at least once per day.

Notes:

Reset shall include the driving of the actuator in one direction for at least twice the calculated drive time of the actuator. Floating control shall NOT be deployed on valves larger than 20mm or on any damper actuators where positive positioning is required.

Damper actuators that are to be driven to only two positions may deploy floating control.

4. Integration of Building Services Hardware

4.1 Definitions of Terms

4.1.1 BMS Integration

The exchange of data between compatible BMS hardware devices of different manufacturers.

4.1.2 Open Systems (HVAC)

Hardware and software solutions that provide a standardized method of communication to achieve data exchange.

4.1.3 BACnet

A standardized open system framework for building management systems managed by ASHRAE.

4.1.4 MODbus

A standardized open system framework for industrial, energy and building management systems (see Modbus.org).

4.1.5 E-BMS

Enterprise BMS – A central system to standardize BMS data integration, display, collection and retrieval for all approved BMS hardware installed at RMIT properties.

4.1.6 GUI

Graphical User Interface – A computerized interface that presents BMS object data in a graphical, simple to understand format. Vendor specific GUI's are often reliant on proprietary software and/or BACnet to read/write data from BMS field and automation level controllers.

4.2. Intent for Integration of BMS & other Services Systems

4.2.1 Independence and Intent

Integration service providers may be independent from BMS installers

The intent is to enable RMIT the freedom to integrate any approved vendor's hardware with the (future) common enterprise BMS system (E-BMS) and associated data servers, and also to integrate different vendor's equipment with each other and thereby avoid duplication or early obsolescence of BMS equipment which in every other respect is within its lifecycle.

4.2.2 Small Projects

Small projects that have an expansion scope and may not be performed by the original installer are still required to be integrated to the common head end GUI (E-BMS or proprietary) to enable RMIT visibility of the system.

4.3. Standardized Deployment

4.3.1 Limitations

Integration service providers shall deploy only approved, standardized RMIT solutions in all activities.

Integration service providers shall NOT install any translation hardware or software without prior approval from RMIT property services.

Any translation devices or software that does not comply with standard BACmet or MODbus implementations and that is opaque to other integrators shall not be acceptable.

Integration service providers shall guarantee data exchange between BMS hardware of similar or differing vendors and generations.

4.3.2 Graphical interfaces

Integration service providers shall guarantee data storage, retention, retrieval and display from BMS hardware of similar or differing vendors and generations

4.3.3 Alarms

Integration service providers shall guarantee alarm annunciation and distribution from BMS hardware of similar or differing vendors and generations

4.3.4 Data Sharing

Integration service providers shall guarantee read and write data sharing with other RMIT systems from BMS hardware of similar or differing vendors and generations

4.3.5 Hardware Decommissioning

Integration service providers shall provide decommissioning of all redundant BMS Hardware that has been replaced as part of the defined scope of works.

4.3.6 Software Decommissioning

Integration service providers shall perform software maintenance tasks associated with the decommissioning of BMS hardware, including:

- Removal of software references in databases
- Removal of software references in graphical user interfaces
- Removal of software references in all other systems
- Maintenance of points lists, drawings and manuals.

- Liaison with BMS Hardware Vendors & Installers
- Integration service providers shall perform all liaison tasks with nominated BMS vendors and installers in order to obtain necessary information regarding integration.

- Service providers shall alert RMIT to any integration issues that may delay completion of the project.

4.3.7 Standard Tasks

Integration service providers shall always deliver the following as a minimum:

- Identification of all hardware and software objects to be integrated
- Validation that existing software licenses are capable of accepting these objects
- Expansion or extension to existing software licenses where necessary
- Integration of all objects to existing BMS server(s)
- Integration of selected objects to other BMS systems where necessary (global strategies etc.)
- Generation of appropriate standard BMS graphics and user interface elements
- Integration of objects with existing data collection, retrieval and display software
- Integration with alarm handling & annunciation system
- Documentation of all integrated objects and systems
- Test & demonstration of all integrated BMS objects and systems with RMIT

4.4. Integration with RMIT Software Services

4.4.1 General

RMIT deploy (or subscribe to) other solutions that do not comply with building services integration standards such as BACnet or MODbus.

Examples of such applications include Archibus and Syllabus Plus.

4.4.2 Description of Principles

BMS Integration with other database API applications both on and off campus and on or off site (including cloud hosted) shall conform the RMIT integration principles and integration reference architecture.

- ITS integration and information (I&IM) platform supports
- Batch integration
- Real time integration including API and
- Managed file transfer

4.4.3 Detailed Design

Integration shall require a detailed solution design and associated engagement including resources at a project cost.

5. BMS Based Metering Systems

5.1 Types of Metering

Metering" refers to the measurement and collection of interval data for the following variables:

- Electricity – single phase and three phase
- Natural Gas
- Thermal Energy – heating, cooling and condenser water
- Combustion Fluids – Diesel etc.
- Potable Water
- Waste/Brown Water
- Harvested Water
- Sewerage
- Recycled Water

5.2 Preferred Hardware Types

BMS installers shall deploy meter hardware that uses embedded non-volatile memory technology to record data at set intervals.

Meter hardware shall be capable of sharing data via communication networks.

5.3 Preferred Communications Hardware

Installers shall deploy interval meters that communicate using RS485 serial or hard-wired Ethernet (CAT 6A only).

5.4 Preferred Communications Protocols

Installers shall deploy BACnet MS/TP, BACnet IP, MODbus RTU or MODbus RTU.

5.5 Alternate Hardware Schemes

Installers may apply for approval to use alternate metering methods that mimic memory equipped units and redundancy.

Where such alternatives are submitted for approval, installers must satisfy RMIT that sufficient segregation between BMS and EMS functions has been provided to guarantee that failure of one system will not affect the other.

5.6 Alternate Communications Protocols

Installers may apply for approval to deploy alternate communications protocols where such a change to the Design Standard will deliver benefits to RMIT. Proprietary protocols will not be approved.

5.7 Alternate Data Storage Schemes

Installers may apply for approval to deploy alternate metering data storage schemes. Schemes that cannot demonstrate effective and secure data validation, redundancy and storage techniques will not be considered.

5.8 Data Protection

Loss of any part of a BMS system shall not affect any part of the metering data collection and storage system.

Energy data shall be protected from loss at least 3 storage locations. (Collection device, intermediate device, IT server). A backup should also be provided for the IT server database.

5.9 Data Validation & Repair

Appropriate software shall be deployed to protect against data corruption. Where utility power supply failures cause data gaps, zero readings shall be recorded.

Where faults or local power supply failures cause data gaps, appropriate software shall be deployed to re-create the missing data based on a historical analysis of the meter interval data. Alerts shall be annunciated to enable RMIT staff to validate the re-created data intervals.

6. Data Collection & Storage

6.1 Definition

Data collection refers to BMS variables (both “native” and integrated) that are measured, controlled or monitored by any part of the BMS. These variables do not include “Metering” items as outlined above in section 4.

6.2 Examples of variables

- Temperature
- Pressure
- Flow Rate
- Valve or damper Position
- Loop output
- Set Point

6.3 Collection & Local Storage

BMS systems shall provide the following minimum data storage functions:

Each ALN controller shall be fully programmable for data collection in regards to object, parameter and frequency interval. Each ALN must have capacity to collect sample data for all hardware points connected to itself and its subordinate FLN controllers at a 15-minute collection interval.

6.4 Database Storage

Each ALN will allow the automatic uploading of the collected data at times set within the ALN to both a proprietary and standard SQL database structures.

Where vendors provide proprietary databases, these databases shall provide a method for automatically exporting data to a standard SQL database structure.

6.5 Data backup

PC servers data will be backed up using the standard RMIT enterprise backup solution (“Commvault”) so the system can be restored in the event of a system failure. Vendors may also elect to provide their own data backup solutions.

Installers shall provide all necessary details regarding storage locations within servers as part of the O&M documentation.

7. BMS Installation, Enclosures, Cabling & Labelling

7.1 Space Allowance for BMS Enclosures

Space shall be allocated specifically for BMS control enclosures at all required locations, especially within mechanical plant rooms and risers

7.2 BMS Enclosures

Hardware shall be mounted in suitable enclosures and provided with oversized voltage transformers to enable future expansion of 15%

Enclosure mounted hardware shall be provided with plastic ducting or other cable tidy solutions to ensure a neat and tidy appearance.

All BMS and associated items within enclosures shall be mounted on a gear tray.

Enclosures shall contain a suitable document holder large enough to accommodate points lists, drawings and manuals.

BMS enclosures must be provided with external labels that identify the manufacturer of the hardware, the installer, building, level, location and ID number of the BMS equipment.

Each item within the enclosure must be identified with a label that details the name and unique ID of the component. *(See labelling in 6.4 below)*

Small enclosures (< 0.2 m^2) shall be either polycarbonate, aluminum or steel

Large enclosures (> 0.2 m^2) shall be aluminum or steel

Cable entry points to enclosures shall be protected with rubber grommets, plastic bushes or other similar permanently mounted cable protection methods. Each entry point shall be reasonably occupied, with spare space to allow for tracing and expansion.

7.3 BMS Equipment

Hardware shall be AC powered

All equipment connections shall be provided with removable plugs equipped with screw terminals.

Terminals must accept at least one 1.0 mm^2 cable.

Terminals shall be limited to no more than two cables.

Terminal unit controllers (FCU, VAV etc.) shall be mounted directly onto the mechanical system hardware which it controls, but shall be provided with dust protection and easy access to all connections.

7.4 Labelling of BMS and Associated Equipment

Each BMS equipment item (or related item such as transformers) shall be identified with an engraved label.

All labels must be manufactured from robust plastic and engraved.

All text must be a minimum of 5 mm height.

All labels shall be affixed using both adhesive and screws or plugs.

7.5 BMS Cabling and Termination

Notes: Refer also to Volume Three : Electrical Systems Design Standards for specific electrical design guidelines.

The following items refer specifically to BMS systems, whilst excluding Ethernet/CAT6A cabling which is documented in Volume Ten : Communications Design Standards.

7.6 Risers

Space shall be allocated within risers for BMS cabling where necessary.

7.7 Cable Classes & Types

All analog and digital sensor cabling shall be ran using twisted shielded cable of a size and type to suit the vendor's hardware.

All signal output cabling shall ran using twisted shielded cable of a size and type to suit the vendor's hardware

All binary outputs shall be connected using 0.75 mm2 (minimum) building wire where interfacing relays are used.

Multicore cables are acceptable for binary outputs, such cables shall be manufactured with each core identified.

All connections to BMS systems and associated interface devices shall be tidy and use suitable ferrules.

7.8 Cable Marking

All BMS cables shall be identified (including those on interface devices).

BMS cables shall be marked at each termination point.

Each BMS cable connection shall be marked with a suitable identification label. Handwritten labels are not acceptable.

Marking systems shall be permanent and have the capacity to include all the characters demanded by the RMIT naming conventions.

Cable marking need not include the building number where it is obvious to the observer at either end of the cable.

Where cables run between cables, the originating building number shall be included in the cable marker (i.e. where the BMS field controller resides).

7.9 Segregation & Bundling

BMS cables shall be segregated from other system functions providing enough clearance to avoid electrical interference.

All BMS cable bundles shall be grouped and clearly marked as BMS every 3 meters (minimum).

7.10 BMS Equipment Naming Conventions

FLN and ALN controllers shall be provided with one label each that uniquely identifies them within the RMIT organization. The label shall include

Building Number (“B” plus 3 characters max)

Level number (3 characters max)

ALN number (3 characters max, shall match installer drawings and points lists)

FLN number (3 characters max, shall match installer drawings and points lists)

All identifying codes shall be clearly separated using a dot.

FLN hardware input/output numbers shall always be marked with 2 digits with leading zero where necessary.

Where input/output expansion modules are used, the host address shall be inserted preceded by “X”

7.11 Controller Label Samples

Sample 1

B12.GND.1.22

Vis: Building 12, Ground Floor, ALN number one (within the building), FLN number 22 (hosted by ALN one)

Sample 2

B115.8.3.1.X1

Vis: Building 115, level 8, ALN 3, FLN 1, I/O expansion module 1

7.12 BMS Cable Naming Conventions

All sensors and controlled devices connecting signal cables shall be provided with cable marking that includes:

ALN number (2 characters max, shall match installer drawings and points lists)

FLN number (3 characters max, shall match installer drawings and points lists)

FLN hardware input/output type (2 characters), or…

FLN hardware input/output number (2 characters)

Note: Where ALN controllers provide more than one FLN network, the character “N” should be inserted prior to the FLN. Network “1” may be omitted where is it deployed as the default.

All identifying codes shall be clearly separated using a dot

FLN hardware input/output types shall be as follows (regardless of the manufacturer's preferred naming which may vary slightly):

UI : Analog/Universal input

BI : Binary/digital input

UO : Analog/universal output

BO : Binary/digital output

Notes: Where two BO points are used to create a floating analog output, these shall be marked as BO

Multiplexed input points shall be marked as UIxMIy

Multiplexed output points shall be marked as UOxMOy

Power supplies to devices shall be clearly marked with the originating enclosure number and the polarity (A or N)

7.13 Cable Marker Samples

Sample 1

1.22.AI.3

Vis: ALN 1, FLN 22, Analog Input 3

Sample 2

3.N2.15.BO.2

Vis: ALN 3, Network 2, FLN 15, Binary output 2

8. BMS UPS Systems

8.1 UPS

This section describes the deployment of UPS systems for BMS related applications only. It does NOT cover UPS systems for any other purposes.

8.2 Power Backup Design

BMS designers & installers shall ensure that any BMS hardware required to maintain its status during failure of the mains power supply shall be provided with a backup power supply.

BMS installers shall utilize RMIT UPS systems where they exist. Where a UPS is required for the BMS solution, but no RMIT UPS system exists, installers are to refer to property services engineers prior to providing their own, independent, non-approved UPS system.

Designers shall liaise with RMIT to ensure that the BMS makes use of any existing large scale UPS solution.

Where no UPS exists, the supply of this shall be the responsibility of the electrical services contractor.

8.3 UPS Power Supply Sizing & Alerts

BMS hardware shall fitted with a communications connection to a power backup solution using BACnet of MODbus.

The UPS solution shall be incrementally sized according to the required BMS load and be integrated to the BMS such that status changes or failures of, or alerts from the backup solution are always transmitted to the BMS. The minimum indications from UPS systems shall be:

- Mains power status
- UPS output power status
- UPS failure
- Battery status

8.4 Other Equipment

Items controlled by the UPS-backed BMS equipment shall also be provided with backup power where necessary for operation during mains power failures.

9. BMS Embedded Software & Control Strategies

9.1 Control Strategies

9.1.1 Standard Control Strategies

Installers and BMS programmers shall request copies of standard control strategies from RMIT prior to commencing the programming of the system. RMIT intend that simple mechanical items (such as FCU or VAV) be programmed and controlled in a uniform way to enable easier service and integration across the entire campus.

9.1.2 Energy Optimization & Global Strategies

Installers and BMS programmers shall deploy algorithms to minimise energy consumption, and shall ensure that set points and dead-bands are programmed in accordance with current RMIT strategies.

Heating and cooling call strategies must be discussed with RMIT prior to deployment to ensure that new mechanical works integrate without disrupting existing energy profiles and sequences whilst accommodating changed heating and cooling loads.

9.1.3 Time Schedules & Occupancy Control

Time Schedules

Where time schedules are deployed to initiate equipment, they shall be set to times and dates in line with RMIT operating times for the building as defined by Property Services

Occupancy Control

Where occupancy detection strategies are deployed as part of the project, BMS installers shall provide graphical indication of the initiating system's status for each zone.

9.1.4 Optimisation & Global Control Strategies

Optimization

BMS installers shall ensure that all control strategies are optimized to minimize energy consumption whilst delivering stable, comfortable conditions.

Global Control

BMS installers shall ensure that global control strategies are robust and do not fail or cause any loss of control following failure of any node.

BMS installers shall integrate with all relevant global control strategies, for example:

- Ambient lockouts
- Common-set points
- Maximum demand limits and load sheds
- Cooling and heating "Calls"
- Power generation plant balancing

9.1.5 Setpoints

BMS installers shall limit zone temperature set-points adjustment to 20 – 25 degrees.

9.1.6 Fall-back Strategies

BMS installers shall ensure that all levels of the BMS system be properly configured to maintain local conditions during communications hardware failure.

Communications failure shall trigger an alarm annunciation event.

9.1.7 Fire Control

Fire Status Indication

- BMS systems shall monitor the status of the FIP for the building (either directly from the FIP or via mechanical services switchboards).
- BMS graphics for each controlled item will indicate the fire signal status.
- A dedicated BMS graphical page shall indicate the overall fire status of the building.
- All fire signals shall initiate an alarm annunciation event.
- Fire signals shall suppress other alarms that may be caused due to control strategies overrides and interruptions.

Fire Condition Control

- Fire conditions shall control mechanical equipment through the use of “Relay Logic” within mechanical switchboards and BMS control panels.
- Dampers shall also be controlled through the use of relay logic.
- BMS hardware shall not be solely responsible for the control of dampers located on fan coil units, air handling units, supply and extract fans during fire modes.
- BMS systems shall follow the same control sequence as that provided by relay logic during fire modes.
- Field controllers (FLN) that provide control of terminal equipment (e.g. VAV units) shall be programmed to drive dampers to positions specified by the fire & mechanical services engineers.

9.2 BMS Embedded User Interfaces

9.2.1 Instructions for Hardware Solutions

Where hardware embedded user interfaces are available (e.g. LCD screens), installers shall provide instructions adjacent to the device describing the operational methods, entering user name and password details (where necessary). Credentials will not be displayed at the embedded interface location, being available to property services personnel only.

9.2.2 Embedded Web Servers

Where embedded user interfaces are deployed using embedded web servers, installers must provide an indication on the device that this is an available option.

Such information shall also include the IP address, with all credential information being available only by liaison with Property Services.

9.2.3 Credentials

Credentials shall not be written down or notes at any embedded interface location.

Default credentials shall be erased at all embedded interface locations.

10. BMS Commissioning

10.1 Methods

Installers shall deploy an RMIT approved method of hardware & software commissioning that is accompanied by standardized documentation.

10.2 Documentation

Points schedules may be modified for use as point-to-point commissioning check sheets.

- Technicians shall approve the following items for each hardware point:
- Functional
- Calibrated
- Integrated in all control algorithms
- Visible on BMS Server
- Visible on GUI
- Alarm annunciation tested
- Data logging
- Available for use via BACnet MSTP and IP (where appropriate)

10.3 Software Testing

Software algorithms shall be fully tested and commissioned both independently and as part of the global strategy for the building and campus.

10.4 User Interfaces

Graphical interfaces, data collection & retrieval and alarm annunciation shall all be subject to the same commissioning techniques and documentation as hardware.

Quality assurance techniques shall be deployed to enable auditing of the commissioning and testing process.

11. BMS Operation & Maintenance Documentation

Each BMS project shall be supplied with a complete set of O&M documentation in addition to the points schedules, design drawings & software documentation described in section 10.

O&M documentation shall be supplied in both printed and electronic formats.

O&M documentation shall be available directly from the GUI.

Projects that use equipment previously deployed in other projects shall still provide the documentation in a document, even if the document thereby replicates previously supplied information.

11.1 Design Documentation

Installers shall provide the following documentation prior to work commencing:

11.1.1 Points Schedules

Points lists including ALN and FLN addresses, point addresses, point names, device type and part number

11.1.2 End Device Schedules

Control valve schedule, including size, type, ports, flow, pressure drop, manufacturer, model, actuator manufacture, model, supply voltage, control signal type and torque or force rating.

Damper actuator schedule, including manufacturer, model, supply voltage, control signal type, torque rating

11.1.3 Integration Schedules

Third party device schedule to be integrated via BACnet or MODbus, including IP or instance addresses where appropriate (use placeholders where final address is unavailable).

11.1.4 BMS Network Architecture

Network architecture drawing, including all ALN and FLN devices, expansion modules, third party interface devices and servers. IP addresses where appropriate (use placeholders where the final address is unknown). Addresses (or range where consecutive) of all FLN controllers.

Refer to APPENDIX A for a sample network topology diagram.

11.1.5 Controller Wiring Diagrams

Every field level controller (FLN) shall have a dedicated drawing showing the connection details for each BMS point.

Where ALN controllers also have field points connected, they must be provided with a connection diagram.

Typical drawings may be submitted where replication of a standard has been deployed (e.g. VAV or FCU terminal units)

Replication drawings must list all units that the drawing applies to.

Enclosure drawings and typical power supply arrangement.

11.1.6 IP Rack Allocation Record

A completed copy of the IP allocation sheet location of equipment using RMIT standardized address formats:

- BB.LL.RRR (Building, Level, Rack)
- IP address
- Field outlet numbers
- MAC address

A copy of this schedule must be available from the BMS GUI

11.2 Operational Documentation

Installers shall provide sufficient documentation with appropriate detail to enable the comprehension of the following items by RMIT and other support staff reasonably familiar with BMS systems:

- Structure of the BMS installed, including networks and locations of controllers
- An overview of the equipment controlled and monitored
- A general description of the overall control philosophy (initiation, occupancy, sequences etc)
- Detailed functional descriptions of control for each typical item of plant, including single line diagrams of plant (air, water, electricity, gas) and sequence diagrams.
- Control maps showing the interconnection of objects and functions. (Or lists of code where object orientation is not deployed).
- Detailed description of heating and cooling call methodologies.
- Detailed description of energy efficiency algorithms.
- Detailed description of data gathering and methods of retrieval and display.
- Detailed descriptions of alarm settings and associated actions.
- Description of any proprietary software necessary to program the ALN, FLN or other devices included within the BMS scope.
- The service provider shall provide a detailed maintenance schedule in the O&M manuals with recommended maintenance requirements over a period of 5 years for RMIT's perusal.

11.3 Manufacturer's Datasheet

Installers shall provide data sheets for each item installed as part of the BMS scope, including:

- Description and photograph
- Technical specifications
- Part number of actual item used (where alternatives are specified on the same sheet)
- User guides for systems where such would be necessary for operation, service or repair

12. BMS Training

12.1 Gap Analysis

Installers shall provide a training gap analysis for each BMS project.

Training shall include only those items identified during the gap analysis process.

12.1.1 Purpose of Training

Training shall enable RMIT property services to:

- Understand, locate & identify controlled equipment
- Locate the BMS equipment responsible for control of plant and equipment
- Physically identify the BMS hardware within each control enclosure
- Comprehend the structure of O&M documentation describing the system

12.1.2 Specific Items

Training shall guide the users in:

- Options for accessing the BMS
- Logging in and out of the BMS
- Navigating the GUI to find plant items
- Understanding each item of feedback
- Understanding the control of equipment
- Time schedules, holidays, occupancy control
- Set point modification
- Accessing data logging and the retrieval of the same
- Use of special functions
- Locating the alarm history, acknowledgement of alarms
- Understanding each system integration and any special items associated with integrations of other building services
- Fire conditions, AS1668 control monitoring, plant default states.

13. Maintenance & Service

13.1 Intent

Allows RMIT to determine which vendors and installers are qualified to provide maintenance & service of BMS systems within the University's built environment, regardless of the manufacturer, vendor, installer of integrator.

13.2 Qualifications & Experience

Service providers shall demonstrate qualifications and competence in the following areas:

- General BMS knowledge
- General mechanical services knowledge
- Hardware & software specific knowledge and experience
- Controls strategies and energy efficiency
- IT systems knowledge and experience
- Networking and infrastructure
- IT security principles

13.3 Response Times

Service providers shall be required to meet the response time requirements of RMIT property services

Normal hours	1 hours
After hours	2 hours

13.4 Defects Liability Period

Service providers shall ensure a defects liability period of a minimum of 12 months is provided, however specific project contract requirements may require this period to be greater than the minimum 12 months required under this design standard. The service provider shall ensure all preventative maintenance requirements are included in the submitted price for the defects liability period. The service provider shall provide a schedule of rates for reactive maintenance for RMIT's consideration as part of the handover documentation.

13.5 Site Knowledge

Site knowledge and experience regarding access to plant & equipment shall be maintained by the contractor, and shall be demonstrated to property services annually.

13.6 Hardware & Software Support

Service providers shall demonstrate their possession of appropriate licenses and qualifications regarding the BMS hardware and software.

Collaborative arrangements are tolerated provided the response times are maintained.

Service providers must ensure that service personnel laptops, tablets etc. used as tools of trade are maintained with updated operating systems including patching and up to date anti-virus and anti-malware software comply to RMIT standards found in this document.

Passwords to all tools of trade must also comply with RMIT security standards.

RMIT will provide user accounts to enable access to RMIT wireless network

13.7 Spare parts

All spare parts to the service provider's BMS at Automation Level shall be available within 6 weeks from placement of order to delivery on-site to RMIT. All spare parts at Field Level Network controller and below shall be available within 5 days from placement of order to delivery on-site to RMIT. Devices controlling critical plant and equipment, generally trigeneration/co-generation plant, chillers, boilers and AHUs shall be available within 2 days from placement of order to delivery on-site to RMIT unless prior written approval is obtained from RMIT in the case of specialised devices.

13.8 Tuning & Continuous Commissioning

Service providers shall demonstrate their competence in constant commissioning and tuning, including the analysis of stored data and associated trends and alarms.

Maintenance and service shall include a component of these activities that shall be demonstrated on a monthly basis through the combined use of BMS reports and written summaries provided as addenda to the standard service and maintenance reports.

14. IT Related – Hardware: Servers & Workstations

14.1 Servers

Server hardware and associated operating software shall not be provided by BMS vendors. ITS will provide solutions meeting the specifications at project cost

BMS servers shall never be located within the buildings which they service.

The minimum server hardware shall be specified by the BMS vendor/installer to match the performance required to support the BMS points, objects and features.

The preferred server software is Windows Server 2012 and shall be provided by RMIT ITS at project cost.

BMS vendors/installers shall advise RMIT ITS of any special software requirements.

Servers for BMS functions shall always be virtualized and managed by RMIT ITS.

Access to the server shall be provided by RMIT ITS via standard RMIT remote access methodology.

14.2 “Thick” Clients

The minimum workstation hardware shall be specified to match the purpose.

Workstations shall be RMIT supplied leased hardware (at project cost) and installed with RMIT managed operating environment that included anti-virus and anti-malware. The preferred workstation software is WIndows 7 Professional.

BMS vendors/installers shall advise RMIT ITS of any special software requirements.

BMS vendors/installers shall advise RMIT ITS of TCP/IP requirements.

14.3 “Thin” Clients

The minimum workstation hardware shall be specified to match the purpose.

RMIT support Internet Explorer 11, Firefox (latest) and Chrome (latest).

BMS vendors/installers shall advise RMIT ITS of any special software requirements.

BMS vendors/installers shall advise RMIT ITS of TCP/IP requirements

15 IT Related - Software : Servers & Workstations

15.1 BMS Software - Purpose

Software licenses are usually required for servers that manage BMS systems hardware. Each vendor/manufacturer supplies a proprietary version of software which is necessary for some functions. Examples of software applications are:

- BMS Database management servers
- Graphical user interface creation and display servers
- Alarm management servers
- Data storage and retrieval

The following clauses ensure that all BMS hardware is supplied with appropriate software.

15.2 BMS Server/Workstation Software Applications

BMS vendors/installers shall ensure that all necessary software is installed for the correct deployment and ongoing management of their BMS field hardware. Subsequent expansions to the base system shall have the software licenses upgrade to match the project.

Installers who use equipment that has not been previously deployed at RMIT and/or has not been provided with a user interface shall supply a software license sufficient for the quantity

New BMS solutions will require IT design and analysis to ensure server software is suitable for deployment at RMIT.

Installers expanding existing networks of the same (or compatible) manufacturer shall provide license extensions sufficient for the quantity of objects/points being installed as part of the works project.

15.3 Operating Systems

Only operating systems reviewed and approved by ITS shall be deployed for BMS servers and workstations.

Typically, Windows Server 2012 is the preferred server operating system. The addition of any servers or new solutions will require a full analysis and design

Typically, Windows 7 is the preferred workstation operating system.

Operating systems shall be reviewed on a regular basis, with security patches being deployed in accordance with RMIT ITS procedures. ITS perform security patching once per month.

Vendors must advise ITS if pending patches will have an adverse effect on any installed BMS software.

16 BMS Field Equipment Firmware Updates

16.1 Qualifications

BMS field hardware requiring firmware updates shall be updated only by qualified vendors and installers after agreement with both ITS and Property Services.

16.2 Testing

All firmware must be fully tested prior to installation and shall not adversely affect any existing BMS control or monitoring tasks.

16.3 Notice

Vendors and installers shall notify and liaise with RMIT ITS and property services prior to any firmware updates.

16.4 Record of Firmware

Firmware revisions shall be constant throughout the RMIT campuses for all devices of the same model.

A record must be kept by the vendor of the current firmware revision and all firmware updates. This record is to be accessible from the GUI.

16.5 Reboot/Restart

Any BMS hardware reboots required as a consequence of firmware updates shall be carried out at a time that does not affect the operational capacity of the serviced area, unless otherwise agreed with Property Services.

17 ITS Related - BMS Hardware & RMIT ITS Infrastructure

17.1 Pre Deployment

Designers that deploy systems with IP capability, and which are intended to be connected to the RMIT IT network infrastructure shall:

Guarantee that hardware does not interfere with existing IT infrastructure

Submit for approval by the Property Services vendor's panel any new item of equipment

17.2 Security

All BMS devices must comply with RMIT ITS security guidelines.

Any BMS equipment to be connected to the RMIT ITS infrastructure must first obtain approval from ITS through the raising of an ITS service "Ticket" raised by RMIT project management (via service desk) or directly by the property services team.

17.3 Design

BMS vendors//installers must provide RMIT ITS a comprehensive network topology diagram with the ticket.

17.4 BMS IP Addresses

ITS shall assign and manage specific "Subnet" ranges where BMS devices are hosted at Campus levels. These addresses will be provided in response to the "Ticket" outlined above. ITS network team will allocate and assign the correct IP ranges for the BMS project.

Note: Information required to submit is outlined in the RMIT Design Standards brief Section 10 Communications

17.5 IP Standards

Devices deployed in the field must support IPV4 address allocation using DHCP, variable subnet mask, and operate in a Layer 3 routed network.

- NTP and DNS support is recommended
- IPV4 & IPV6 support preferred

17.6 Integration of BMS Hardware with Services IP Systems

Prior to deployment, installers shall provide a written description of the method of integration with other building services devices residing on the RMIT IT network infrastructure including:

- Purpose of integration
- Protocols
- Addresses
- Data requests and responses
- Estimated required bandwidth
- Server location and IP address
- Redundancy levels during network failure

- Amount of data (transactional data) that needs to traverse the environment (IE: from the controller to the server or vice versa).
- Amount of data (backup related data).
- Time the data transfer is initiated and the interval that the data transfer is initiated.
- Flow diagram or topology of the BMS environment detailing which units communicate together.
- Which TCP/IP ports are utilized

Note: This document can be incorporated into the BMS network topology diagram where appropriate and such information does not cause complication and/or confusion.

17.7 TCP/IP Ports

BMS Vendor/installer shall provide the required TCP or UDP ports and data flow and/or direction.

This port information shall be included with the network topology at the time of the raising of the ticket and shall include:

Source	Location	Destination	Port Type	Port Number
ALN ID#	**B8, L10, C3**	**Server, Siemens**	**TCP**	**22**
Server, Siemens	**Data Centre**	**ALN ID#**	**UDP**	**5888**

17.8 Ethernet Cabling of BMS IP Enabled Equipment

All Ethernet cabling for the connection of field BMS equipment to the RMIT IT network is to conform to the RMIT Design Standards Brief Section 10 Communications.

This includes but is not limited to :

Ethernet UTP cabling must conform to Commscope's Krone Cat6A solution

Cabling is terminated on RK45 outlet in the field and connected to equipment using a Commscope Krone factory made and tested blue patch lead as approved by ITS for use in Cat 6A solutions

All horizontal Ethernet cabling for the connection of BMS equipment to the RMIT IT network is to be supplied, installed and terminated by the prime communications project contractor. Contact details for this contractor are available from RMIT Property Services and ITS.

Individual trades will not arrange their own cabling installer.

Ethernet UTP cabling from RMIT communication rooms will be supplied, installed, tested, certified and as built documentation provided as outlined in the RMIT design standard “Section 10 communications”.

Installation is to be by a Commscope ND&I certified 20 year approved installer. Use of non Commscope Krone ND&I certified installers is not permitted.

Note: All other UTP or STP cables installed for other BMS purposes (e.g. MSTP LAN, sensor cables etc) shall not terminate in the RMIT ITS communication room

17.9 IP Networking and Communication Hardware

BMS IP equipment shall only use RMIT supplied switches and routers. BMS vendors shall not supply any network equipment that will be permanently deployed.

No isolated IP networks and or network equipment are to be installed unless approved by ITS senior network manager

Note: Refer to Section 17.2 for descriptions of temporary networks for commissioning purposes.

18 ITS Related - Wireless Technologies

18.1 Definition & Limitations

Wireless technologies in the 2.4 Ghz and 5 Ghz spectrum shall not be permanently deployed within the RMIT campus at any time. This includes, but is not limited to:

WiFi	IEEE 802.11 and future iterations
Bluetooth	IEEE 802.15.1 and future iterations
ZigBee	IEEE 802.15.4 and future iterations

18.2 Temporary Wireless Networks

Temporary wireless technologies may be deployed during commissioning by BMS installers and commissioning technicians.

Such networks shall be approved by RMIT ITS prior to their deployment to ensure no interference with any existing wireless networks in the same area.

All temporary wireless networks shall be decommissioned and removed prior to handover and the commencement of defects liability period.

Prior to installing any temporary wireless the BMS vendor/installer shall inform RMIT ITS via Project Management team or Property Services by the raising of a BAU ticket.

Temporary WIFI solution design proposals must satisfy RMIT ITS that any temporary solution shall not interfere with existing WIFI networks or associated infrastructure.

BMS vendors/installers must also confirm to RMIT ITS that the WIFI solution will be de-commissioned at the conclusion of commissioning.

18.3 De-Activation

RMIT ITS will de-activate any temporary WIFI network that either:

- Was unapproved by ITS
- Was approved but causes interference with other ITS infrastructure

19 ITS Related - Security

19.1 ALN & FLN (Automation and Field Level Networks)

Installers shall provide an administrator's level password to RMIT prior to the commencement of defects liability period (DLP).

Passwords shall comply with RMIT ITS standards and shall be maintained according to the same standards.

19.2 Passwords

Format shall as far as possible match standard RMIT ITS guidelines:

- Complexity
- Storage
- Integration with windows credential manager

19.3 Off Site Access

Access to BMS systems shall NOT be possible other than through the approved RMIT ITS internet connection. Installers must not attach secondary access systems to any part of the BMS system.

19.4 Physical Security

BMS hardware that provides an access point capability shall be provided with a secure enclosure complete with a standard RMIT key-lock. Where BMS hardware is located within cupboards and risers, security shall be provided by a standard RMIT key-lock.

BMS hardware shall at no time be freely accessible by staff, students or the public.

19.5 "Dongle" Ports

Where BMS field hardware has the capability of utilizing a wireless dongle for direct communications to the internet (i.e. via 3G/4G modem) this capability shall be disabled both by software configuration and by permanent hardware physical blocking.

Ports that do not enable remote access directly via wireless 3G/4G modems do not need to be permanently disabled.

Where local ports that do enable remote access directly via wireless 3G/4G modems and are required for service and maintenance (e.g. in the case of TCP/IP failure) RMIT ITS shall be notified.

19.6 Maintenance of Security

Maintenance of all software related security issues shall be the responsibility of the nominated BMS service contractor. This contractor shall advise property services as security patches become available. This contractor shall also advise property services if physical security is compromised.

19.7 Documentation

Vendors and installers shall provide sufficient comprehensive documentation to enable RMIT property services and ITS to manage security concerns. Deployment of patches shall remain the vendor's and/or service contractor's responsibility.

Devices that have been identified as not meeting RMIT security requirements may be disconnected from the IT infrastructure by ITS.

20 ITS Related - Remote Access

20.1 General

Remote access to BMS systems may only be achieved with the prior approval of ITS, and using only approved methods of access.

Approved methods of access are limited to SSL VPN with a specific vendor account, which can be obtained by Property Services raising a ticket on behalf of the vendor.

20.2 Direct Internet Access

Direct access from the internet to BMS network hardware via modems and dongles not part of the RMIT ITS managed network is expressly prohibited.

BMS automation level (ALN) hardware that provides hardware ports that enable such access to be achieved shall be physically disabled.

BMS field level (FLN) I/O hardware that allows access across the field level network to other I/O controllers shall have access restricted to a single MS/TP network.

BMS automation level (IP) hardware that allows access to other BMS automation and/or field level hardware on the network either via proprietary software or standard terminal style interfaces shall be disabled and protected until required for use. Only authorized BMS technicians shall have access to these hardware ports. RMIT ITS shall be advised of these access ports.

20.3 Tunneling from External Locations

Proprietary BMS configuration and service tunneling software shall gain access only through the approved methods of access. (SSL VPN with vendor account)

20.4 RMIT Intranet Access

Access to BMS hardware and servers shall be available from inside the RMIT firewalls. BMS vendors/installers shall provide all necessary information to RMIT ITS via the raising of a ticket. Such information shall include:

- Software description
- TCP/IP ports requirements
- IP Address requirements

21 ITS Related - Audit Trail

21.1 General

An audit trail is required to track changes made by any users of the BMS system.

21.2 Minimum Information

Audit trails on servers must be configured to record the following information:

- Time and date of all items and activities collected
- User log on/off time and date
- Overrides and changes to values time and date
- Activity regarding hardware database change, reloads, firmware upgrades etc. time and date

22 ITS Related - Alarms & Alerts

22.1 General

Alarms are to be generated by BMS systems field equipment and directed to the vendor's BMS server. Alarms are to be recorded within the server's database and re-directed to users' email and SMS accounts.

22.2 Alarm Routing

The routing of the alarms to users shall be via the use of RMIT's email and SMS alarm handling systems.

22.3 Annunciation & Message Format

Installers shall provide a common data output format that is directed to a common RMIT alarm handling and annunciation system for distribution to recipients via email and SMS.

The formatting of the message shall be discussed with RMIT property services prior to deployment.

22.4 Alarm History Sharing

Vendors shall provide a method of sharing all alarm events with a common database application that shall be part of the future E-BMS.

23 APPENDIX A – NETWORK TOPOLOGY DIAGRAM