Networking Working Group
Internet-Draft
Intended status: Informational
Expires: January 8, 2011

J. Martocci
Johnson Controls Inc.
Anthony Schoofs
University College Dublin
Peter van der Stok
Philips Research Laboratories

July 8, 2010

Commercial Building Applications Requirements
draft-martocci-6lowapp-building-applications-01

Abstract

Building management systems have evolved toward IP communication at the enterprise level during the past decade. IP implementation at the real-time control and sensor layers would provide a single pervasive protocol usable across the entire system increasing flexibility and code reuse. This document will describe the topology of these building networks, the application protocols widely used in their deployment and the application use cases.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 8, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Terminology

Actuator: A field device that controls and/or modulates a flow of a gas or liquid; or controls electrical distribution.

BACnet: Building Automation Control Network. A ISO application protocol used in building management systems.

Channel: Radio frequency sub-band used to transmit a modulated signal carrying packets.

DALI: Digital Addressable Lighting Interface. A protocol used in lighting systems.

Fire: The term used to describe building equipment used to monitor, control and evacuate an internal space in case of a fire situation. Equipment includes smoke detectors, pull boxes, sprinkler systems and evacuation control.

FMS: Facility Management System. A global term applied across all the vertical designations within a building including, Heating, Ventilating, and Air Conditioning also referred to as HVAC, Fire, Security, Lighting and Elevator control.

HVAC: Heating, ventilation and air conditioning. This term is broadly used to define anything in the building that addresses air flow and occupant comfort.

Intrusion Protection: A term used to protect resources from external infiltration. Intrusion protection systems

Lighting: The term used to describe building equipment used to monitor and control an internal or external lighted space. Equipment includes occupancy sensors, light switches and ballasts.

Luminaire: Another term for a light fixture installed in a ceiling.

MS/TP: Master Slave Token Passing; the EIA-485 data link used in BACnet. This data link uses a software token passing mechanism allowing for multiple multi-dropped masters on the network. A master node can only access

the media while it secures the token. MS/TP also supports slave nodes. These less complicated devices never receive the token and can only address the media when requested from a master node.

Security: The term used to describe building equipment used to monitor and control occupant and equipment safety inside a building. Equipment includes window tamper switches, door access systems, infrared detection systems, and video cameras.

2. Overview

Facility Management systems (FMS)are deployed in a wide variety of commercial building topologies, including single buildings, multi-building single site environments such as university campuses and widely dispersed multi-building multi-site environments such as franchise operations. These buildings range in size from 100K square feet (10k square meters) structures (5 story office buildings), to multi-million sqft skyscrapers (110 story Shanghai World Financial Center) to complex government facilities (Pentagon). The described topology is meant to be the model to be used in all these types of environments, but clearly must be tailored to the building class, building tenant and vertical market being served.

The following sections describe the FMS system architecture from the lowest layer to the highest layers in the hierarchy. Each section describes the basic functionality of the layer, its networking model, power requirements and a brief description of the communication requirements. The entire section references the block diagram noted in Figure 1. This figure depicts six major subsystems comprising an FMS. These subsystems all have layered solutions starting at the sensor layer and moving upward in complexity toward the enterprise network layer. While these six subsystems are common to many facilities, they are by no means the exhaustive list - a chemical facility may require a complete fume hood management system; a manufacturing facility may require interfacing to the PLC subsystem; or a multi-tenant facility might require a comprehensive power management subsystem. The objective in the architecture is to integrate all common functions into the system yet allow maximum flexibility to modify these systems and add other subsystems as dictated by the customer.

Commercial buildings have been fitted with pneumatic and subsequently electronic communication pathways connecting sensors to their

controllers for over one hundred years. Pneumatics were displaced by simple electronics and dry contacts in the 1960's. Smart processor based sensors displaced simple contacts in the 1970's. Localized digital control, introduced in the 1980's allowed applications to operate independently from the upper layers of the system. Multi-dropped twisted pair sensor/controller communication networks displaced high cost cabled networks.

The 1990's ushered in the use of Ethernet IP networks at the enterprise level. This transition allowed the previously independent proprietary communication networks to coexist on the enterprise IP LAN network. This migration reduced installation costs and allowed pertinent building data to be injected onto the enterprise application suite. Proprietary protocols were displaced by industry standard application protocols such as BACnet and LON for HVAC; and DALI for Lighting.

Recent economic and technical advances in wireless communication allow facilities to increasingly utilize a wireless solution in lieu of a wired solution; thereby reducing installation costs while maintaining highly reliant communication. Wireless solutions will be adapted from their existing wired counterparts in many of the building applications including, but not limited to HVAC, Lighting, Physical Security, Fire, and Elevator systems. These devices will be developed to reduce installation costs; while increasing installation and retrofit flexibility. Sensing devices may be battery, scavenged, or mains powered. Actuators and area controllers will be mains powered. Today, different networks based on their own standard (e.g. BACnet, DALI) do not share cabling, sensors or actuators easily. The arrival of IP for building control will coalesce these topologies.

The objective of this draft is to describe topologies, protocols and application use cases. It will describe the application benefits and concerns in converting to pervasive IP networks. It will further describe the IP services required to operate these systems. Finally, it will describe how the building data and IT data models might converge to allow a free flowing of data on the converged FMS/IT network.

3. FMS Topology

3.1. Introduction

To understand the network systems requirements of an FMS in a commercial building, this document uses a framework to describe the

basic functions and composition of the system. An FMS is a horizontally layered system of sensors, actuators, controllers and user interface devices orchestrated to work together over selected communication media. Additionally, an FMS may also be divided vertically across alike, but different building subsystems such as HVAC, Fire, Security, Lighting, Shutters and Elevator control systems as denoted in Figure 1. These distinct areas are termed 'silos'. Currently, the separation between the silos is rather sharp. Gateways provide connections between the silos to support all encompassing applications. With future IP deployment applications will have a flat addressing space for accessing all nodes in any silo.

Much of the makeup of an FMS is optional and installed as required by the customer. These systems are expensive and must be designed to allow for incremental purchases as dictated by the customer's budget cycle.

Sensors and actuators have no standalone functionality. All other devices support partial or complete standalone functionality. These devices can optionally be tethered to form a more cohesive system. The customer requirements dictate the level of integration within the facility. This architecture provides excellent fault tolerance since each node is designed to operate independently but will accept overrides from the higher layers when the higher layers are available.

Heating, Ventilation and Air Conditioning (HVAC); Fire; Security and Lighting are components that can be tethered together into a cohesive set of all encompassing applications tailored to the customer's whim. Shutter control is an emerging application domain prevalent in the European market. These major subsystems are connected logically through application software called Building Applications.

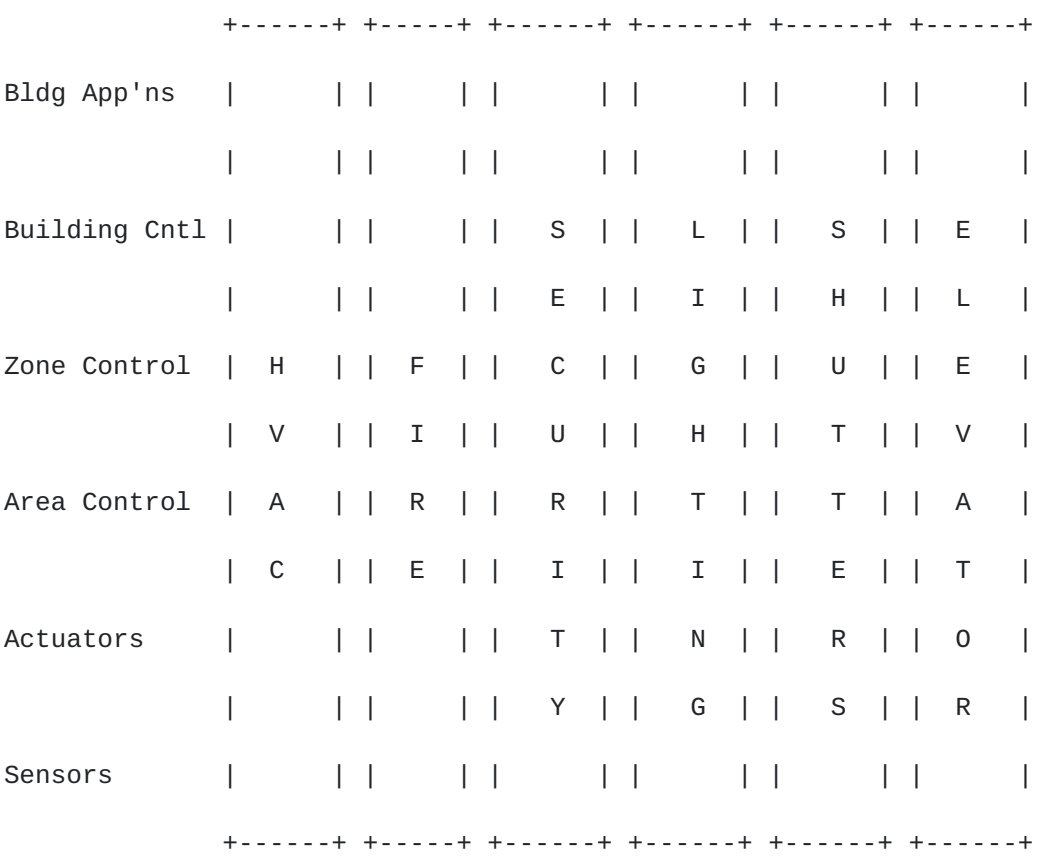

Figure 1 - Building Systems and Devices

3.2. Sensors/Actuators

An FMS may be composed of many functional stacks or silos that are interoperably woven together via Building Applications. Each silo has an array of sensors that monitor the environment and actuators that effect the environment as determined by the upper layers of the FMS topology. The sensors typically are the leaves of the network tree structure providing environmental data into the system. The actuators are the sensors' counterparts modifying the characteristics of the system based on the input sensor data and the applications deployed.

3.3. Area Controllers

An area describes a small physical locale within a building, typically a room. Public spaces such as hallways and atria are also controlled by area controllers. The HVAC, Security and Lighting functions within a building address area or room level applications running in the area controllers. Area controls are fed by sensor

inputs that monitor the environmental conditions within the room. Common sensors found in many rooms that feed the area controllers include temperature, occupancy, lighting load, solar load and relative humidity. Sensors found in specialized rooms (such as chemistry labs) might include air flow, pressure, CO2 and CO particle sensors. Room actuation includes temperature setpoint, lights and blinds/curtains.

3.4. Zone Controllers

Zone Control supports a similar set of characteristics as the Area Control albeit to an extended space. A zone is normally a logical grouping or functional division of a commercial building. A zone may also coincidentally map to a physical locale such as a floor.

Zone Control may have direct sensor inputs (smoke detectors for fire), controller inputs (room controllers for air-handlers in HVAC) or both (door controllers and tamper sensors for security). Like area/room controllers, zone controllers are standalone devices that operate independently or may be attached to the larger network for more synergistic control.

3.5. Building Controllers

Building Controllers orchestrate the overall building control. These devices provide higher level functionality such as web servers, scheduling, time series data archival, energy monitoring and reduction, and alarm management. Additionally they will cooperate with the other silos to provide synergistic applications as noted in the use case sections that follow.

4. FMS Communication Media

Today most FMSs communicate over four media; DALI, EIA-485, Ethernet and wireless.

For HVAC instrumentation, sensors, actuators, area controllers, zone controllers, and building controllers most often connect via EIA-485 3-wire twisted pair serial media operating nominally at 38400 to 76800 baud. This allows runs to 5000 ft without a repeater. With the maximum of two repeaters, a single multi-dropped communication trunk can serpentine 15000 ft.

For lighting the DALI standard provides a 5-wire cable containing control and power-supply lines. Up to 64 control units can be connected to one line. The maximum distance between two directly connected DALI devices is 300m operating at 1200 bits/s.

The HVAC, Fire, Access, Intrusion and Lighting subsystems are integrated using LAN based Ethernet technology. These enterprise devices connect to standard Cat-5e through workgroup switches. WLAN communications can replace the Ethernet connection if the application can operate within the WLAN performance characteristics. Currently building controllers typically support a RJ-45 connection. WLAN connections require an external wireless bridge. Multi-building sites can also connect onto the facility intranet if the intranet performance matches the application requirements.

Recently sensors, area controllers and zone controllers have been deployed on wireless mesh systems. 802.15.4 based mesh systems seem to be the technology of choice by most manufacturers due to the cost point of the radio technology and communication robustness.

5. FMS Communication Protocols

5.1. Controller/Sensor/Actuator Communication Protocol

The sensors, actuators, area controllers, zone controllers, and building controllers all utilize BACnet, DALI, or LON protocol. BACnet is an ISO world-wide Standard application layer protocol designed to maximize interoperability across many products, systems and vendors in commercial buildings. BACnet was conceived in 1987 and released in 1995 for the HVAC industry. Since that time Fire, Security and Lighting functionality has been added.

BACnet supports six media types including Ethernet (802.3 and IP), EIA-485, Arcnet, LON, RS-232 and ZigBee.

BACnet supports all expected network services including functions such as device and object discovery; unicast and broadcast messaging; full routing; flow control and fragmentation; and network security.

BACnet MS/TP is the BACnet data link for EIA-485 networks. MS/TP is a token passing protocol (implemented in software) allowing master/slave and peer-to-peer communication simultaneously. Devices must designate themselves as slaves or masters on the network. Slave devices may only access the network when solicited by a master device. Masters may communicate to any node on the network whenever it holds the token. BACnet MS/TP has a 1-octet MAC address allowing for a maximum of 254 devices per network segment. (Address 255 is reserved for broadcast designation).

BACnet/IP addressing currently supports IPv4 addressing only. An IPv6 working group has been commissioned by the BACnet Committee to develop the needed changes for BACnet to support IPv6.

The DALI standard was conceived in the late 1990 and consolidated in the IEC 62386 standard (formerly IEC 60929). DALI network is ordered in 16 groups of each maximally 64 devices. 16 scenes can be defined grouping sets of devices together to receive the same command sequences. A DALI network is usually a lighting subnet connected to the building network with a LON DALI gateway.

5.2. Enterprise Communication Protocol

Multiple protocols are supported at the enterprise level of the FMS since this layer supports both the embedded control operation and the user interface.

5.2.1. Peer-to-peer Controller Communication

Building Controllers orchestrate the overall FMS system operations. Control and data access functions implemented at this level utilize BACnet IP. BACnet IP provides the complete building object model and requisite services across all the FMS silos. Since BACnet is deployed on the lower layers of the system, utilizing it to control operations at the highest layer of the system is prudent. BACnet IP implements UDP/IP with its own transport layer. It is designed to operate efficiently and transparently on all IP networks.

5.2.2. Enterprise Communication

While BACnet and LON are the control protocols of choice; it is out of scope for most enterprise applications. Web Services and SNMP frequently is added to the enterprise layer to assist in integration with end-user applications and Network Management Systems respectively. The enterprise level also supports most ancillary IT protocols such as SMTP, SNTP, DHCP and DNS.

6. FMS Device Density

Device density differs depending on the application and code requirements. The following sections detail typical installation densities for different applications.

6.1. HVAC Device Density

HVAC room applications typically have sensors and controllers spaced about 50ft apart. In most cases there is a 3:1 ratio of sensors to controllers. That is, for each room there is an installed temperature sensor, flow sensor and damper controller for the associated room controller.

HVAC equipment room applications are quite different. An air handler system may have a single controller with upwards to 25 sensors and actuators within 50 ft of the air handler. These sensors may include a discharge air temperature, a static pressure sensor, a CO sensor, a CO2 sensor, a return air temperature and a mixed air temperature.

A chiller or boiler is also controlled with a single equipment controller instrumented with 25 sensors and actuators. Each of these devices would be individually addressed. Air handlers typically serve one or two floors of the building. Chillers and boilers may be installed per floor, but many times service a wing, building or the entire complex via a central plant. Sensors typically instrumented on a chiller include chilled water temperature, condenser water temperature, and pump status.

These numbers are typical. In special cases, such as clean rooms, operating rooms, pharmaceuticals and labs, the ratio of sensors to controllers can increase by a factor of three. Tenant installations such as malls would opt for packaged units where much of the sensing and actuation is integrated into the unit. Here a single device address would serve the entire unit.

6.2. Fire Device Density

Fire systems are much more uniformly installed with smoke detectors installed about every 75 feet. This is dictated by local building codes. Fire pull boxes are installed uniformly about every 150 feet. A fire controller will service a floor or wing. The fireman's fire panel will service the entire building and typically is installed in the atrium.

6.3. Lighting Device Density

Lighting is also very uniformly installed with ballasts installed approximately every 10 feet. A lighting panel typically serves 48 to 64 zones. Wired systems typically tether many lights together into a single zone. Wireless systems configure each fixture independently to increase flexibility and reduce installation costs.

6.4. Physical Security Device Density

Security systems are non-uniformly oriented with heavy density near doors and windows and lighter density in the building interior space. The recent influx of interior and perimeter camera systems is increasing the security footprint. These cameras are atypical endpoints requiring upwards to 1mbps data rates per camera as contrasted by the few kbps needed by most other FMS sensing equipment. To date, camera systems have been deployed on a proprietary wired high speed network or on enterprise VLAN. Camera compression technology now supports full-frame video over wireless media.

7. FMS Installation Methods

Wired FMS installation is a multifaceted procedure depending on the extent of the system and the software interoperability requirement. Unlike most IP installations, FMSs are installed from the outside-in. That is the sensors, actuators and controllers are installed first. Later the Zone Controllers are installed; and finally the system is connected to the enterprise network.

At the sensor/actuator and controller level, the procedure is typically a two or three step process. Most FMS equipment is 24 VAC equipment that can be installed by a low-voltage electrician. He/she arrives on-site during the construction of the building prior to the sheet wall and ceiling installation. This allows him/her to allocate wall space, easily land the equipment and run the wired controller and sensor networks. The Building Controllers and Enterprise network are not normally installed until months later. The electrician completes his task by running a wire verification procedure that shows proper continuity between the devices and proper local operation of the devices.

For lighting networks this means that light sensor, presence sensor, switches, and luminaires are all connected within a room and sometimes already connected to a room controller. Commissioning is for DALI executed with a laptop to map network addresses to physical devices.

Later in the installation cycle, the higher order controllers are installed, programmed and commissioned together with the previously installed sensors, actuators and controllers. In most cases the IP network is still not operable. The Building Controllers are completely commissioned using a crossover cable or a temporary IP switch together with static IP addresses.

Once the IP network is operational, the FMS may optionally be added to the enterprise network. Wireless installation will necessarily need to keep the same work flow. The electrician will install the products as before and run continuity tests between the wireless devices to assure operation before leaving the job. The electrician does not carry a laptop so the commissioning must be built into the device operation.

8. Building Application Use Cases

The Building Application layer is a software layer that binds the various system silos into a cohesive systemic application. This discussion in not meant to be inclusive. Rather it is meant to show how these diverse systems can be coordinated to provide innovated synergistic applications for the customer safety and comfort.

8.1. Fire and Smoke Abatement

Most local codes now require commercial buildings to incorporate comprehensive fire and life/safety systems into a building. It is well documented that loss of life in a building is mainly caused by smoke inhalation rather than the fire itself. Agencies, such as UL (in the US market), have developed fire certification programs that govern fire and smoke operations in commercial buildings. These programs require very rigorous interactive testing for certification. In addition to the obvious need to minimize life/safety situations in a building, facility operators are highly encouraged to implement these systems due to insurance cost reductions.

The fire and smoke abatement application requires a highly coordinated interaction between the fire silo and the HVAC silo. The fire system detects the smoke or fire and reports it to the HVAC system. While the fire system is issuing evacuation notices, sounding the alarms and flashing the strobes; the HVAC system automatically shuts down all fan systems in the immediate area (to starve the fire) while simultaneously opening all external dampers and ratcheting up the fans in the adjacent areas to purge the smoke.

Meanwhile, the lighting systems will immediately turn on all safety lights in the area to assure safe passage for the occupants. It will also create light trails to assist occupants to the doors.

The physical security system will unlatch all doors to assure immediate egress of the occupants.

The elevator control system will either shut off entirely or bypass normal operation to assist with the emergency responders.

The fire and smoke systems operate in either a manual or automatic mode. The automatic mode is a preprogrammed set of events that control the fire automatically. The manual mode provides critical fire and smoke information at a centralized display to be controlled by a Fire Marshal. In practice, the fire system will be set to automatic mode and operate accordingly until the Fire Marshall arrives. At that point the system is normally overridden to manual mode so that the Fire Marshall can control operations from the command center as deemed necessary.

While the smoke abatement operation could be the province of the fire system alone, economics dictate that the fire system off-loads the smoke abatement operation to the HVAC system. In practice, the fire system will receive the initial fire indication by one or more of its smoke detectors. It will then inform the HVAC system of the physical locale of the fire. The HVAC system will then take charge of the smoke abatement operation by automatically adjusting the air handlers and dampers. The HVAC system must incorporate a comprehensive prioritization scheme throughout its system. This prioritization scheme must allow all smoke operations to take control precedence over all other control operations including manual operator control. All affected devices must support a supervision policy that assures that all operations requested were executed properly. The system must automatically return to well-defined normal operational state once the smoke situation has abated.

8.2. Evacuation

Evacuation is another systemic operation that may be activated as part of the Fire/Smoke Control application, or may be activated for other reasons such as terrorist threats. Evacuation requirements most often will activate subsystems of the Fire, Security and Lighting silos. The Fire system normally supports the intercom subsystem in the facility. The intercom system will then trigger the recorded voice evacuation instructions. This may be in concert with the fire system audio indications if a fire situation is active or standalone. The lighting subsystem will be activated to turn on the lights and evacuation paths to aid in the evacuation. The security system will coincidentally open all doors to allow a smooth safe egress from the building. If the building also supports elevator control, the elevators will operates as directed by a preprogrammed evacuation policy.

8.3. Occupancy/shutdown

A major energy saving technique in commercial buildings is to automatically commence HVAC and lighting operations prior to building occupancy. Conversely, building shutdown allows the systematic reduction in HVAC and lighting operations as the building becomes unoccupied.

The HVAC system is usually charged with defining occupied and unoccupied times. The Fire and Security operations are always operable and lighting is most often subservient to HVAC. Occupied/unoccupied schedules are typically programmed into the system by facility operations; however, it could be learned adaptively by the security's access control system. The target occupancy time drives the HVAC subsystem to turn on all ventilation equipment at an optimal time so that each space is ready for occupancy at the prescribed time. These algorithms will be adaptive over time but also include systemic instrumentation such as outdoor air and relative humidity to turn on the equipment at the last possible moment yet still meet the target environmental needs just before occupancy.

The lighting systems are turned on/off as a function of the overall room light intensity and the presence of persons within the room. Switching on is immediate on arrival of persons, switching off is done with a suitable delay, possibly involving dimming of lights.

Conversely, the HVAC systems will also determine the earliest possible time it can shut down heating/cooling yet still control the setpoints to meet the requisite parameters. Lighting again gets off easier since the lights can be extinguished as soon as they are not needed.

Building owners may use the lighting systems to pace the janitorial service providers by defining a strict timetable that the lights will be on in a given area. Here, the janitorial service providers will need to keep in step to complete their work prior to the lights being turned off.

Facility Management Systems often include a telephone interface that allows any late workers to override the normal HVAC and lighting schedules simply by dialing into the system and specifying their locale. The lights and fan system will continue to operate for a few extra hours in the immediate vicinity. The same applies to occupancy sensors in meeting rooms. Either by automatic sensing or a simple push of the occupied switch, the HVAC and lighting schedules will

extend the normal schedule for the meeting room.

8.4. Energy Management

The occupancy/shutdown applications noted above optimize runtime of large equipment. This in itself is a major component of energy savings. However, even during occupancy large equipment can be modulated or shutoff temporarily without affecting environment comfort. This suite of applications run in the HVAC domain, however the HVAC silo will interact with the lighting system to reduce the lighting load to help in the overall reduction of energy.

The load rolling, demand limiting and demand response applications allow for the sequencing of equipment to reduce the overall energy profile or to shave off peak energy demands in the facility. The FMS system will constantly monitor real-time energy usage and automatically turn unneeded equipment off (or reduce the control setpoint) to stave off peaking the facility's electrical profile. Demand peaks set by commercial facilities are frowned upon heavily by utilities and are often accompanied by huge energy charge increases for upwards to 1 year.

Recently real-time pricing has furthered the ability to save energy. This allows a facility to proactively either use or curtail energy based on the price/KWH of the energy. Again, the HVAC subsystem takes the lead in this application. It can either poll the price structure from the Utility off the Internet, or the current pricing will be forwarded to the facility by the Utility. The HVAC subsystem can then automatically defer unneeded operation or temporarily reduce the cooling or lighting load as the cost warrants. As always, the HVAC subsystem is charged with seamlessly returning the components to their normal operating conditions at the close of the energy event.

8.5. Fault Detection and Diagnostics

HVAC primary equipment such as air handlers or chillers often have capital expenditure costs in the $100k range. These systems are critical to operation of the building and comfort to its tenants. Contemporary HVAC subsystems can track usage and performance operation of these devices in time and trigger alarms if the performance characteristics fall outside the expected statistic usage profile. This fault detection application can be further enhanced by adding automatic diagnostic modes that define the source problem. The diagnostics evaluation may suggest changing clogged air filters,

inspecting a failed pump or even rebuilding the chiller mechanics due to erratic vibration analysis.

9. Building Application Protocol Requirements

This section contains the overall set of building application requirements as dictated by the previous discussion.

9.1. Physical Layer Requirements

9.1.1. Wired and Wireless Implementations

The protocol MUST support both wired and wireless IP implementations.

9.1.2. Cost Effective Wired Installation

The protocol MUST support wired media that is readily installable by electricians. Its amortized per connection installed cost SHOULD NOT exceed of the cost of the end device. That is, if the cost of the device is $X; the total installed cost shall not exceed $2X, where X is typically < $75.

9.1.3. Cost Effective Wireless Installation

The protocol MUST support wireless mesh that is readily installable by electricians. Its amortized per connection installed cost SHOULD NOT exceed of the cost of the end device. That is, if the cost of the device is $X; the total installed cost shall not exceed $1.5X, where X is typically < $75.

9.1.4. Global Wireless Applicability

Wireless devices MUST be supportable on unlicensed bands (such as the 2.4Ghz)that are applicable globally.

9.1.5. Constrained Power Sensors

The protocol MUST support wireless end devices that operate with battery power or by energy scavenging. These devices will likely sleep with a 99% duty cycle.

9.2. Network Layer Requirements

9.2.1. TCP/UDP

Connection based and connectionless services MUST be supported.

9.2.2. Fragmentation

Packet fragmentation must be supported.

9.2.3. Data Rate Performance

An effective data rate of 20kbps is the lowest acceptable operational data rate acceptable on the control networks.

9.2.4. Interference Mitigation

The wireless network MUST automatically detect interference and migrate the network to a better channel to improve communication. Channel changes and nodes response to the channel change MUST occur within 60 seconds.

9.2.5. Real-time Performance Measures

A node transmitting a 'request with expected reply' to another node MUST send the message to the destination and receive the response in not more than 120 msec. This response time SHOULD be achievable with 5 or less hops in each direction. This requirement assumes network quiescence and a negligible turnaround time at the destination node.

9.2.6. Packet Reliability

Reliability MUST meet the following minimum criteria :

< 1% MAC layer errors on all messages; After no more than three retries

< .1% Network layer errors on all messages;

After no more than three additional retries;

< 0.01% Application layer errors on all messages.

Therefore application layer messages will fail no more than once every 100,000 messages.

9.2.7. Packet Routing

Unicast packets MUST be routable across any two nodes of the network.

9.3. Installation and Commissioning Requirements

9.3.1. Device Setup Time

Network setup by the installer MUST take no longer than 20 seconds per device installed.

9.3.2. Unavailability of an IT network

Product installation and local commissioning MUST be performed by an application engineer prior to the installation of the IT network including switches, routers, DNS and DHCP servers.

9.4. Application Layer Object/Node Requirements

9.4.1. Object Model

The application protocol must adhere to a well defined object model. This model must support generic objects (e.g. AI, BI, AO, BO) and semantic objects (e.g. temperature sensor, pump, door lock, light ballast)

9.4.2. Object Location

The protocol MUST optionally support determination of the physical location of a device.

9.4.3. Node Discovery

The protocol MUST support the discovery and binding of other nodes anywhere on the internetwork by name or address by using a single broadcast or multicast request packet.

9.4.4. Object Discovery

The protocol MUST support the discovery and binding of two or more objects anywhere on the internetwork by either name or address.

9.4.5. Object List

The protocol MUST support supplying the entire object list of all objects created in a given node.

9.4.6. Property List

The protocol MUST support a node returning a complete property list of all mandatory and optional properties defined for a given node.

9.4.7. Service List

The protocol MUST support supplying the entire list of services supported for a given node.

9.4.8. Consistent Error Reporting

The protocol must support a rigorous error reporting mechanism that is consistent across all objects and nodes.

9.5. Application Layer Solicited Service Requirements

9.5.1. Reading Datum

The application protocol MUST support a means to read a single piece of data (property) from a targeted node and object. Read requests must be validated via an ACL. The default ACL allows reading of any property.

9.5.2. Reading Data from an Object

The application protocol MUST support a means to read multiple data items from a targeted node and object with a single request. Read requests must be validated via an ACL. The default ACL allows reading of any properties.

9.5.3. Reading Data from Multiple Objects

The application protocol MUST support a means to read multiple data items from multiple objects on the same node with a single request. Read requests must be validated via an ACL. The default ACL allows reading of any properties.

9.5.4. Reading Data with Wild Cards

The application protocol MUST support a means to read multiple data items from multiple objects on the same node using a wild card mechanism. Read requests must be validated via an ACL. The default ACL allows reading of any properties.

9.5.5. Reading Large Data Items

Whenever an array or list can get larger than what is supported by the MTU or fragmented packet; the object MUST support a means to allow reading the data over multiple requests.

9.5.6. Object Creation and Deletion

The application protocol MUST support a means to create and delete objects. Creation requests must be validated via an ACL. The default ACL does not allow object creation or deletion.

9.5.7. Object Property Writing

The application protocol MUST support a means to write for the first time or to modify the current value of a property. Property writing requests must be validated via an ACL. The default ACL does not allow object property writing. Properties are the province of the server and hence, the server may at anytime and for any reason prohibit property writing.

9.5.8. Atomic Object Property Writing

The application protocol MUST support a means to write for the first time or to modify the current value of multiple properties atomically. Property writing requests must be validated via an ACL. The default ACL does not allow object property writing. Properties are the province of the server and hence, the server may at anytime and for any reason prohibit property writing.

9.5.9. Object Property List Writing Addition

The application protocol MUST support a means to write for the first time or to modify the current value of a list property. Property writing requests must be validated via an ACL. The default ACL does not allow object list property writing. Properties are the province of the server and hence, the server may at anytime and for any reason prohibit property writing.

9.5.10. Object Property List Writing Deletion

The application protocol MUST support a means to delete an element from an existing list. The service SHALL error out if the requested list item to be removed is not a element of the list.

9.5.11. Downloads

The application layer MUST support a means to download data and programs. Download requests are validated by an ACL.

9.6. Application Layer Unsolicited Service Requirements

9.6.1. Property Value(s) Change Notification

The application protocol MUST support a means to request data callbacks on a change to a specified property or object. Subscriptions may timeout at a periodic basis or may be cancelled by the client at any time. Subscriptions must persist a reboot.

9.6.2. Alarm Notification

The application protocol MUST support clients requesting alarm notification to selected objects. When the object transitions into the 'alarm' state for a predefined time, nodes subscribing to this alarm will be notified of the state change. Alarm subscriptions may timeout at a periodic basis or may be cancelled by the client at any time. Subscriptions must persist a reboot.

10. Traffic Pattern

The independent nature of the automation systems within a building plays heavy onto the network traffic patterns. Much of the real-time sensor data stays within the local environment. Alarming and other event data will percolate to higher layers as alarm events occur.

Systemic data may be either polled or event based. Polled data systems will generate a uniform packet load on the network. This architecture has proven not scalable. Most vendors have developed event based systems which passes data on event. These systems are highly scalable and generate low data on the network at quiescence. Unfortunately, the systems will generate a heavy load on startup since all the initial data must migrate to the controller level.

They also will generate a temporary but heavy load during firmware upgrades. This latter load can normally be mitigated by performing these downloads during off-peak hours.

Devices will need to reference peers for sensor data or to coordinate across systems. Data will migrate from the sensor level upwards through the local, area, then supervisory level. Bottlenecks will typically form at the funnel point from the area controllers to the supervisory controllers.

11. Security Considerations

TBD

12. IANA Considerations

This document includes no requirement to IANA.

13. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

14.2. Informative References

[I-D.ietf-roll-terminology]Vasseur, J., "Terminology in Low power And Lossy Networks", draft-ietf-roll-terminology-00 (work in progress), October 2008.

Authors' Addresses

Jerry Martocci
Johnson Controls
507 E. Michigan Street
Milwaukee, Wisconsin, 53202
USA
Phone: 414.524.4010
Email: jerald.p.martocci@jci.com

Anthony Schoofs
CLARITY Centre for Sensor Web Technologies
University College Dublin,
Dublin 4 Ireland
Phone: +353 1 7162488
Email: anthony.schoofs@ucdconnect.ie

Peter van der Stok
Philips Research
High Tech Campus
Eindhoven, 5656 AA
Netherlands
Email: peter.van.der.stok@philips.com