Networking Working Group
Internet-Draft
Intended status: Informational
Expires: January 14, 2009

J. Martocci, Ed.
Johnson Controls Inc.

July 14, 2008

Commercial Routing Requirements in Low Power and Lossy Networks
draft-martocci-roll-commercial-routing-reqs-00

Abstract

The ROLL Working Group was recently chartered by the IETF to define routing characteristics for low power embedded devices. ROLL would like to serve the Industrial, Commercial, Home and Urban markets. Pursuant to this effort, this document defines the functional and cost requirements for installing integrated facility management systems in commercial facilities.

The routing requirements for commercial building applications are presented in this document. Commercial buildings have been fitted with pneumatic and subsequently electronic communication pathways connecting

sensors to their controllers for over one hundred years. Recent economic and technical advances in wireless communication allows facilities to increasingly utilize a wireless solution in lieu of a wired solution; thereby reducing installation costs yet 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, security, fire, and elevator products. These devices will be developed to reduce installation costs; while increasing installation and retrofit flexibility. Sensing devices may be battery or mains powered. Actuators and area controllers will be mains powered.

To meet the cost target, these devices must have a total installed cost below that of the traditional wired alternative; yet maintain reliability on par with wired devices. The total installed cost includes the infrastructure, product, installation, commissioning, labor and operational costs of the device over its 30 year lifespan. Except for special circumstances such as flexible installation (e.g. airports) or cosmetics (e.g. museums, there is nothing compelling about installing wireless solutions inside a building unless it can be accomplished below the cost of a wired installation. This document will define the requirements necessary for wireless technology to displace wired infrastructure and meet this objective.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

TABLE OF CONTENTS

1. Terminology

6LoWPAN - 6loWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. 6lowpan is the name of the working group in the internet area of IETF. 6lowpan is the coupling that is aimed at allowing IPv6 packets to be sent to and received from Personal Area Networks, more specifically over IEEE 802.15 based networks

Actuator - A field device that modulates a flow of a gas or liquid; or controls electricity distribution..

ASHRAE - American Society of Heating, Refrigerating and Air-Conditioning Engineers

Commissioning Tool Any physical or logical device temporarily added to the network with the express purpose of setting up the network operational parameters. For interoperability purposes, devices entering the network SHOULD try to discover the commissioning tool and receive its parametric information from it. However, devices may elect to set themselves up by accessing other devices directly if the commissioning tool is not available.

NOTE: This device may also set application parameters, but is out of scope of the Network layer.

Controller - A field device that can receive sensor input and automatically change the environment in the facility by manipulating digital or analog actuators.

Field Device - Any physical device installed in the commercial building environment used to monitor and/or control some portion of the facility.

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.

FFD - Full Function Device. An 802.15.4 device that can route messages across the mesh in addition to providing an end application. Most FFD are line powered since they must always be ready to forward messages.

FMS - Facility Management System. A global term applied across all the vertical designations within a building including, HVAC, Fire, Security, Lighting and Elevator control.

HVAC - Heating, Ventilation and Air Conditioning. A term applied to the comfort level of an internal space.

IETF - Internet Engineering Task Force

Intrusion Protection ? A term used to protect resources from external infiltration. Intrusion protection systems utilize door locks, window tampers and card readers.

LLN - Low power and Lossy networks (LLNs) are typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4, Bluetooth, Low Power WiFi

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.

RFD - Reduced Function Device. An 802.15.4 device that can send messages on the network; receive messages from the network; but cannot route messages across the network. In most cases these devices are edge devices of the network.. RFDs may be line powered, but also can be battery powered since they play no role on the mesh.

ROLL - Routing over Low power and Lossy networks. This IETF working group will develop routing characteristics and rules for supporting LLNs utilizing 6LoWPAN.

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.

Sensors - A field device that monitors an environmentation condition in a building and reports its findings to higher order devices for control and alarming operations.

TC - Trust Center. A logical device on the network that is trusted by the network members. The TC administers security policy.

2. Introduction

Facility Management Systems (FMS) are deployed in a large set of vertical markets including universities; hospitals; government facilities; K-12; pharmaceutical manufacturing facilities; and single-tenant or multi-tenant office buildings. These buildings range in size from 100K sqft structures (5 story office buildings), to 1M 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 sensor, actuator and area controller and zone controller layers of the topology. (NOTE: The Building Controller and Enterprise layers of the FMS are excluded from this discussion since they typically deal in communication rates requiring IP and WLAN communication technologies. Each section describes the basic functionality of the layer, its networking model, power requirements and

a brief description of the communication requirements. Product and installation cost constraints are also included.

3. FMS Topology

3.1 Introduction

To understand the network systems requirements of a facility management system 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. Additionally, an FMS may also be divided vertically across alike, but different building subsystems such as HVAC, Fire, Security, Lighting, and Elevator control systems as depicted in Figure 1.

```
**************************************************************************
*                                                                        *
* (Note that Figure 1 does not appear in this the txt version of this    *
* document. Please see the PDF version to view the figures).             *
*                                                                        *
**************************************************************************
```

Much of the makeup of an FMS is optional and installed at the behest of the customer. Sensors and actuators have no standalone functionality. All other layers support partial or complete standalone functionality. These devices can optionally be tethered to form a more cohesive system. The customer decides how much of this vertical ?silo? will be integrated to perform the needed applications within the facility. This approach provides excellent fault tolerance since each node is designed to operate in an independent mode if the higher layers are unavailable.

3.2 Sensors/Actuators

As Figure 1 indicates an FMS may be composed of many functional 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. More recently, sensors were wired devices deployed on closed networks.
In 1995, the BACnet protocol was released by ASHRAE that defined interoperable objects and services within the HVAC silo. BACnet has grown to be an international standard now including extensions for Fire, Access, Intrusion and Lighting functions.

Another protocol widely deployed in building automation systems is LonWorks. Lonworks was submitted to ANSI and was accepted as a standard for control networking (ANSI/CEA-709.1-B). The protocol can be transported over media such as twisted pair, powerlines, fiber optics and RF.

3.3 Area Controllers

An area describes a small physical locale (300 ? 500 ft2) within a building, typically a room. As noted in Figure 1 the HVAC, Security and Lighting functions within a building address area or room level applications. 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.

The controllers deployed within a room are most often standalone devices that can provide the necessary functionality without further assistance by the higher layers of the system. However when these devices are connected to the higher system layers, these controllers can provide manual override, time series and event data to the higher layers for further analysis. Likewise, the enterprise level can then override the local control from a centralized location. When connected to the higher layers, the controllers deploy a fail-soft algorithm that reverts to local control if the higher order communication is lost.

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. Table 1 describes some examples of zones for the various functional domains within a commercial building.

Table 1 Examples of Commercial Zones

```
**************************************************************************
*                                                                        *
* Note Table 1 does not appear in this the text version of               *
* this document. Please see the PDF version to view the table.  It is    *
* captured in text form as best as possible below...                     *
```

* *
****

Functional Domain - HVAC

Zone - Air Handler ? the area served by
a single fan system; typically a
floor or adjacent floors in a
building.

Functional Domain - Lighting

Zone - A bank of lights that all
operate consistently

Functional Domain - Fire

Zone - An area of a facility that will
all operate consistently for
example fed by the same fan
system; covered by the same set
of smoke detectors or follows
the same pressurization and
annunciation rules. The zone
may also be a functional
grouping when a certain area is
governed by a set of fire
dampers.

Functional Domain - Security

Zone - A subset of the building
operating in a similar fashion
for example a logical collection
of lockable doors.

Functional Domain - Shutters

Zone - Shutter control is typically
limited to windows in a room or
in a given direction. That is,
in the morning all shutters on
the East side of the building
may close.

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.

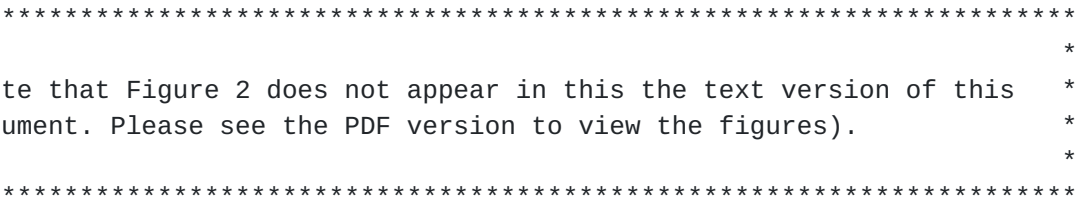
Zone controllers may have some onboard sensor inputs and also provide

direct actuation; however, zone controllers will also direct the actions of its underlings via commands as well as respond to environmental changes reported by its underlings. For example, an Air Handler controller might directly sample the duct pressure, the supply air temperature and return air temperature. However, it may also send commands to other networked devices querying the outdoor air temperature and relative humidity. Similarly, a fire panel may have all the smoke detectors directly wired; yet send commands to other adjacent fire panels to request their status if a fire condition arises.

4. Wired Communication Media

Commercial controllers are traditionally deployed in a facility using twisted pair serial media following the EIA 485 electrical standard operating nominally at 38400 to 76800 baud. This allows runs to 5000 ft without a repeater. With the maximum of three repeaters, a single communication trunk can serpentine 15000 ft.
Most sensors and virtually all actuators currently used in commercial buildings are "dumb", non-communicating hardwired devices. However, sensor buses are beginning to be deployed by vendors which are used for smart sensors and point multiplexing. The Fire industry deploys addressable fire devices, which usually use some form of proprietary communication wiring driven by fire codes. Figure 2 defines the devices, media types and protocols on the wired network.

Figure 2. Traditional Wired Media and Protocols and Controller Types



5. Wireless Communication Media

FMS vendors are now developing product line extensions that allow sensors, actuators, room controllers and area controllers to communicate wirelessly. To date, the technology of choice seems to be 802.15.4 at 2.4Ghz which has data rates comparable to wired alternatives. Figure 3 defines the network parameters for wired and wireless solutions with examples of typical connections and bit rates.

Figure 3a. Wired Network Parameters

```
  **************************************************************************
  *                                                                        *
  * Note Figure 3a does not appear in this the text version of             *
  * this document. Please see the PDF version to view the table. It is     *
```



```
  * captured in text form as best as possible below...                    *
  *                                                                        *
  **************************************************************************
```

Network Name: Sensor Bus
Media: EIA-485
Communication Rate: 9.6-76.8 kbps
Protocols Supported: BACnet MS/TP
Addressable Range: 8-bit
Typical Number of Devices Supported: 1- 16

Network Name: Field Bus
Media: EIA-485
Communication Rate: 38.4 -76.8 kbps
Protocols Supported: BACnet MS/TP
Addressable Range: 8-bit
Typical Number of Devices Supported: 1- 100

Network Name: Enterprise Bus
Media: Cat-5e
Communication Rate: 10/100 mbps
Protocols Supported: BACnet IP, Web Services, SNMP
Addressable Range: IPv4
Typical Number of Devices Supported: thousands

Figure 3b. Wireless Network Parameters

```
  **************************************************************************
```

```
  *                                                                     *
  * Note Figure 3b does not appear in this the text version of          *
  * this document. Please see the PDF version to view the table.  It is *
  * captured in text form as best as possible below...                  *
  *                                                                     *
  ***********************************************************************
```

Network Name: Sensor Bus
Media: 802.15.4
Communication Rate: 240 kbps
Protocols Supported: BACnet/802.15.4
Addressable Range: 8-bit
Typical Number of Devices Supported: 1- 10

Network Name: Field Bus
Media: 802.15.4
Communication Rate: 240 kbps
Protocols Supported: BACnet/802.15.4
Addressable Range: 8-bit
Typical Number of Devices Supported: 1- 100

Network Name: Enterprise Bus

Media: 802.11b/g
Communication Rate: 11/54 mbps
Protocols Supported: BACnet IP, Web Services, SNMP
Addressable Range: IPv4
Typical Number of Devices Supported: hundreds

6. Device Spatial Deployment

Device density differs depending on the application. 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. 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 most

often service a wing, building or the entire complex via a central plant.

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.

Fire systems are much more uniformly installed with smoke detectors installed about every 50 feet. 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.

Lighting is also very uniformly installed with ballasts installed 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.

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. Installation Procedure

Wired FMS installation is a multifaceted procedure depending on the extent of the system and the software interoperability. However, 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 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. This workflow works presently because the controller and sensor networks are dedicated.

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. Commercial Building Product Requirements

The following are the requirements for a network used to integrate building sensor actuator and control products. Note that these requirements may include requirements outside the scope of ROLL, yet must be considered as part of providing IP communications of commercial building sensing, actuating and controlling devices.

These requirements are drafted assuming that 6lowpan is the defined base protocol. Furthermore, it is assumed that the network layer will deploy a mesh architecture. If different protocols are developed or 6lowpan is redefined, some of the requirements will change.

****
*

```
  * Note the following table does not appear in this the text version of   *
  * this document. Please see the PDF version to view the table.  It is    *
  * captured in text form as best as possible below...                     *
  *                                                                        *
```

****

I. Product Requirements

1.Requirement

Solutions MUST support both wired and wireless implementations,

1. Rational

Commercial Building vendors will not support multiple product lines differentiated only by the physical layer access deployed. Local codes and product governance (e.g. UL, FM) will mandate wired alternatives for at least the next decade.

2. Requirement

Wireless devices MUST be supportable at the 2.4Ghz ISM band Wireless devices SHOULD be supportable at the 900 and 868 ISM bands as well.

2. Rational

For world-wide applicability, the 2.4gHz band must be supported. **802.15.4 also supports 900 and 868.** The routing protocol should not preclude these bands.

3. Requirement

The software stack requirements for sensors and actuators MUST be implementable in 8-bit devices with no more than 128kb of flash memory (including at least 32Kb for the application code) and no more than 8Kb of RAM (including at least 1Kb RAM available for application).

The software stack requirements for room controllers SHOULD be implementable in 8-bit devices with no more than 256kb of flash memory (including at least 32Kb for the application code) and no more than 8Kb of RAM (including at least 1Kb RAM available for application)

3. Rational

Existing sensors, actuators and controllers are deployed with this processor technology and memory size. Because of the cost sensitivity for these products, little additional resources can be added and still contain the cost point.

4. Requirement

The software stack requirements for controllers MUST be implementable in 16-bit devices with no more than 256Kb of flash memory (including at least 92Kb for the application code) and no more than 16Kb of RAM (including at least 4Kb RAM available for the application.

4. Rational

Existing controllers are deployed with this processor technology and memory size. Because of the cost sensitivity for these products, little additional resources can be added and still contain the cost point.

5. Requirement

A network (PAN) SHALL operationally support 1000 FFD and 1000 RFD devices

5. Rational

These numbers include full support for all HVAC, Fire, Lighting, Security and elevator controllers and sensors on a 50kSq ft floor plate.
This requirement assumes a PAN per floor. The FFDs and RFDs in the enfire facility will be significanltly higher.

6. Requirement

Sensor/Actuator/Controller addressability MUST be unique site wide. All addressable nodes MUST be accessible to all other nodes in the internetwork.

6. Rational

Existing technology does not support inter-PAN communication.
Building Applications require this for applications such as outdoor air/relative humidity sensing which is instrumented once but its data needs to be available network-wide.

7. Requirement

Device addressability MUST support at least 255 sensors/actuators for

each room/area controller.

7. Rational

Addressability consistent with existing ranges.

8. Requirement

Device addressability MUST support at least 255 room/area controllers for each floor controller

8. Rational

Addressability consistent with existing ranges.

9. Requirement

Devices implementing the ROLL features MUST be able to support the BACnet protocol.

9. Rational

BACnet is a world-wide ISO protocol standard that is often mandated to the commercial building vendors by the building owner. BACnet already supports an IPv4 data link and is investigating extensions for IPv6. Most FMS vendors already support BACnet. It would be extremely advantageous for 6lowpan and ROLL to support the necessary attributes to support this protocol.

10. Requirement

Devices implementing the ROLL features MUST be able to support the LON protocol.

10. Rational

LON is a commercial building control protocol especially strong in Europe.

11. Requirement

The routing protocol MUST define a communication scheme to assure compatibility of IPv4 and IPv6 devices.

11. Rational

All existing BACnet/IP devices are IPv4. The expected lifetime for a device installed in a commercial building is at least 15 years.

12. Requirement

It MUST be possible to fully commission devices from the network, without requiring any additional commissioning device (e.g. laptop). The device MAY be completely configured for network operation by setting a bank of switches. The number of switches MUST not exceed 16 switches.

12. Rational

Installers have no access to sophisticated installation equipment such as laptops. These folks prefer to simply set a bank of on-board switches to configure the device for local operation.

13. Requirement

The system MUST support devices with pre-assigned Link Local Static Addresses

13. Rational

RFD devices such as temperature sensors and smoke detectors will be installed prior to any IT network. The unique IPv6 address must be represented in the **16 bit address space currently designated in 802.15.4; and not need to**

be changed as the system is defined or as replacement devices are required.

14. Requirement

Replacement of failed devices MUST allow the new device to assume the address of the failed device without reconfiguration of additional devices in the network.

14. Rational

Inter-node application references are common across FMS systems. To support plug-and-play replaced devices must be able to assume the old device address. Replacement is typically performed by service personnel that (much like installers) have little networking experience.

15. Requirement

ROLL SHOULD add transmit power modulation algorithms to drive transmit

power to only what is necessary to route data to the next device.

15. Rational

802.15.4 does not require transmit power regulation. This combined with the collision avoidance algorithm can reduce network bandwidth efficiency when a few devices are ?shouting? packets. Empirical testing has shown that much of the parallel communication nature of the mesh can be lost when nodes are transmitting with higher power than necessary.

16. Requirement

The total installed cost including but not limited to the installation, commissioning and testing of a wireless sensor and controller MUST be at least 10% less than that of an equivalent wired device.

16. Rational

Since a wireless connection is never as reliable as a wired connection, the totally installed cost of a wireless system needs to be significantly less than that of a wired system.Also, due to local code requirements and governance (e.g. UL) , the need for wired equivalent devices will be mandated for many years even once wireless technology has been proven reliable. This forces a requirement that the wireless installation be less than a wired installation given functional equivalence. Therefore unless the overall wireless cost is at least 10%

less than the wired cost, the installers will likely select the wired alternative.

17. Requirement

Sensing devices MUST be supportable using battery (or other non-line based) power. The solution MUST support power savings modes that will support devices accessing the network at a rate of not more than 1/minute at a duration time of less than 5 msec to operate with not more than 2 AA alkaline cells for duration of not less than 5 years.

17. Rational

Existing 802.15.4 mesh implementation?s sleep mechanism supports this level of power. Existing implementations already support this level of power efficiencies.

18. Requirement

RFDs SHOULD target for operation using viable energy harvesting techniques such as ambient light, mechanical action, solar load, air pressure and differential temperature.

18. Rational

(NOTE: This paragraph intentionally left empty)

19. Requirement

To support high speed code downloads, a mechanism MUST be defined to download FFD devices in parallel yet support guaranteed delivery.

Devices receiving a high speed download
MAY cease normal operation, but upon completion of the download MUST automatically resume application and complete network operation.

19. Rational

Required mode to expeditiously download 100 controllers/sensors simultaneously. Serial updates of controllers do not meet customer expectations for ?downtime? and increase preventive maintenance on-site time by vendor techs.

9. Installation/Commissioning Requirements

The following are the installation and commissioning requirements for a network used to integrate building sensor actuator and control products. Note that these requirements may include requirements outside the scope of ROLL, yet must be considered as part of providing IP communications of commercial building sensing, actuating and controlling devices.

****
*

```
  * Note the following table does not appear in this the text version of   *
  * this document. Please see the PDF version to view the table.  It is    *
  * captured in text form as best as possible below...                     *
  *                                                                        *
  **************************************************************************
```

II. Installation/Commissioning Requirements

20. Requirement

Product installation and local network communication verification MUST be performed by traditional trades people (e.g. electricians) unfamiliar with IT communication technologies and procedures.

20. Rational

To maintain existing installation costs, installation needs to be provided by existing resources in the existing work flow.

The typical installation workflow commences with the electrician installing the room level devices. He/she must then be able to verify acceptable local operation. Sensors, actuators and controllers are typically installed prior to sheet wall and ceiling installation. These devices must be commissioned and checked out prior to the typical installation of the IT server network

21. Requirement

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

21. Rational

Currently, the installer simply needs to set an address using an on the on-board means (e.g. switches) to fully define the network settings for the device.

22. Requirement

Product commissioning MUST be performed by an application engineer prior to the installation of the IT network.

22. Rational

Application engineers typically carry electronics such as a laptop and/or PDA but are not familiar with IT devices such as DNS and DHCP servers.Typically the IT network is not installed at the time that the room and equipment controllers are commissioned for local control.

NOTE: This was not at issue with EIA-485 or existing 802.15.4 mesh infrastructures since these dedicated infrastructures were installed concurrently with the devices.

23. Requirement

A seamless means of merging PANs MUST be defined.

23. Rational

Installation of a large building is typically done in parallel by many resources. Each resource will want to work in his/her area independently, yet the fully commissioned system must operate cohesively under a single PAN

24. Requirement

Network setup MUST support network commissioning times of no more than 15 minutes per sensor/controller pair.

24. Rational

Current sensor/controller pairs can be configured with network parameters in less than 15 minutes. See below for allowable setup times for network security.

25. Requirement

For wireless implementations, solutions MUST support a total material, apportioned backhaul and labor cost not to exceed $1.00/ft as compared to a wired implementation.

25. Rational

This cost follows existing wired cost models

26. Requirement

Devices SHOULD support an ?ad hoc? like mode (ala 802.11) allowing for temporary point-to-point communication during the download and commissioning phase. AD HOC mode MAY be mutually exclusive from normal operational mode.

26. Rational

To assist in simple installation, an ad hoc mode (similar to 802.11) SHOULD be considered for easy point-to-point commissioning of the device.

```
**************************************************************************
*                                                                        *
* Note the following table does not appear in this the text version of   *
* this document. Please see the PDF version to view the table.  It is    *
* captured in text form as best as possible below...                     *
*                                                                        *
**************************************************************************
```

10. Networking Requirements

The following are the networking requirements for a network used to integrate building sensor actuator and control products. Note that these requirements may include requirements outside the scope of ROLL, yet must be considered as part of providing IP communications of commercial building sensing, actuating and controlling devices

III. Network Requirements

27. Requirement

Routing MUST support unicast, multicast and broadcast services (or IPv6 equivalent)

27. Rational

Commercial building devices must interact. While installed independently, they must discover needed devices, objects and services at boot.

28. Requirement

Packet disassembly and reassembly (i.e. fragmentation) MUST

support packet sizes to 512 octets.

28. Rational

BACnet MS/TP supports a 501 NPDU octet size for its sensor/controllers networks.

29. Requirement

Discovery domains SHALL be provided to minimize traffic infiltration beyond what is necessary. Discovery is needed to find devices and bind objects.

29. Rational

For node discovery, local and global broadcast domains must be supported (or IPv6 equivalent)

30. Requirement

Nodes MUST be able to be logically grouped at the network layer (e.g. multicast, VLAN). New members MUST be able to be added to the group; existing members MUST be deletable from the group.

30. Rational

Currently the hierarchical network structure provides clean independence from subnet to subnet. This mechanism needs to be maintained even though IP is a flat network space.

31. Requirement

Addressing MUST allow devices to join a logical group (e.g.

VLAN) and then transparently operate
within the domain of the group.

31. Rational

Existing hierarchical wired topology supports this requirement.

32. Requirement

Connection based and connectionless services MUST be supported

32. Rational

All existing FMS IP communication uses UDP with BACnet providing transport services. Connection based services are also required for applications such as code downloads

33. Requirement

Routers MUST support quality of service prioritization to assure timely response for critical FMS packets (e.g. Fire and Security events)

33. Rational

Network prioritization is already supported in BACnet and must be supported on the ROLL networks.

34. Requirement

Path selection MUST be based on path quality, rather than signal strength only. Path quality includes signal strength, available bandwidth, hop count and communication error rates.

34. Rational

Existing wireless systems determine path on RSSI only which is not always suitable.

35. Requirement

Communication paths MUST adapt toward optimality in time.

35. Rational

On demand algorithms will not optimize paths until needed.

Empirical testing has shown that a commercial building recovering from a momentary loss of power will have a very random device recovery. This leads to obtuse non-optimal communication paths. Periodical path rediscovery of routers will optimize paths and reduce latency.

36. Requirement

To augment real-time performance, the network layer SHOULD be configurable to allow secondary and tertiary paths to be established and used upon failure of the primary path

36. Rational

Real-time applications often cannot incur the added latency of path discovery. Nodes SHOULD try to establish alternate source/destination paths that can readily be used SHOULD the primary path fail.

37. Requirement

Devices SHOULD optionally persist communication paths across boots

37. Rational

Empirical testing has shown that path discover and orphan

reassignments of devices at boot can heavily effect network performance. Devices SHOULD be directed by the application to either maintain or purge path information in warm-start and cold-start conditions.

38. Requirement

The route discovery mechanism SHOULD allow a source
node (sensor) to dictate a configured destination node

(controller) as a preferred routing path.

38. Rational

Many room controllers will interact locally
with sensors and actuators (within 30 feet). In these
cases the sensor/actuator binding SHOULD allow
the application to select the child/parent
preferred path. This will reduce unnecessary network
traffic.

Some existing wireless systems select paths without
input from the application.

39. Requirement

The network layer SHOULD support both asymmetric and
symmetric routes as requested by the application layer.
When the application layer selects asymmetry the network
layer MAY elect to find either asymmetric or
symmetric routes. When the application layer requests
symmetric routes, then only symmetric routes SHALL be
utilized.The default SHALL be asymmetric routes.

39. Rational

Asymmetric paths typically promote better overall
communication between nodes at the cost of varied
latency times and excess path discovery
broadcasts.Symmetric paths reduce path
discoveries especially in applications where
every message expects a response.The application
SHOULD be able to configure this network feature.

40. Requirement

Mobile devices SHOULD be capable of joining a new PAN and
associating to that network within 15 seconds.

40. Rational

Certain features such as location tracking must
support mobility. The association requirement is
heavily relaxed from streaming applications such as
VoIP, but yet must perform at a level to assure building
communication continuity,

41. Requirement

RFDs MUST be able to receive information from
other devices on a regular basis.

41. Rational

Existing existing 802.15.4 mesh implementations only
cache 1 message from 1 parent to all children for only 7
seconds. This communication mechanism is too
restrictive. Sleeping RFD must have a more robust
mechanism defined to receive message of
interest when they awake.

42. Requirement

Commercial Building FFD and RFD devices MUST all be
periodically monitored to assure that the device is
viable and can communicate data and alarm information as needed.

42. Rational

The overhead to support this requirement at the
application layer will inordinately effect network
traffic. The network layer SHOULD maintain on-going
traffic tables to indirectly assure that the network
nodes are operable.

43. Requirement

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

43. Rational

Current event based systems require 10kbps sustained
throughput. Polled system will require
more bandwidth.

44. Requirement

The network MUST automatically detect interference and migrate the network to a better 802.15.4 channel to improve communication. Channel changes and nodes response to the channel change MUST occur within 60 seconds

44. Rational

Existing 802.15.4 mesh implementations have begun deploying frequency agility after empirical testing indicates that scaled networks cannot reside on a single channel without interference.

45. Requirement

ROLL MUST adhere to the existing 802.15.4 frame format and MUST not impinge on the available payload size

45. Rational

The existing 128 octet packet supports only about an 80 byte payload. Reducing this payload size to include more overhead will reduce the types of applications that can successfully be deployed.

46. Requirement

To improve diagnostics, the network layer SHOULD be able to be placed in and out of ?verbose? mode. Verbose mode is a temporary debugging mode that provides additional communication information including at least total number of packets sent, packets received, number of failed communication attempts, neighbor table and routing table entries.

46. Rational

The dynamic path discovery mechanisms used in a mesh networks continually alter the communication paths, latency and reliability. It is currently very

difficult to extract communication data from the stack to analyze failures. The stack SHOULD incorporate intrinsic mechanisms.

47. Requirement

Network diagnostics such as PING and Trace Route
SHOULD be supported with extensions in Trace Route
describing wireless parameter information.

47. Rational

The dynamic path discovery mechanisms used in a mesh
networks continually alter the communication paths,
latency and reliability. It is currently very difficult to
extract communication data from the stack to
analyze failures. The stack SHOULD
incorporate intrinsic mechanisms.

48. Requirement

A node transmitting a ?request with
expected reply? to another node SHALL 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.

48. Rational

Measured empirical data from existing embedded mesh
networks using the 15.4 radio.

49. Requirement

Reliability SHALL 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% App?n layer
errors on all
messages.

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

49. Rational

Measured empirical data from existing embedded mesh
networks using the 802.15.4 radio.

50. Requirement

The ROLL device SHALL support neighbor tables with
a minimum of 16 entries.ROLL routing SHALL
age neighbor table entries to assure table integrity

50. Rational

Consistent with existing meshing algorithms.

51. Requirement

The ROLL device SHALL support routing tables with a minimum
of 32 entries.ROLL routing SHALL age routing table
entries to assure table integrity

51. Rational

Consistent with existing meshing algorithms.

52. Requirement

ROLL routing SHALL support router table entry sizes
adjustable on a per node basis.

52. Rational

Due to the non-uniform nature of the message flow within commercial buildings, some nodes will require significantly more routes than other nodes.

53. Requirement

All nodes in the system MUST support upwards to 10 hop paths to other nodes in the system.

53. Rational

802.15.4 devices operate best inside buildings at 75 to 100 feet. This requirement will allow source devices to be placed 750 to 1000 feet from its destination device.

54. Requirement

The system MUST support several priority levels according to the IP QoS information.

54. Rational

The Fire and Security domains must transmit packets without the threat of being bogged down by the HVAC, Lighting and Shuttering domains.

```
**************************************************************************
*                                                                        *
* Note the following table does not appear in this the text version of   *
* this document. Please see the PDF version to view the table.  It is    *
* captured in text form as best as possible below...                     *
*                                                                        *
**************************************************************************
```

11. Security Considerations

The following are the security requirements for a network used to integrate building sensor actuator and control products. Note that these

requirements may include requirements outside the scope of ROLL, yet must

be considered as part of providing IP communications of commercial building sensing, actuating and controlling devices.

11.1 Security Requirements

55. Requirement

Devices MUST optionally support a network security policy that includes but is not limited to device and user authentication; payload (only) encryption and packet encryption.

55. Rational

The commercial building market is very diverse ranging from privately owned office buildings to military complexes such as the Pentagon. The security models deployed need to be robust and adaptable to the threat level expected.

56. Requirement

Network security MUST thwart malicious intent including but not limited to broadcast storms, spoofing and replay attacks

56. Rational

As with all networks (especially wireless networks), miscreants can deleteriously effect the network operation and performance. A robust set of security policies are required to thwart these attempts; yet must fit into the processor and memory footprint prescribed above.

57. Requirement

Configuration and Operational network security policies MUST be supportable on all devices. ?out-of-box? security

policy SHALL be ?disabled?, but configurable to its
needed level on site. At the customer?s discretion the
security policy SHALL remain ?disabled? during system
operation.

57. Rational

The security policy must be tailored for the installation. As noted in the installation requirements, the installer has no security threat to deal with since the building is not yet occupied. Setting all security ?off? as the out-of-box state allows the installer to complete his task unimpeded.

58. Requirement

The routing protocol MUST allow changing security policies via network operations. The routing protocol MUST also allow changing security policies at the device or out-of-band.Changing security policies MAY require another device (e.g. laptop) to implement.

58. Rational

Since the installer will not be setting security, the devices will need to have their security policies defined en masse over the network. However, as new devices are added to the network at a later date, or failed devices are replaced, the security policy also needs to be administered locally.

59. Requirement

Security policies MUST be increasable or decreasable in the field. Changing security policies can only effect the changed node for no more than 15 minute duration. It can have no ill effect on other operational modes in the network. Changing security policies SHALL not require a network restart. If MAY however require the effected node to be restarted.

59. Rational

Due to the dynamic nature of the buildings and devices, security policies must be easily administered and changed across the network.

60. Requirement

Security policies must be settable and resettable on devices

that are not physically accessible and have no integrated displays

60. Rational

Current implementations support a TC that
can send security information across the air to all
devices.

61. Requirement

While the network is being changed, devices MUST
temporarily support both security policies until the
entire network has been modified. Once modified, devices
MUST not continue to support both policies

61. Rational

Commercial building systems are mission critical real-time
systems that must maintain operation during systemic
events.

62. Requirement

Additional network devices MUST not be required
including Network Managers, Trust Centers and
coordinators. This is not to say that these functions
cannot exist, only to say that they must not be targeted to
devices that only support that sole function.

62. Rational

FMS customers do not want to pay for ?boxes? that add no
application value to their system.

63. Requirement

Devices critical to network operation (e.g. Network Coordinators, Trust Centers) MUST support redundancy mechanisms. Failed network devices MUST optionally be

assigned secondary devices that will assume these functions in less than 2 minutes from failure.

OR

The network architecture MUST allow continued, albeit reduced functionality, if the critical device(s) fail or are somehow disconnected from the network.

63. Rational

Mission critical systems cannot fail and hence have network policies that allow continued operation in case of device failures.

64. Requirement

The network MUST support multiple security policies simultaneously.

64. Rational

RFD (e.g. temperature sensors) may not require any security yet controllers may require some level of security. The HVAC domain may require minimal security; yet the Fire domain may require high security. These need to be on-site customer decisions.

65. Requirement

Device authentication MUST be supported

65. Rational

The Fire domain requires proper authentication from the user device to assure proper clearance when resetting a fire panel.

11.2 Security Use Cases

The following are the security use cases further detail the requirements

upon the system nodes for different levels of security. The five use cases are not exhaustive of the commercial building market, but are a reasonable spectrum of cases covering many of the needs. Each of the cases is further detailed by three sections ? 1) use case specifications, 2) allowed setup time and 3) allowed network disturbance.

```
**************************************************************************
*                                                                        *
* Note the following table does not appear in this the text version of   *
* this document. Please see the PDF version to view the table.  It is    *
* captured in text form as best as possible below...                     *
*                                                                        *
**************************************************************************
```

11.2.1 No Security Threat

Site Characteristics - Private Office Buildings,Single Building
Single Tenant Facility, Owner Occupied, Not vendor interoperable,
No Public access to facility

Commercial Applications - HVAC, Lighting

Governance - None

Threats - None. Building occupants have no reason to be a security risk

Allowed time to setup network security when:

Merging Commissioned Islands - 15 minutes to allow one TC to acquiesce to
the other TC. All device security SHOULD be the same.
If on different PANs, allow 20 minutes for PAN change.

Increasing Security Policy - A network SHOULD be able to monotonically
increase its security policy. All devices within
the PAN MUST detect the policy change and increase its policy
within 10 minutes.

Installing Devices - 0 minutes per device

Replacing Devices - 0 minutes per device

Allowed Network Disturbance when:

Merging Commissioned Islands - Devices on the island being added MUST not be affected by the coalescence of the islands.
Devices being moved MAY be effected while movement occurs

Increasing Security Policy - All PAN Devices MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST

support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Reverting to Commissioning Mode - Not applicable since already at lowest security level.

Commissioning Tool not available on-line - System MUST operate without effect, New devices can be added using existing default key either by off-band means or from operational Commissioning Tool

Trust Center fails - System MUST operate without
affect, New devices can be added using existing default key either by off-band means or from operational Commissioning Tool

New Software Update Downloaded - Network Security feature MUST be unaffected by software download. Only the device currently being upgraded affected.

New Device Added = There MUST be no disruption of the existing network

Failed Device Replaced - (RFD) - associated FFD (i.e.
parent) MAY be affected when RFD
replaced. (FFD) - associated RFD(s) MAY be
affected while FFD replaced. Remaining network not affected

11.2.2 Low Security Threat

Site Characteristics - Commercial Real Estate,
Multi-tenant facilities, Universities, Health Care,

Vendor interoperability

Commercial Applications - HVAC, Lighting, Door Access
Video Monitoring

Governance - None

Threats - Miscreants (aka students) causing havoc

Allowed time to setup network security when:

Merging Commissioned Islands - 10 minutes to merge once TC to acquiesce to the other TC established. The merge shall occur automatically without requiring the installer to visit each PAN device.

Increasing Security Policy - A network SHOULD be able to monotonically increase its security policy. All devices within the PAN MUST detect the policy change and increase its policy within 10 minutes.

Installing Devices - 1 minute per device

Replacing Devices - 1 minute per device

Allowed Network Disturbance when:

Merging Commissioned Islands - Devices on the island being added will not be effected by the coalescence of the islands. Devices being moved can be effected while movement occurs

Increasing Security Policy - All PAN Devices MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Reverting to Commissioning Mode - A PAN MUST be able to revert back to its commissioning state and its 'out of the box' security policy. One device, multiple devices or all devices in the PAN MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Commissioning Tool not available on-line - System operates without effect,

New devices can be added using existing key either by off-band
means or from operational Commissioning Tool

Trust Center fails - System operates without effect,
New devices can be added using existing key either by off-band

means or from operational Commissioning Tool
New Software Update Downloaded - Network Security feature uneffected by software download. Only the device currently being upgraded effected. Device will get security info either through out-of-band means or TC.

New Device Added No disruption of existing network

Failed Device Replaced - RFD - associated FFD (i.e. parent) MAY be effected when RFD replaced. FFD - associated RFD (s) MAY be effected while FFD replaced. Remaining network not effected

11.2.3 Medium Security Threat

Site Characteristics - High Occupancy, High Rise Buildings

Commercial Applications - HVAC, Lighting, Door Access, Video Surveillance, UL Smoke Control, Fire Secondary Reporting

Governance - UL,ULC

Threats - Device Authentication on specific devices only to assure automatic device control occurring only to specific devices.

Allowed time to setup network security when:

Merging Commissioned Islands - 10 minutes to merge once TC to acquiesce to the other TC established. The merge shall occur automatically without requiring the installer to visit each PAN device.

Increasing Security Policy - A network SHOULD be able to monotonically increase its security policy. All devices within the PAN MUST detect the policy change and increase its policy within 10 minutes.

Installing Devices - 5 minutes per device requiring authentication, 1 minute for all other devices.

Replacing Devices - 10 minutes per device requiring authentication, 1 minute for all other devices.No devices can be added to the system unless authorized by the TC.

Allowed Network Disturbance when:

Merging Commissioned Islands - Devices on the island being added will not be effected by the coalescence of the islands. Devices being moved can be effected while movement occurs

Increasing Security Policy - All PAN Devices MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Reverting to Commissioning Mode - A PAN MUST be able to revert back to its commissioning state and its 'out of the box' security policy. One device, multiple devices or all devices in the PAN MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Commissioning Tool not available on-line - Devices can be added to the secure network by accessing the Trust Center directly.

Trust Center fails - System still operates. No new devices can be added until the TC is again operational. A report of the TC failure is forwarded to the user.

New Software Update Downloaded - New software cannot be downloaded to the device until it authenticates the software and device. The system MUST continue to run uneffected.

New Device Added - No disruption of existing network

Failed Device Replaced - RFD - associated FFD (i.e. parent) MAY be effected when RFD replaced. FFD - associated RFD (s) MAY be effected while FFD replaced. Remaining network not effected

11.2.4 High Security Threat

Site Characteristics - Clean Rooms, Hospital ORs, Pharmeceuticals

Commercial Applications - HVAC, Lighting, Door Access, Video Surveillance
UL Smoke Control, Secondary Reporting,Primary Fire Reporting,
Critical Environments

Governance - UL,ULC,FDA

Threats - Device Authentication on specific devices only to assure automatic device control and user access occurring only to specific devices.

Allowed time to setup network security when:

Merging Commissioned Islands - 10 minutes to merge once TC to acquiesce to the other TC established. The merge shall occur automatically without requiring the installer to visit each PAN device.

Increasing Security Policy - A network SHOULD be able to monotonically increase its security policy. All devices within the PAN MUST detect the policy change and increase its policy within 10 minutes.

Installing Devices - 5 minutes per device requiring authentication, 1 minute for all other devices.

Replacing Devices - 10 minutes per device requiring authentication, 1 minute for all other devices

No devices can be added to the system unless authorized by the TC.

Allowed Network Disturbance when:

Merging Commissioned Islands - Devices on the island being added will not be effected by the coalescence of the islands. Devices being moved can be effected while movement occurs

Increasing Security Policy - All PAN Devices MUST be made

aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Reverting to Commissioning Mode - A PAN MUST be able to revert back to its commissioning state and its 'out of the box' security policy. One device, multiple devices or all devices in the PAN MUST be made aware of the impending policy change. No impact can occur on the network at this time. Once the change commences, devices on the PAN MUST support both policies temporarily until the TC explicitly tells the device to use the new policy. At that point, the old policy MUST be inactivated.

Commissioning Tool not available on-line - Devices can be added to the secure network by accessing the Trust Center directly.

Trust Center fails - System still operates. No new devices can be added until the TC is again operational. A report of the TC failure is forwarded to the user.

New Software Update Downloaded - New software cannot be downloaded

to the device until it authenticates the software and device. The system MUST continue to run uneffected.

New Device Added - Devices MUST be added at a scheduled time convenient to the customer. The network MAY be down while they are added. Better though if it need not be down.

Failed Device Replaced - RFD - associated FFD (i.e. parent) MAY be effected when RFD replaced. FFD - associated RFD (s) MAY be effected while FFD replaced. Remaining network not effected.

11.2.5 Very High Security Threat

Site Characteristics - Government, Military, Homeland Security

Commercial Applications - HVAC, Lighting, Door Access, Video Surveillance, UL Smoke Control, Secondary Reporting, Primary Fire Reporting, Critical Environments

Governance - UL, ULC, FDA, CoE

Threats - Access onto the network at all
times MUST be protected (i.e. joining). Security key
definition MUST be protected from malicious surveillance of the

network. Once authenticated onto the network, all data messages MUST be encrypted to ward against malicious intent.

Allowed time to setup network security when:

Merging Commissioned Islands - 10 minutes to merge once TC to acquiesce to the other TC established. The merge shall occur automatically without requiring the installer to visit each PAN device.

Increasing Security Policy - Not applicable since at the highest security level. Reducing security would defeat the application and would need to be a scheduled activity.

Installing Devices - Devices will be out-of-band configured with the security policy. The TC will need to be manually configured to allow the device to join the network.

Replacing Devices - Devices will be out-of-band configured with the security policy. The TC will need to be manually configured to allow the device to join the network.

Allowed Network Disturbance when:

Merging Commissioned Islands - The Commissioning device MUST be a trusted configured node on the network as are all other devices. Nodes already on the network cannot be deleteriously effected by the addition of the new nodes. Each device being added to the network MUST be manually added through user authentication at the TC.

Increasing Security Policy - Not applicable since at the highest security level. Reducing security would defeat the application and would need to be a scheduled activity.

Reverting to Commissioning Mode - Not applicable, the network will always be in its operable security state. The commissioning tool MUST be added to the network and execute the same security policies as do all other nodes.

Commissioning Tool not available on-line - Devices can be added to the secure network by accessing the Trust Center directly.

Trust Center fails - System remains in 'secure join' mode. No device except the failed TC can be added to the network.

New Software Update Downloaded - The downloading device MUST join the network. The downloading device MUST authenticate to each device being downloaded before the download commences. All existing security data is lost as the new software downloads. Once downloaded, the device MUST reestablish itself onto the network via a manual network join operation.

New Device Added - New devices MAY be manually authenticated to the network via a manual network join operation. Once joined, the device MUST obtain its security information in a secured manner.

Failed Device Replaced - New devices MAY be manually authenticated to the network via a manual network join operation. Once joined, the device MUST obtain its security information in a secured manner.

12. Traffic Patterns

TBD

13. Open Issues

Other items to be addressed in further revisions of this document include traffic patterns.

14. IANA Considerations

This document includes no request to IANA.

15. Acknowledgements

Thanks to the Johnson Control internal review team that provided over 150 insightful comments during the requirements inspection.

Additional thanks to the ZigBee Commercial Building Automation (CBA) Profile Group for their input on the Security Use Cases.

16. References

16.1 Normative References

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

16.2 Informative References

[I-D.culler-roll-routing-reqs]
J.P. Vasseur and D. Culler, "Routing Requirements for Low-Power Wireless Networks", draft-culler-roll-routing-reqs-00 (work in progress), July 2007.

[draft-brandt-roll-home-routing-reqs-01]
A. Brand and J.P. Vasseur, "Home Automation Routing Requirement in Low Power and Lossy Networks," draft-brandt-roll-home-routing-reqs-01 (work in progress), July 2007.

[draft-pister-roll-indus-routing-reqs-01]
Industrial Routing Requirements in Low Power and Lossy Networks
draft-ietf-roll-indus-routing-reqs-00, April 2008

BACnet ? A Data Communication Protocol for Building Automation and Control Networks.
ANSI/ASHRAE Standard 134-2004

Authors' Addresses

Jerry Martocci
Johnson Controls Inc.
507 E. Michigan Street
Milwaukee, Wisconsin 53201 USA
Email: jerald.p.martocci@jci.com

Ted Humpal
Johnson Controls Inc.
507 E. Michigan Street
Milwaukee, Wisconsin 53201, USA
Email: ted.humpal@jci.com

Nicolas Riou
nicolas.riou@fr.schneider-electric.com

Jon Williamsson
jon.williamson@tac.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).