CABA

North America's Home & Building Automation Association

Best-Practices Guide for Evaluating Intelligent Building Technologies

IS 2002-28

This Report is provided exclusively to CABA members, at no charge.

Continental Automated Buildings Association

INFORMATION SERIES

Continental Automated Buildings Association

CABA is pleased to provide this publication in the interest of furthering discussion and education in the home and building automation industry. **CABA** members can obtain additional copies by contacting:

CABA

North America's Home & Building Automation Association

M-20, 1200 Montreal Road, Ottawa, ON K1A 0R6
Tel: 613.990.7407; Fax: 613.991.9990
E-mail: caba@caba.org
Web: www.caba.org

Membership and publications inquiries: 1.888.798.CABA (2222)

This Report is provided exclusively to CABA members, at no charge

.

Best-Practices Guide for Evaluating Intelligent Building Technologies

IS-2002-28

Best-Practices Guide for Evaluating Intelligent Building Technologies

Acknowledgements

Funded by:

Industry Canada   Industrie Canada

Public Works and Government Services Canada   Travaux publics et Services gouvernementaux Canada

Developed by:

Kenneth P. Wacks, Ph.D.
Management & Engineering Consultant
9 Pinewood Road
Stoneham, MA 02180
Tel: 781.662.6211, Fax: 781.665.4311
E-mail: kenn@alum.mit.edu
Web site: www.kenwacks.com

with valuable assistance from the following systems specialists from Public Works and Government Services Canada (PWGSC):

- Edward Morofsky (Building Energy & Control Engineering Specialist)
- Ben Stach (HVAC Building Systems Controls)
- Ivan Pasini (Lighting)
- Tony Colantonio (Building Envelope)
- Simon Foo (Smart Structures)
- Marek Dziedzic (Connectivity)
- Karen Pero (Productivity / Work Environment)
- Ed Kutrowski (Energy R&D)
- Brian Kyle (Facilities Life-cycle Management)
- H. Vaidyanathan (Digital Simulation/Animation)
  and
- Winston Hetherington (Building Automation) from BASS Consultants.

Project Management by:

Kirk McElwan, Technical Director
Continental Automated Buildings Association (CABA)
Building M-20, 1200 Montreal Road
Ottawa, ON K1A 0R6

December 2, 2002

TABLE OF CONTENTS

1 INTRODUCTION 1

2 CATEGORIES FOR SUBSYSTEM TECHNOLOGIES 3

3 AUDIENCE FOR THIS GUIDE 3

3.1 Criteria Cross Reference to PWGSC Project Phases Table 6

4 CRITERIA ORGANIZED BY CATEGORY 7

4.1 SUBSYSTEM OPERATION WITHOUT NETWORK CONNECTION 7

4.1.1 Features 8
4.1.2 Performance 8
4.1.3 Operating Environment Factors 9
4.1.4 Failure and Emergency Operations 10
4.1.5 Support and Maintenance 10

4.2 SUBSYSTEM OPERATION IN A BUILDING AUTOMATION ENVIRONMENT 12

4.2.1 Interaction with Other Subsystems 13
4.2.2 BAS Equipment 14
4.2.3 BAS Features 15
4.2.4 BAS Management Issues 17
4.2.5 System Management Issues 17
4.2.6 Communications Protocol Issues 19
4.2.7 Application Layer Features 20
4.2.8 Lower Layer Features 21

4.3 SUBSYSTEM BUSINESS CONSIDERATIONS 22

4.3.1 Subsystem Manufacturer 22
4.3.2 Documentation 23
4.3.3 Cost / Benefit Issues 24
4.3.4 Training Availability 26
4.3.5 Industry Education 27

1. Introduction

This guide builds upon the *Technology Roadmap for Intelligent Building Technology*, where an Intelligent Building is defined as:

> *A building and its infrastructure providing the owner, operator and occupant with an environment that is flexible, effective, comfortable and secure through the use of integrated technological building systems, communications and controls.*

Ideally, a building is judged intelligent when the building subsystems provide the occupants with productive and comfortable conditions by responding to and enhancing the workplace environment. A century ago comfort was judged very differently from now because of expectations fueled by advances in technology. Back then, large windows were important for delivering light and fresh air. The primary objective was productivity, not comfort. Occupants needed light to see their work and reduce accidents, and fresh air to keep them awake. Comfort is now being measured in terms of ergonomics, which seeks to decrease discomfort by reducing heath risks. Thus, the choices of building subsystem technologies greatly influence the perception and measure of an Intelligent Building. For this reason, this best-practices guide focuses on technical and business issues that can be evaluated and scored objectively compared to judgements of comfort.

Please note this guide will need to be updated as new technologies make refinements in building control feasible. For example, the proliferation of dimmable lights for comfort and energy management was made possible in recent decades by the introduction of sophisticated electronic ballasts for fluorescent lamps.[1]

Building control has traditionally been organized into autonomous subsystems such as lighting and HVAC control. As buildings are automated, these formerly independent subsystems are interconnected to deliver integrated services. Interconnection among subsystems is enabled by equipping each subsystem with facilities for data communications. Therefore, topics such as communications protocols and local area networks become important as integration enablers.

A key characteristic of intelligent building technology is subsystem synergies. In an intelligent building, the infrastructure services of each subsystem are monitored and controlled through a common network that is integrated to form a homogeneous and interoperable system. The value of such a system is greater than the sum of its parts

[1] For further information about comfort and end-user satisfaction in relation to specific technologies and the intelligent building, please see "Sustainable Design Can Be an Asset to the Bottom Line" by Judith Heerwagen, Ph.D. in *Environmental Design + Construction*, July 15, 2002 (www.edcmag.com). She references the Balanced Scorecard (BSC), developed by Robert Kaplan and David Norton in 1996. According to Dr. Heerwagen, the BSC "assesses four categories of performance [of sustainable buildings]: financial, business process, customer/stakeholder relations and human capital development."

through the interaction of subsystems. Examples of interaction include the coordination of HVAC, security, and lighting subsystems, so only occupied areas of buildings are cooled and illuminated.

This guide consists of criteria by which intelligent building technologies can be evaluated. The topics in this guide are important for various audiences, such as building owners and managers, intelligent building designers, installers, etc. Also, these criteria are relevant at various stages of building planning, construction, commissioning, and operations. The following phases have been specified in the Public Works and Government Services Canada (PWGSC) *Project Management Practice Standard*:

a) Planning

b) Definition

c) Implementation

d) Commissioning

e) Operating

f) Evaluation

Candidate technologies applicable to the following subsystems will be considered for evaluation:

a) Security and access control

b) Lighting

c) Life safety

d) HVAC

e) Vertical transport (elevators and escalators)

f) Energy management and power distribution

g) Tenant telecommunications (telephone, data networks)

h) Communications within the public spaces (public address, elevators)

i) Building structure monitoring (leaks, corrosion, etc.)

Please note that this list was determined by consensus of the managers of this project. Possible extensions of this list might include:

a) Metering and monitoring of natural gas and other outside energy sources.

b) Monitoring and control of potable water and hot water for domestic use.

2. Categories for Subsystem Technologies

This section organizes the criteria for evaluating intelligent building subsystem technologies into broad categories. The specific criteria are described in Section 4 of this report.

The abbreviation *BAS* means Building Automation System. This term will be used when referring to the communications network infrastructure for building automation. The use of BAS avoids confusion with a network for data and other networks that will be operating in the building whether the building is smart or not.

A BAS communications network interconnects subsystems. The term *subsystem* includes the nine categories of services defined in the previous section (security, lighting, HVAC, etc.). The typical equipment constituting a subsystem includes sensors, actuators, user interfaces, and controllers. The term *node* refers generically to any of these components in a subsystem that may be connected to a communications network.

3. Audience for this Guide

As noted in the introduction, the criteria are relevant for various stages of building planning, construction, commissioning, and operations. Table 3.1 shows which criteria categories apply at each PWGSC project stage. Please note that some criteria categories affect more than one project stage. This list reflects the judgement of the PWGSC team that participated in this project and the author.

Intelligent building subsystems and building automation systems are integral to daily activities in the building and affect building owners, managers, building engineers, technicians, and tenants. Thus, all parties should be involved in selecting subsystems and network functions to complement their responsibilities. In practice, however, intelligent building features are selected during the planning and design phases prior to building construction or renovation.

According to PWGSC, the team involved in a building project includes:

a) Project Leader (Owner/Investor)

b) Project Manager (Implementor)

c) Facilities Manager (Operator)

d) Tenant/User

In addition, this team is supplemented by consultants and contractors. The entire building project team is the audience for this guide. If consultants are assigned tasks to select building automation technologies, they should consider the needs of the actual users. They are expected to be aware of the options and to understand the activities of the ultimate users: building engineers, service technicians, facility operators, building managers, tenants, and even visitors.

PWGSC defines the project stages as follows:

a) Planning Phase

   1) Establish consensus on the requirements of the client and the range of options to be explored.

   2) Determine regulatory considerations and any preliminary investigations needed.

   3) Prepare data and descriptions required for project approval by the owner/investor, including a list of options and recommended choices.

   4) Assist the owner/investor in preparing an investment analysis, budget, schedule, organization, and controls.

b) Definition Phase

   1) Provide further clarification to the planning phase.

   2) Determine the tasks and resources required.

   3) Secure funding.

   4) Secure regulatory approvals.

   5) Define the project plan in detail.

   6) Establish control mechanisms for the project.

7) Define consulting services needed and select consultants.

c) Implementation Phase

1) Organize and share information with the project team.

2) Establish financial and work-product controls.

3) Create designs and evaluate them against the project goals including the budget.

4) Create plans and specifications for tender to select contractors.

5) Proceed with construction. Evaluate the contractors and consultants to confirm completion of contract obligations.

d) Commissioning Phase

1) Ensure that the financial goals have been met.

2) Transition from construction to operation.

3) Transfer from implementers to owner/investor to operator.

4) Start up systems, test, and adjust operation. Confirm performance and acquire permits.

e) Operating Phase

This phase is complete when "there is a facility in service that responds to the opportunity or need identified by the client during the planning phase." [Section 3.5 of PWGSC *Project Delivery System*.]

1) Establish, test, and record the operating performance of the building systems.

2) Establish a preventative maintenance program.

3) Define an operating and maintenance budget.

4) Respond to specific requests for services from the owner/investor.

f) Evaluation Phase

During this phase the owner/investor determines how well the building project conforms with plans in areas of project management, technical performance, design performance, time, and cost.

Table 3.1 Criteria Cross Reference to PWGSC Project Phases

	PWGSC Project Phases					
Criteria Category (below) applies to Project Phase (right)	Planning	Definition	Implementation	Commissioning	Operating	Evaluation
4.1 Subsystem operation in default stand-alone mode						
1. Features	✓	✓	✓			
2. Performance		✓	✓	✓		
3. Operating environment factors			✓		✓	
4. Failure and emergency operations			✓		✓	✓
5. Support and maintenance				✓	✓	✓
4.2 Subsystem operation in a building automation environment						
1. Interaction with other subsystems	✓	✓	✓			
2. BAS equipment		✓	✓			
3. BAS features			✓			
4. BAS management issues				✓		
5. System management issues				✓		
6. Communications protocol issues			✓			
7. Application Layer features			✓			
8. Lower Layer features			✓			
4.3 Subsystem business considerations						
1. Subsystem manufacturer			✓			
2. Documentation				✓	✓	
3. Cost / benefit issues	✓					✓
4. Training				✓	✓	
5. Industry education	`✓	✓	✓	✓	✓	✓

4. Criteria Organized by Category

The criteria for this guide are presented for each category followed by explanations, examples, and supplier questions where appropriate.

These criteria form a comprehensive set of guidelines for evaluating an intelligent building subsystem. Please note that analyzing a subsystem against the criteria is not simply a set of YES/NO answers. As will be explained, some criteria enumerate a set of parameters, while others require a description of capabilities. The primary value of this best-practices guide is to ensure that all relevant issues are considered when making a choice of subsystems suitable for linking into a building automation network.

The evaluation of subsystems and networks may be facilitated by defining a reference building. Candidate subsystems and networks can then be evaluated in relation to this reference or standard building. PWGSC calls this approach "Assumed Existing Prerequisites" when dealing with existing buildings[2].

At a minimum, integrated subsystems offer the building manager operational efficiencies through convenient access and remote control. However, even greater benefits accrue from new services and user interfaces not present in any individual building subsystem. The use of XML programming and database technology may be incorporated in the interconnections among subsystems to enable activities that extend beyond traditional subsystems.

For example, lighting, security, and HVAC subsystems could be coordinated during an emergency to enhance life safety. The intelligence of system coordination is logically located at a layer above the subsystems. Such coordination features are the selling points of building automation to owners, managers, operations personnel, and tenants.

4.1 Subsystem operation without network connection

For reliable building operation, each subsystem should be designed to function autonomously when not networked to other subsystems. Some services enabled by integration may not be available. However, all subsystems should be designed so essential services continue to be delivered in the default stand-alone mode.

---

[2] Please see the table on Intelligent Building Budget Effects on page 27 of the 1999 PWGSC *"Intelligent Building Concept Report"* accessible at: ftp://ftp.pwgsc.gc.ca/rpstech/Controls/Intelligent/intbldgRep.pdf.

4.1.1 Features

Considerable custom design is involved in the control of large buildings. Therefore, subsystem features are not necessarily determined from catalog specifications. Instead, a designer may develop a list of features when preparing a request for proposal (RFP) or building control specification. A preliminary design document may identify special features of the design that are required, for example, in order to meet energy targets.

a) Application Description

General description of the stand-alone applications of the subsystem (e.g., a lighting system that can be controlled centrally by the building manager, customized for each office, varied according to ambient outside light, etc.).

b) Application Flexibility

Ability to reprogram applications with low-level firmware changes (linking sensors and actuators) and software changes affecting algorithms. (e.g., program motor actuators for gradual startup to reduce stresses.)

c) Application Model

A clear explanation of the subsystem functions using generic terminology, block diagrams, and flow-control schematics.

d) Application Object-Oriented Model

A formal description of the subsystem functions using the object-orient paradigm that is widely employed in systems design.

e) Control Strategies

Central versus distributed control. (Distributed control avoids a possible weak link if a controller fails.)

4.1.2 Performance

Equipment from building control manufacturers may specify a range of values for the features listed below. The designer is responsible for determining the precise needs of the building and ensuring that the equipment can be tailored to these requirements.

a) Subsystem Capacity

Number of buildings on a campus, size of each building, number of floors, number of nodes, etc. served by the subsystem.

b) Range of Operating Parameters

Settable parameters, such as temperature, lighting lux (lumens per square meter), supply voltage, etc.

c) Response Time

Response times to user inputs, sensor changes-of-state, external commands, etc.

d) Operating Methodology

Preset algorithm versus dynamic adaptation to operating environment, response to commands from building manager and tenants, response to change of state of sensors, etc.

4.1.3 Operating Environment Factors

The designer will need to deduce the operating capabilities of the chosen equipment and possibly consult with the manufacturer to determine whether the environmental factors specified can be accommodated.

a) Accommodation of Application-Specific Parameters

Examples: internal and external temperature, wind speed, number of occupants, etc.

b) Impact on Building Environment

Generation of heat, audible noise, electrical noise, electromagnetic field egress, etc.

c) “Greening” Value of Subsystem

Estimated environmental impact of subsystem operation in terms of energy and fuel usage, ability to switch fuels, heat and pollution exhaust, quantities of consumables required (fluids, filters, etc.), recycling potential of consumables, and the eventual disposal cost of the subsystem, including any hazardous materials.

d) Operating Requirements

Requirements for cooling or heating of subsystem equipment, power conditioning, electromagnetic shielding from ingress, physical clearances and services access, susceptibility to environmental contaminants including dust, etc.

4.1.4 Failure and Emergency Operations

The designer is responsible for verifying that the chosen equipment can meet the failure and emergency operations requirements specified by the PWGSC *National Master Specifications*, Sections 138XX. These sections deal with Building Automation Systems. They were formerly called *Energy Monitoring and Control Systems* (EMCS).

a) Subsystem Failure Modes

Expected time between failures, degree of robustness (continues operating even when some functions fail). Automatic or manual reconfiguration after partial failure. Fails in a safe mode. Resiliency of the design including redundant (backup) components to survive failures.

b) Network Failure Mode

Offers diversity through multiple network paths. Can revert to stand-alone operation if the network fails (possibly with reduced functionality).

c) Emergency Control

Ability to segregate and isolate portions of network in reaction to emergencies such as fire, flood, or other building damage. Degree of manual intervention required and estimated time for network reconfiguration in an emergency.

4.1.5 Support and Maintenance

These issues are particularly relevant to owner personnel who provide support and maintenance, rather than contracting it to the suppliers or to third-party vendors. The building maintainers and operators will require appropriate skill-sets for the following tasks.

Some of these topics are addressed in the requirements of the master specification for the building.

a) Configuration

Plug-and-play versus manual configuration, impact on configuration of subsystems, reconfiguration for tenant changes, custom applications for specific buildings, transfer of configuration parameters to new or additional subsystems, etc.

b) Upgrades to Applications and Performance

Application extensions and subsystem performance enhancements through software and/or firmware changes.

c) Installation of Upgrades

Time to install upgrades, number of installers required, impact of installation on building operation, impact of installation on building tenants, etc.

d) Operation Monitoring

(1) Which subsystem parameters will be monitored?

(2) How will subsystem parameters be monitored (automatic versus manual monitoring of system performance)?

(3) What is the schedule for monitoring subsystem parameters (periodic logging of routine usage vs. exceptional occurrences)?

(4) How will the monitored data be presented and to whom (e.g., the building tenant, the building operator, the supplier)?

(5) How will operation monitoring improve subsystem performance?

(6) Can the system(s) be monitored off-site from a remote location? What equipment is needed to accomplish this?

e) Requirement for Maintaining Standby Power for Critical Operations

f) Options for Subsystem Operation in an Emergency

Provisions for offsite operation and control capabilities in emergency and security situations.

g) System Test Procedures

Test plans for confirmation of proper operation upon system installation, commissioning, and reconfiguration. Ability to test subsystem components upon installation into an area that will be inaccessible when the building is completed (such as building structure monitors).

Programs for scheduling routine tests of subsystems and components (e.g., motorized blinds might be scheduled for a full system test twice annually; computer controls and calibration might be tested monthly, while motors are subject to a monthly visual inspection and a full inspection annually).

Note that some of the tests mentioned may require skills possibly beyond the capabilities of the building operations staff. Management needs to decide how this is to be handled. The design team would need this information before completing their design in order to ensure a comprehensive design.

h) Diagnosis of Problems

Options for diagnostics: self-test capabilities, built-in user-operated test facilities, attachable test equipment, down-loadable test routines, ability to isolate failing components, ability to repair on-site, ability of building subsystem to continue operating during repair.

It is recommended that whichever diagnostics are required, they should be executed automatically with very clear action directives as needed for problem resolution. Requirements will change from an “I don’t care” response to “I need every detail” depending on the building management approach taken.

4.2 Subsystem Operation in a Building Automation Environment

This section covers a host of issues, many of which must be addressed by the system designers. Natural Resources Canada and the Institute for Research in Construction of the National Research Council Canada were among the sponsors of *High-Performance Commercial Buildings: A Technology Roadmap* at the U.S. Department of Energy (DOE). The goal of this roadmap was to “help to shape the future of commercial buildings, making them healthier, more productive, and more desirable places to learn, work, and play.”[3] The participants were particularly concerned that the present process of designing and installing building automation systems is fragmented among many companies even when they are collaborating on a joint building project. [p. 13 of the DOE report] This leaves a gap between expectations of building owners for an integrated system solution and the ability of designers to deliver. For now, some contractors are filling this gap with proprietary solutions. Therefore, requiring that specifications be based on open protocols or recognized national or international standards as a minimum is an attempt to address the future proofing of systems and avoid proprietary solutions.

All of the items in this section need to be addressed during the design phase. Several items cannot be addressed until some project parameters are provided so that elementary decisions can be made to establish a basis for other items. Good management of the design process is essential to ensure a successful outcome. The level of detail and areas of knowledge would suggest a team approach. The intent of a team should be to work towards a common objective rather than depend on a limited set of experts who may be perceived as aloof in the building design organization.

Because most networking issues are highly technical, these topics are usually assigned to designers. However, if a true integrated network is expected, representatives of owners and tenants must be involved in the design process. Issues such as network management, network reliability, and security are critical for owners and tenants alike. In some instances there can be conflicting interests that

[3] http://www.eren.doe.gov/buildings/commercial_roadmap

can and must be resolved. Owners, tenants, and designers must agree when there are choices for complying with network standards, such as structured cabling methods, communications protocols, and redundant routing options.

4.2.1 Interaction With Other Subsystems

a) BAS Functions

What services are offered through the joint operation of subsystems (e.g., a lighting system that flashes warnings to evacuate when the fire system detects a problem)?

b) Legacy Systems

Ability to integrate legacy systems not designed for networking into a network of subsystems.

A decision must be made early in the intelligent building design process whether to interface to legacy systems or to replace them. It has been demonstrated many times that replacement or upgrade is the best long-term solution.

c) Network Access

Ability to access the network and subsystem controllers for monitoring and control via a central user interface. Ability to install backup user interfaces for emergency access.

d) Remote Access From Offsite

Ability to operate networked subsystem from outside the building. Provisions for sufficient communications gateways to provide access to the BAS via the Internet or via dial-in.

e) Observable and Controllable Parameters

Which parameters (such as temperature value, light level, or other sensor values) are observable (accessible) via a communications network linking to other subsystems and user interfaces? Which parameters are controllable (can be changed remotely)?

f) List of Interoperable Systems

With which other subsystems can the subsystem being evaluated communicate? What services and benefits can be provided through subsystem interoperation?

g) Diagnosis and Repair

Ability to determine the source of a problem in a networked environment: a specific subsystem, the interaction between subsystems, or communications network components separate from the subsystems (e.g., a user interface or network server common among multiple subsystems). Ability to affect a short-term repair until the problem can be addressed.

4.2.2 BAS Equipment

a) User Interface

(1) Ability to share a common user interface to monitor and access multiple subsystems.

(2) Supplier and support for the user interface that is not likely to be part of one of the building subsystems.

(3) Options for user authentication (to validate the user identification) and authorization (to control what the user can access). Options for levels of authorization to regulate the access privileges granted to various personnel. The granularity of access control will need to be defined.

b) Interface Between Device and Network

Communications hardware and software, connectors, or any special filters.

c) Communications Media

Media options (wired, RF, IR, fiber optics, etc.). Maximum length of each medium. Alternatively, the subsystem may be specified as conforming to a national or international wiring standard. The statement of conformance or conformance class will imply the media options and maximum medium length.

d) Interconnection Among Building Networks

Support for a uniform network across all subsystems. Support for communications gateways, routers, bridges, and repeaters. If the subsystem conforms to a national or international communications standard protocol, network interconnection capabilities may be determined from the protocol specification.

e) Power Supplies for Communications

Power requirements for network devices. Power available for devices powered directly from the network medium. If Power over Ethernet (PoE) is offered, the features implemented must be specified to determine compatibility when networked with subsystems from various manufacturers.

f) Communications Tools

For network installation, troubleshooting, routine maintenance, management functions (e.g., address assignment). Accommodation of any standards, such as DHCP and BootP (Dynamic Host Configuration Protocol and Bootstrap Protocol) for address assignment of nodes by a server, should be noted.

g) Building Facilities to Accommodate Network Equipment

Wiring closets, chases, raceways, etc. Spaces for communications room, controllers, user interfaces, and servers. Conformance to building wiring standards, such as IS-11801, proposed IS-18010, CAN/CSA T529-95, or TIA-568 should be noted.

4.2.3 BAS Features

Please note that all the features described in this section may be inferred if a subsystem conforms to a national or international standard. If the subsystem does not conform to a standard, the subsystem may be open or proprietary. An open specification is made available to the public by the developer. However, there is no assurance of consistency, support, or updates. A proprietary system is owned by the supplier, who controls access to the specifications. In either case of an open or proprietary specification, interoperability among subsystems may be problematical. Please note that there is strong motivation to specify only those subsystems that are based on standards in order to promote interoperability.

a) Network Structure

Network topology: physical, logical, redundant media (in case the primary transmission medium fails).

b) Network Access

Medium access control: contention, token, time-division multiplex, interrupt-driven, polling. Standard protocols such as Ethernet, CDPD, and IEEE-802.11b define the medium access control.

c) Network Control

Message transmission control: central or distributed. Availability of redundant controllers (in case the primary controller fails).

d) Network Security

Provision in the network communications protocol to preserve data integrity by detecting and correcting bit errors, protecting against spurious data from interfering with subsystem operation, and alerting personnel to possible attempts to compromise network security.

Please note that network security addresses security in the communications network. Overall BAS security must be a responsibility that is shared by each subsystem. The objective is to detect and isolate breaches locally before they affect the entire BAS. The designers of each subsystem should specify the level of security available.

e) Network Configuration

Ability to segment the network to limit access. Ability to isolate portions of the network, permanently or temporarily (e.g., isolate life-safety systems as may be required by legal codes or by corporate security procedures, risk assessment, and operational protocols).

f) Network Capacity

Maximum number of devices that can be connected to the network. Maximum number of devices that are active (ready to send or receive). Minimum number of devices needed for network operation.

g) Network Bandwidth

Frequency bandwidth made available to each BAS device node for data transmission. Is this bandwidth available continuously? Must the bandwidth be allocated to an application statically or dynamically? Is the bandwidth shared by multiple nodes?

h) Network Performance

Maximum number of nodes attempting to transmit simultaneously. Maximum delivery time for a message. Maximum round-trip latency for an average-size message plus the corresponding response. Maximum message size. Maximum number of packets per message. Average traffic load as a function of number of active devices. Relationship between average traffic load and peak traffic load (to determine traffic growth possible). Ability to achieve a specified Quality of Service (QoS), possibly by assigning priority levels to messages. These parameters infer bandwidth and latency requirements that may be implied by a statement of conformance to a standard protocol, such as Ethernet (wired or wireless) or cellular (2, 2.5, or 3G).

i) Error Control

Types of communication errors detectable. Effective error rate after correction by use of error correcting codes ("forward error correction") or by use of retransmission ("feedback error correction"). Conformance to a standard protocol will infer the error rate. Any ability of the application to lower error rates further through error detection and message retransmission should be noted.

4.2.4 BAS Management Issues

a) Network Configuration

Which and how many subsystem components are required for operation on a network linked to other subsystems?

b) Network Expansion

Additional components required per incremental expansion of the subsystem. Software changes required for network expansion.

c) Network Reconfiguration

Methods for isolating a network section to alter, remove, disconnect, or repair a subsystem. Methods for changing to alternate media, if applicable.

d) Network Security

Procedure for conducting a system-wide risk assessment. Tools for assessing the security risk in various network configurations. Tools to protect interconnected subsystems from security breaches via the network.

e) Network Management Integration

Ability of the system to be integrated into any of the standard network management tools (HP OpenView, NetView, CA UniCentre, etc.). Support for SNMP management of the network [passive (send alarms) or active (accept modifications)].

4.2.5 System Management Issues

a) Network Enabling And Disabling

Impact on other subsystems as a subsystem is enabled or disabled. Assurances and guarantees provided by manufacturer regarding the reliability of subsystems when operating in a network that may be undergoing changes.

b) Network Configuration

Procedures for accommodating changes in tenants, office layouts, and building automation services.

c) Network Commissioning During Construction

Ability to commission those portions of the network supporting subsystems that will be inaccessible once the building is completed (such as building structure monitoring).

d) Network Commissioning For Tenants

Ability to commission sections of the building by enabling networked subsystems as tenants move in. Procedures for commissioning subsystems, connecting them to the network, and provisioning services so that existing operations are not impacted.

e) Network Provisioning and Reconfiguration

Ability to enable and disable specific network functions, possibly done by the tenants without calling building management.

f) Network Upgrades

Ability to install future generations of the communications protocol with minimal impact on system operation.

g) System Maintenance

Facilities for system performance monitoring. Monitoring for incipient network problems. Procedures for communications fault detection, reporting, and recovery. Communications network self-test initiation and reporting. External access for system maintenance.

h) System Usage Accounting

Accounting for preventive maintenance and for billing for tenant services.

i) Operator Interface Conveniences

Options that enhance the user interface to facilitate convenient and accurate system administration. For example, a graphical user interface to enable system management services. Web-based services possibly from subsystem servers, a building-wide server, or a server maintained by a facilities management company.

4.2.6 Communications Protocol Issues

If a standard communications protocol is implemented, the details in this section may be inferred by referencing the standard. For a standard with many service options, the options available in a particular subsystem must be identified. Examples of standards for building automation include BACnet (HVAC control), ANSI/EIA-709 (based on LonTalk), TIA-568 (building wiring), and IEEE-802.11b (WiFi radio frequency communications).

a) Formal Communications Protocol

Is a formal communications protocol implemented? Does the protocol conform to the OSI (Open Systems Interconnect) Reference Model for Communications or a similar standard, such as TCP/IP?

b) Protocol Obsolescence

Expected life span of the communications protocol. Is there a users' group or trade association that actively encourages the developer to improve the protocol?

c) Internet Protocols

Does the network operate as an intranet? Can the system operate without explicit IP addresses (using an automatic address generator)? Can external control be exercised via the public Internet (with appropriate security) for remote access? If so, are public IP addresses assigned to each node, or are addresses assigned locally (e.g., using DHCP – Dynamic Host Configuration Protocol) and translated in a router (e.g., using NAT – Network Address Translation)?

d) Communications Protocol Conformance

Are the protocol and implemented layers proprietary, open, or standard? Do conformance specifications exist for certifying that the protocol implemented in the subsystem conforms to the protocol specification? Are there procedures for certifying that security provisions are implemented properly for data integrity, user authentication, and levels of user authorization?

4.2.7 Application Layer Features

This section and the next section refer to communications protocol features organized into the seven layers of the OSI Reference Model for Communications, as defined by ISO 7498 (issued by the International Organization for Standardization of Geneva, Switzerland). The Application Layer is Layer 7 of the OSI Reference Model.

a) Application Language

Is a formal language defined? Is there support for commands and event reporting? Is there support for language macros, including abbreviated codes for common actions, and conditional actions at a remote device (IF-THEN-ELSE, DO-WHILE, DO-UNTIL, REPEAT n TIMES, etc.)?

b) Data Management

Does the language include support for file management and transfer, graphical data transfer, electronic mail, database access, event reporting, recording a series of trend data, data compression when sending large files? Are there provisions for linking to offsite and dispersed data storage?

c) Application Language Extensions

Support by the manufacturer for language extensions to be shared by all customers? Do customers receive support to add private extensions to the language?

d) Application Message Transfer

Protocol message confirmation options: message sent, message received, transmission error report, message understood by recipient, requested action executed by recipient, wait for response from recipient before next message is sent. Summary of message confirmation options: Sent, Received, Actioned, Resolved.

e) Addressing of Devices on the Network

Addressing options: flat or hierarchical, local (unique address on the building network) or global (unique address worldwide, like an Ethernet address), individually addressable, addressable as a group of devices, addressable via system broadcast to all devices, addressable according to function (e.g., all alarms), address can be mapped to a name via a name server. (Addresses may be assigned at Layer 7 and at lower layers, such as Layers 2 and 3.)

4.2.8 Lower Layer Features

This section refers to communications protocol features of Layers 1 to 6 of the OSI Reference Model for Communications.

a) Message Security (OSI Layer 6)

Offers data encryption, user authentication, use authorization, supports standard security methodology, such as SSL / TLS (Secure Sockets Layer / Transport Layer Security protocols).

b) Session Control (OSI Layer 5)

Allows more than one port or dialogue simultaneously between different elements at the sending device and the receiving device through a single connection between the device and communications channel. Checkpoints the flow of messages, and then continues the dialogue if there is an interruption in communications.

c) Transport Layer Functions (OSI Layer 4)

Segments long messages into maximum packet sizes acceptable to the network layer. Provides flow control across the communications network. Assembles packet segments into messages and checks for any missing packets or redundant packets. Acknowledges receipt of a group of packets at a time using a “window” protocol. Provides end-to-end acknowledgement of message delivery. Offers various grades of service to trade-off communications errors for throughput. Manages a connection for connection-oriented protocols. Can place a message on redundant communications channels for enhanced reliability. Alternatively, the network may be specified as conforming to a national or international communications standard, which may include these transport layer functions.

d) Network Layer Functions (OSI Layer 3)

Accommodates network routers. Supports flood routing of packets (to all parts of the network) and / or directory routing of packets (to restricted media on the network). Allows dynamic route changes for connectionless protocols according to network loading, or as sections of the network are added or deleted. IP protocol provides security using the IPSec (IP Security protocol).

e) Data Link Layer Functions (OSI Layer 2)

Offers acknowledgement for connectionless packet transmission service over network segments (between devices and routers)? Recognizes a retransmitted packet. Supports a connection-oriented service and streaming data. Provides priority access to the communications channels upon request.

Maintains fair access to a shared medium, possibly with contention or with token passing. Detects and corrects channel errors and invalid packets.

f) Physical Layer (OSI Layer 1)

Supports a network using shared media (e.g., Ethernet, token bus, token ring). Supports specific or multiple media?

4.3 Subsystem Business Considerations

4.3.1 Subsystem Manufacturer

This section deals with information about subsystem manufacturers that should be considered in qualifying suppliers before contracts are awarded. Therefore, some of these criteria should be included in calls for proposals that specify the project requirements.

a) Manufacturer's experience in developing networked subsystems.

Years in the networking business. Variety of networked products for sale. Reputation in the building systems business nationally and internationally.

b) Participation in trade associations developing standards and practices for building automation.

c) Size of manufacturer market share that is based on proprietary subsystems.

d) Is the manufacturer willing to interoperate with products and components from other manufacturers, including competitors?

Willingness of manufacturer to be accountable for and to support components and subsystems from multiple manufacturers.

e) Is the manufacturer willing to adapt catalog products to specific requirements of a building installation?

f) Does the manufacturer participate on national and international standards bodies?

Is the manufacturer willing to propose changes to the protocol as may be needed to adapt the subsystem to the building environment? Does the manufacturer have the skill and reputation to achieve acceptance of proposals by the standards body?

g) Code Modifications

Does the manufacturer participate in rule-making procedures, such as public hearings, legislative committees, and political lobbying, to encourage the writing of codes that do not impede networked subsystems?

h) What procedures are in place for the manufacturer to notify users of bugs, fixes, and subsystem updates (e.g., software changes)?

i) Is the manufacturer willing to provide references to subsystem buyers?

j) Does the manufacturer have experience dealing with electrical and mechanical contractors?

What is the reputation of the manufacturer among the trades in the local community? Can the manufacturer recommend specific contractors?

k) Does the manufacturer have experience in dealing with networking contractors?

What is the reputation of the manufacturer among the local networking community? Can the manufacturer recommend any specific contractors?

l) Is the manufacturer willing to help sell the benefits of the networked subsystem to tenants?

m) Is the manufacturer willing to allow building managers or third-party developers to alter the subsystem operation as needed for the building environment?

n) Can the manufacturer provide names of third-party developers for custom changes in the subsystem?

o) Are there alternate suppliers of the subsystem technology for a competitive evaluation, or if the chosen manufacturer were to fail or discontinue support?

4.3.2 Documentation

Documentation is essential for proper installation and use of intelligent building control. Procurement contracts issued to suppliers should stipulate the scope and audience for each document.

a) Availability of a non-technical summary to help make a business case for the networked subsystem.

b) Appropriate documentation for installers, operators, maintenance personnel, and tenants.

c) Is the manufacturer willing to provide additional technical details to adapt to building environment?

   Sufficient technical documentation so building management staff or third-party supplier can add custom features as needed.

4.3.3 Cost / Benefit Issues

When this project was planned, PWGSC and the Continental Automated Buildings Association (CABA) decided to develop this guide with the initial goal of evaluating various intelligent building technologies (e.g., a wired network versus a power line carrier network versus a radio frequency network). A future guide could provide the basis for a quantitative system for scoring commercial products being considered for purchase. Since technologies may represent a generic category of products, costs referenced in this section are relative. This means that we can rank-order costs of various technologies. When specific products and prices are compared, quantitative comparisons can be made. Until then, technologies may be judged qualitatively, such as "less expensive," "same cost," or "more expensive."

The items listed in this section are useful to consider while planning the intelligent building. Many of the topics should involve senior management to enlighten them about the cost/benefit tradeoffs in choosing a high tech solution for building control.

a) Purchase cost of subsystem with basic communications capabilities.

   Alternatively, consider the cost of adding communications capabilities to an existing system.

b) Cost for any installation personnel required.

   Contractor experience with chosen subsystems. Contractor training costs.

c) Cost of any tools required for installation and for maintenance.

d) Cost of a systems integrator, responsible for organizing subsystems into a cohesive system via the communications network.

e) Possible cost reduction in building construction because of less space required for raceways and spaces using shared network media or wireless-network solutions.

f) Possible churn-cost reduction from the use of plug-and-play technology and reduction in technological obsolescence by facilitating the easy and economical introduction of new technologies, or replacement of dated technologies.

g) Cost for any inspection and certification of proper and safe operation required by a governmental agency.

h) Costs to building operators for management and maintenance of the subsystem, including any training costs.

i) Cost to outsource or hire facilities operators to run and maintain networked subsystems.

j) Any licensing fees, royalties, or metered operating costs (per use charges).

k) Costs to tenants to learn and operate networked subsystems.

l) Possibility of offsetting operating costs with revenues from tenants.

   Revenues from higher rental values. Revenues per usage or rental of network subsystem by tenant from the building manager.

m) Benefit of increased employee satisfaction and comfort.

n) Benefit of improved organizational productivity, including:

   (1) Speed of building service delivery.

   (2) Reduced operations and maintenance (O&M).

   (3) Reduced energy costs.

   (4) Minimal environmental impact that enhances community and client perception of the building.

   (5) Attraction and retention of employees.

o) Cost of expanding the communications network interface (e.g., to other media).

   Cost of additional network components required in the subsystem equipment (e.g., interface module, plugs, RF equipment) and on the communications network (e.g., new jacks, wall plates, RF equipment).

p) Life cycle costs, considering all the costs listed above.

q) Warranty costs and provisions.

r) Costs of specific contractual provisions for network operation and maintenance shared among manufacturers and third-parties.

s) Impact of network subsystems on liability insurance cost.

t) Benefits of higher market rents sustainable by an intelligent building compared to a conventional building.

The combination of building automation subsystems with a BAS communications network to interconnect these subsystems may raise the ranking of the building so it is perceived as higher class than a building without a BAS. This would justify a higher rental scale.

u) Benefits of additional income from possible fees for intelligent building services offered by the building management to the tenants.

v) Benefits of lower tenant-turnover because the building services can be adapted to changes in tenants' needs.

The key to adapting building automation subsystems and a BAS network to tenants is plug and play integrated technologies. The ideal system offers cost-effective turnkey solutions for building owners. This translates into reduced costs for modifying a space as tenants' requirements change.

Turnkey solutions are defined as workplace and building environmental changes required for accommodating each new tenant (or existing tenant with revised operating needs). This allows for a "box or briefcase" move rather than a retrofit or renovation with each new tenant.

4.3.4 Training Availability:

Training should be available for:

a) Installers.

b) Building managers to run the networked subsystems.

c) Maintenance personnel.

d) Tenants.

e) There should be provision for training to be ongoing and to become a requirement of an organization's learning plan for those involved with operations, maintenance, and related aspects of the subsystems.

4.3.5 Industry Education

Provided by subsystem manufacturer or by an organization recommended by the manufacturer.

Designers and building managers should encourage manufacturers to provide opportunities for knowledge transfer to building automation practitioners. Educational institutions should incorporate building automation materials into curricula for training architects, building engineers, building operators, and building managers.

Ultimately, education about intelligent buildings must reach the decision-makers considering an investment in the intelligent building arena. There have been too many unhappy owners of installations with low technology who are hesitant to adopt the new and "unproven" high tech systems. There should be:

a) Educational materials for architects, building engineers, and consultants so they can plan networked subsystems.

b) Education for building owners and managers on ancillary services using networked subsystems that can be offered to tenants for revenue beyond the lease.

c) Education of construction companies to install building structural sensors properly during construction for a subsystem to monitor the building structure.

d) Education materials for unions to support the installation of networked subsystems.

e) Education materials for the insurance industry describing the impact of networked subsystems on insurable risks, such as fire and life safety.