



# Integrated Building Management and Security System

Building Automation & Security

[www.lonix.com](http://www.lonix.com)

# INTEGRATED BUILDING MANAGEMENT AND SECURITY SYSTEM

## INDEX

- 1 GENERAL.....3**
- 1.1 GREEN BUILDING REQUIREMENTS.....3
- 1.2 SYSTEM INTEGRATION .....3
- 1.3 USER INTERFACES .....4
  - 1.3.1 Professional User Interface.....4
  - 1.3.2 Occupant User Interface .....5
- 1.4 SYSTEM ARCHITECTURE .....5
  - 1.4.1 Service Level.....5
  - 1.4.2 Management Level.....6
  - 1.4.3 Control Level.....6
  - 1.4.4 Field Level.....7
- 2 BUILDING MANAGEMENT AND SECURITY SYSTEMS.....7**
- 2.1 BUILDING AUTOMATION .....7
  - 2.1.1 Distribution of intelligence.....7
  - 2.1.2 Usage of I/O points.....7
  - 2.1.3 General Purpose Controllers .....8
  - 2.1.4 Special Purpose Controllers.....8
- 2.2 LIGHTING CONTROLS .....8
- 2.3 CONSUMPTION METERING .....8
- 2.4 ACCESS CONTROL AND INTRUDER ALARMS.....9
  - 2.4.1 Network Controllers.....9
  - 2.4.2 Interface Panels.....9
  - 2.4.3 Readers.....10
- 2.5 VIDEO MONITORING.....10
- 2.6 FIRE ALARMS .....10
- 2.7 OTHER SYSTEMS.....10

# 1 General

## 1.1 GREEN BUILDING REQUIREMENTS

In order to fulfill the requirements of Green Building standards and initiatives, the systems shall support integration with a standard integration platform, advanced controllability, and sophisticated monitoring, measurement, verification and versatile reporting. The most important prerequisite for achieving Green Building status is the efficient functional integration of building systems. The systems shall function smoothly together according to modes of the building or the space, prevailing conditions and needs/preferences of the users. The integrated operations shall be fully automatic, triggered by one input, having appropriate impact to all systems in the building.

System integration shall enable significantly lower energy consumption, real-time control and monitoring, and dynamic graphics according to needs. System integration shall create better environmental air quality, radically improved energy performance and increased water efficiency, according to requirements of LEED and other Green Building standard and initiatives.

System integration shall also allow for efficient system maintenance and full-scale service provisioning with radically lower cost and better quality services. Easy access to building systems shall ensure that everything is in perfect condition and functions in the optimal way at all times. Should anything disturbing happen, immediate response shall be available. Integration shall facilitate undisturbed conditions in the building and sustainable development through minimized energy consumption, first-class security and significantly lower life cycle costs.

## 1.2 SYSTEM INTEGRATION

The System provider shall furnish and install a fully integrated Building Management System (BMS), incorporating distributed control techniques and standard open communication networks. The system shall be implemented as an integrated, open solution, which enables Service Center connectivity through standard Building Operating System (BOS) interface.

The integrated systems shall include controls and monitoring of the whole building (BMS and Security) and each room/apartment whenever applicable.

**Integrated Building Management and Security Systems** shall include the following subsystems:

- BMS / Building automation (cooling/heating control, ventilation control, pumps, etc.)
- Lighting control of common areas
- Consumption metering of water, electricity, cooling (heating) energy and gas
- Access control system for common areas
- Intruder alarm system for common areas
- Video monitoring system for common areas
- Fire alarm system
- Central battery system

Whenever applicable, **Guest Room Controls** shall include the following subsystems:

- Room temperature controls
- Lighting controls, dimming groups
- Lighting controls, on/off groups
- Controlled sockets, enabled/disabled
- Curtain controls (optional)
- Water consumption metering (optional)
- Electricity consumption metering (optional)
- Cooling energy consumption metering (optional)

***Please refer to a separate specification for Guest Room Controls.***

Whenever applicable, **Home Automation** shall include the following subsystems:

- Cooling/heating control of each apartment
- Ventilation control (when applicable)
- Lighting controls
- Curtain controls
- Other electrical controls
- Leakage/moisture alarms
- Access control
- Intruder alarms
- Camera surveillance (when applicable)

***Please refer to a separate specification for Home Automation for Apartments.***

All systems shall be integrated with the open Building Operating System (BOS) platform as described in the System Architecture. The BOS shall provide standard connectivity to the Service Center, which shall be capable of providing advanced maintenance and security services.

System Architecture shall be as specified in the following chapter.

Responsibilities of the system provider according to normal specifications and practices.

### **1.3 USER INTERFACES**

Systems shall be accessed through the Building Operating System (BOS). System must have two main user interface types – professional user interface and occupant user interface.

#### **1.3.1 Professional User Interface**

The system shall enable a client-based User Interface for professional usage and for central monitoring of systems (Service Center usage). The professional User Interface shall allow for at least the following:

- Alarm monitoring and alarm handling by multiple operators
  - Intruder alarms
  - Fire alarms
  - Alarms from electrical and mechanical systems
  - System maintenance alarms
  - Video monitoring
- Remote diagnostics, energy optimization and trending
  - Setpoint adjustment
  - Control optimization
  - Peak load management
  - Trending
  - Remote diagnostics of system/devices
  - Preventive maintenance
  - Consumption reports for energy management and billing
- Logs and reporting
- User profile and role management
- Access rights management

The professional User Interface shall be implemented as a client application, which includes an automatically adapting tree structure of the building, building's parts, individual spaces, different systems and parts of systems. The tree structure can be used for navigation through the system.

All systems connected to Building Operating System can be accessed through the same graphical User Interface. The client software can be installed to unlimited number of remote computers or laptops. The client software shall allow for remote Internet usage of several sites using the same client.

The professional User Interface shall show system views, floor plan views, trend view, alarm view and event log view per building and system layer. Any alarm shall be shown in red color in both graphical views and tree structure. Each alarm message shall include shortcut to relevant graphical system and floor plan view.

### 1.3.2 Occupant User Interface

Subsystems in e.g. meeting rooms, hotel rooms or residences shall be usable through a graphical browser-based occupant User Interface, using touch screen panel PC's, tablet PC's, IPTV, home computers, laptops, PDA's and mobile phones. The User Interface shall comply with requirements defined in the System Architecture.

The browser-based occupant User Interface shall be generated automatically using the structure of the building defined in the Building Information Model. The browser-based User Interface shall utilise latest web technologies, such as AJAX. The user interfaces shall provide easy access to frequently needed functionality, such as lighting controls, temperature setpoint modifications, alarms, and configuration of scenes and modes of the space. The same user interface functionality shall be usable through any device with a browser.

The browser-based occupant User Interface shall allow for at least the following actions:

- Changing the mode of the space
- Modifying the mode settings of the controlled devices
- Changing the setpoints
- Modifying the control settings (e.g. dimming level)
- Manual controls
- Door controls
- Camera views
- Alarm list browsing

## 1.4 SYSTEM ARCHITECTURE

The system shall be implemented as an integrated, open solution, which enables Service Center connectivity through standard Building Operating System (BOS) interface.

The System Architecture shall consist of four levels:

- Service Level
- Management Level
- Control Level
- Field Level

The system shall be completely modular in structure and freely expandable at any stage. Each level of the system shall operate independently of the next level up as specified in the system architecture. For example, Control Level shall operate independently without support from Management Level.

The system shall be fully consistent with the latest industry standards. To enable efficient functional system integration and to provide maximum flexibility and to respond to changes in the building use, the system offered shall support the use of LonWorks, Modbus, M-bus, Ethernet TCP/IP and Internet communication technologies.

### 1.4.1 Service Level

Service Level shall allow the systems to be connected without additional software to one or several Service Center(s), for providing centralized remote monitoring, alarm and fault detection of connected building management and security systems.

The Service Center shall be capable of accessing remotely the systems through a standard interface through the BOS platform. The standard connectivity shall enable providing advanced maintenance and security services, such as security alarm monitoring, maintenance alarm monitoring, remote diagnostics,

main user capability, remote control and optimization of all systems, energy optimization, trending and reporting services.

The Service Center shall support connectivity of multiple sites in multi-operator environment. Predefined alarms from connected sites – e.g. intruder alarms, dirty filter notifications or leakage alarms, for example – shall appear in the alarm list with a specified priority. Alarms shall be stored in the central database.

Remote diagnostics of site systems and devices shall enable proactive maintenance of technical systems, energy optimization and efficient management of the infrastructure. Centralized monitoring of all connected sites with main user capability shall enable e.g. set point changes, manual controls and camera controls by using the remote connection.

#### **1.4.2 Management Level**

Management Level shall provide a uniform view to all systems through the open Building Operating System (BOS) platform. All the systems - controls of cooling, ventilation and lighting, consumption measurements, access controls, intruder alarms, fire alarms and NVR/DVR systems - shall be integrated with the BOS using device drivers.

The BOS shall offer at least the following common services to be used by all connected systems:

- Alarms
- Historical trending
- Logs and reporting
- User profile and role management

To ensure fault-tolerant system functionality, the Management Layer shall not be responsible for any controls. The critical control functionality is taken care of by the intelligence on the Control Layer. The Management Layer shall provide standard connectivity through the BOS platform with the Service Level, with capability to support very advanced maintenance and security services. The BOS software shall also be capable of acting as a gateway between systems conveying messages, for example, from IP or Modbus devices to LON devices and vice versa.

The BOS shall collect trends from defined points, collect and forward alarms from the systems. The BOS shall enable efficient management of user rights. The BOS shall be capable of forwarding alarms to mobile phones using SMS, local alarm printers or to Service Center. It shall be possible to browse the alarm history for reporting and statistical purposes.

The BOS shall include a structured XML object model of the building, its parts and spaces, its connected systems, system parts and effect areas of each system. The XML object model shall comply with COBA XML schema.

The BOS shall include an open interface for other applications to interact with the connected systems. Communication method between BOS and Client applications shall include at least Java Messaging Service (JMS). No other primary interfaces are recommended. Web interfaces shall be used for light-weight clients, e.g. automatically generated browser-based user interfaces in residences for Panel PC's, PDA's or IPTV.

The network technology shall be based on the IT standards, such as TCP/IP, and be compatible with latest LAN/WAN technology. The operating system of the BOS server shall be Linux. The BOS shall be capable of supporting current and future building management protocols through implementation of network interface drivers. The BOS shall be capable of current and future systems and devices through implementation of device drivers.

#### **1.4.3 Control Level**

The Control Level shall consist of a distributed network of smart controllers, which communicate to each other using a commonly known field bus as specified herein. Connectivity towards Management Level shall utilize standard TCP/IP protocol.

The controllers shall include all the intelligence of the system. All communication shall be event based, real-time peer-to-peer communication. All controllers shall be capable of operating autonomously independently of Management Layer. For example, all systems react to alarms on the Control Layer without interference from upper layers.

Each automation controller shall be capable of handling several different systems in parallel through flexible distribution of I/O points. Automation controllers shall function as autonomous units and form an intelligent system by communicating in real time over the free topology (FTT-10) Local Operating Network (LON) using standard network variables (SNVT). Security controllers shall utilize RS-485 connection between the network controller and the interface panels.

#### **1.4.4 Field Level**

The Field Level shall consist of industry standard sensors and actuators, industry standard (wiegand) card readers and IP cameras. Field level is specified per system in next chapter.

## **2 Building Management and Security Systems**

Building Management and Security Systems, including building automation, lighting controls, consumption measurements, access control, intruder alarms, video monitoring, fire alarms, central battery system and home automation, shall be integrated using the Building Operating System (BOS) as the integration platform, which shall provide functionality as described in the System Architecture.

### **2.1 BUILDING AUTOMATION**

Building automation includes control and monitoring of cooling/heating system, ventilation system, pumps, tanks, lifts etc. All mechanical and electrical systems shall be monitored and controlled by smart control nodes connected to Local Operating Network (LON).

Building automation systems shall be integrated with lighting controls, security systems and fire alarm system as specified in the System Architecture. Building automation shall be connected to the central user interface through the Building Operating System (BOS).

#### **2.1.1 Distribution of intelligence**

The intelligence of the automation systems shall be distributed into Smart Control Nodes, which are connected to control network (LON). Smart Control Nodes must be commonly used during past 10 years in large scale commercial facilities, such as offices, business centers or hotels. It shall be possible to integrate the systems on Control Level without interference of Management Level, according to System Architecture.

Communication between Smart Control Nodes shall be peer-to-peer communication via a Free Topology (FTT-10) Local Operating Network (LON) with the Standard Network Variables Types (SNVT). All communication shall be event based. Nodes shall be intelligent modules, capable of operating autonomously independently of Management Level. For example, all systems must be able to react to alarms on the Control Level without interference from upper levels.

#### **2.1.2 Usage of I/O points**

Each node shall have about 10 I/O points to achieve maximum reliability and flexibility. Each node shall be capable of handling several different systems in parallel through flexible distribution of I/O points. The I/O points of the Control nodes shall be as follows:

- DI: Digital indication, from potential free contact
- DO: Digital control, open collector
- AI: Analog input, standard measurements 0-10 VDC, PT1000 or Ni1000-LG.
- AO: Analog control, 0-10 VDC or 20 mA

The Control nodes shall include PID controllers and ON/OFF (thermostat) functions for implementing the control loops used in engineering system process controls. Logical functions shall be implemented using configurable software objects in the Control nodes.

Field devices are connected to Control nodes using the common industry standards:

- PT-1000 for temperature
- 0-10 V for other sensors and actuators
- Potential free contacts for ON/OFF indications and push buttons
- 24 V relays for ON/OFF controls
- Impulses for consumption measurements

To guarantee openness, flexibility and cost-efficient maintenance of the integrated systems, the field devices shall not include independent control logic.

Control nodes are placed to the nearest electric cabin, side of air-handling units or in separate cabins when adequate. All systems shall use the same control network cabling, which uses free topology to maximize flexibility for future modifications and to minimize the need for cables. Electrical design should utilise star topology for controlled loads to maximize flexibility for changes.

### **2.1.3 General Purpose Controllers**

General Purpose Controllers shall be freely configurable to achieve maximum reliability and flexibility and to meet the sequence of operation and future modifications.

Configuration shall be done with a graphical system configuration tool, which shall be compatible with the Building Operating System (BOS). The tool shall produce BOS compatible XML document about all integrated systems, which can be used as such to run the BOS.

### **2.1.4 Special Purpose Controllers**

Special Purpose Controllers shall be used as autonomous controllers in rooms, zones and fan coil units. Each Special Purpose Controller alone shall be capable of controlling temperature, air quality (CO<sub>2</sub>) and lighting in the room or zone. Special Purpose Controllers shall communicate on LON bus.

It shall be possible for the FCU controller to automatically change the FCU motor speed based on temperature deviation. The FCU controller shall regulate the cooling valve to meet the desired temperature conditions. FCU controllers shall communicate on LON bus and shall be integrated with BMS system to enable energy optimization and reporting.

## **2.2 LIGHTING CONTROLS**

Lighting of common areas of the building shall be controlled by smart control nodes, which shall be connected to LON field bus in the same way as described in the chapter Building Automation. Lighting controls shall be implemented as part of the integrated Building Automation system.

Lighting groups in the common areas are on/off controlled (and/or dimmed) as follows:

- Using local push buttons (on/off, on/off/up/down, lighting scenes)
- On occupancy
- Based on illumination level (dusk)
- Time schedules

Lighting controls are integrated with building automation and security systems and connected to the central user interface through BOS.

## **2.3 CONSUMPTION METERING**

Consumptions of water, electricity, gas and cooling energy shall be measured in each area / apartment. Water and electricity meters shall be equipped with impulse outputs. Impulse outputs are connected to Smart Control Nodes, which are connected to Local Operating Network (LON). BTU meters shall be

connected direct to control network. All consumptions shall be trended into BOS's database for generating regular consumption reports.

Different type of reports have to be generated for professional users and occupants. Occupant reports must be easy to understand and they must increase environmental awareness according to LEED and other green building initiatives.

## **2.4 ACCESS CONTROL AND INTRUDER ALARMS**

Access control system shall be integrated with building automation, lighting controls and other security systems using the Building Operating System (BOS) as the integration platform.

Access control shall be implemented with proximity readers, control nodes, electronic keys and electronic locks. Users can be classified so that they have access only to the spaces they are allowed to enter according to programmed time schedules. The access control system is connected to BOS for full control and reporting, and integrated into the central user interface.

Intruder alarm system shall include perimeter protection and indoor surveillance. Monitored doors and windows shall be equipped with magnetic contacts. Movement detectors used in indoor surveillance shall be sensitive enough for presence detection of a single person, so that they can also be used for lighting controls and air-conditioning controls.

Intruder alarms are seamlessly integrated on software level to access control, CCTV/DVR/NVR, lighting control and building automation. Granted access disarms the alarm zones automatically. In case of burglary the system gives an alarm, which is relayed through BOS to Service Center and/or to specified mobile phones.

### **2.4.1 Network Controllers**

Network Controllers shall connect access control and intruder alarm system with Management Level using an open interface utilizing TCP/IP protocol.

Network Controllers shall connect with up to 32 Interface Panels using RS-485 bus. The door/reader Interface Panels shall operate also autonomously with no connection to a Network Controller. Network Controllers shall buffer the offline transactions from Interface Panels when connection to the BOS server is down and send the transactions when the connection is restored.

The Network Controller shall enable access control database with 44.000 card holders. The memory of the Network Controller shall be easily expandable to accommodate up to 250.000 card holders. Each card holder can belong to max 8 access groups. The total number of available access groups in the system shall be 65.535. Each access group shall have a schedule based access to defined door groups.

The Network Controllers shall be able to communicate with each other to create large-scale area control solutions with independent control logics. Area control solutions shall be expandable using TCP/IP network to include door/reader Interface Panels located under several Network Controllers.

Network Controller shall have local inputs for tamper and battery failure for indications and alarms.

### **2.4.2 Interface Panels**

The selection of Interface Panels shall include at least Door/Reader Interface Panel, Input Monitor Interface Panel and Output Control Interface Panel. The Interface Panels shall connect with Network Controllers using RS-485 bus.

Door/Reader Interface Panels shall have two reader interfaces utilizing standard Wiegand protocol. Depending on application, the panel can be configured to control two sets of separate doors with a reader and an exit button, or one door with two-side readers (entry/exit).

In addition to the two reader interfaces, the Door/Reader Interface Panels shall have the following inputs and outputs: door monitor input, exit button input, strike relay output, auxiliary relay output.

Door/Reader Interface Panels shall be capable of indicating door forced and door held alarms also locally by using the internal beeper of the reader.

Interface Panels shall have local inputs for tamper and battery failure for indications and alarms.

The Input Monitoring Interface Panel shall be used to interface e.g. magnetic contacts and motion detectors to indicate alarm events. The Input Monitoring Interface Panel shall include 16 supervised alarm inputs and 2 relay outputs.

Output Control Interface Panel shall be used mainly to control lifts. The Output Control Interface Panel shall have 12 relay outputs and 2 supervised alarm inputs.

It shall be possible to create complex I/O linking and rules between Network Controllers and Interface Panels.

### **2.4.3 Readers**

The system shall support a variety of readers using standard Wiegand protocol, including plain readers, keypad readers, long-range readers and biometric readers. Readers should be based on 125 kHz proximity technology or 13.56 MHz contactless smart card technology, e.g. Mifare or iCLASS.

The system shall support a variety of credentials, including but not limited to e.g. traditional proximity cards and tags.

## **2.5 VIDEO MONITORING**

Video monitoring shall be implemented with Digital Video Recording (DVR) or a fully IP based Network Video Recording (NVR) system. The video monitoring system shall be integrated to BOS server so that the system shall start recording video stream upon triggering from intruder alarm system, access control, CCTV or any other system integrated to BMS.

The video monitoring system shall support both analog and IP cameras. The system shall preferably run on Linux operating system. Usage can be done both via video monitoring system's own User Interface Client and the integrated user interface of the BOS.

In addition to the software based user interface, it shall be possible to additionally expand the operator workstation with hardware based keypad and joystick interfaced with the system.

## **2.6 FIRE ALARMS**

Fire alarm system shall be integrated with BMS for monitoring. Fire alarm system can be integrated either by 1.) using potential free contacts of Fire Alarm Panels connected to control modules or as 2.) using system driver which gives alarm information on individual sensor level to BOS. In both cases alarms are relayed to BOS and shown in the integrated graphical user interfaces. Ventilation is shut down in the area concerned.

## **2.7 OTHER SYSTEMS**

Other systems shall enable integration to BOS, whenever applicable.

-----END OF SECTION-----