

28 00 00 Electronic, Safety & Security

Fire Alarm Systems – General

- .1 Queen's University has a sole source partnership agreement with Siemens Building Technologies Cerberus Division for the supply of all fire alarm equipment. Designers should contact Siemens in order to obtain assistance in producing a design optimized for Siemens equipment.
- .2 Fire alarm systems will conform to all applicable codes and standards.
- .3 Addressable fire alarm systems will be provided in all buildings exceeding three stories in height above ground or exceeding 5000 m² in gross area. Conventional systems may be used in smaller buildings.
- .4 Addressable fire alarm systems shall be installed as two-stage systems with the general alarm delay set to zero. Full two-stage operation will be implemented at the university's discretion. Conventional systems shall be single stage, non-coded.
- .5 Control panels shall be easily accessible with the annunciator portion visible to the fire department personnel at the main entrance and located to the satisfaction of all fire departments concerned.
- .6 Fire alarm systems are monitored centrally by both Fire Monitoring of Canada (FMC) and Queen's Emergency Report Centre (ERC). Separate, normally-closed contacts shall be provided in the control panel to provide trouble, supervisory and alarm signals to FMC, and trouble, supervisory, and alarm signals to the ERC. Conduit is required from the interface box to an ITS Comms Room - coordinate with PPS. FMC requires both Ethernet and telephone connections. ERC requires a hardwired connection to the nearest Queen's security panel. System commissioning requires that both central monitoring stations be operational before acceptance testing commences.
- .7 System verification is to be provided by Siemens Building Technologies, Cerberus Division.

Fire Alarm Systems – Products / Materials

- .1 Long life lead acid batteries shall be used for standby power.
- .2 Metering shall be provided to monitor the battery voltage and charging current.
- .3 Wiring shall be in conduit, and be shielded low-energy red jacketed cable approved for fire alarm use. Solid copper wire size to be that recommended by the manufacturer.
- .4 Ground fault indication shall be provided.
- .5 Visible trouble signal and audible signal with silencing switch shall be provided.
- .6 Each end of line device shall be located in a separate box with a distinctive cover adjacent to the last station of the line or in the riser terminal box on a terminal strip labelled with the zone number. The method used must be consistent through the building.
- .7 The preferred audible device is a horn. Emergency voice systems should be used only where there is a demonstrated need or a code requirement.
- .8 Strobes shall also be provided throughout the building above and beyond OBC requirement.

Fire Alarm Systems – Installation

- .1 The fire alarm graphic shall be developed in conjunction with PPS. The graphic shall be submitted to PPS in the current revision of AutoCAD or another mutually agreed format. Use of active graphic displays is strongly discouraged.
- .2

- .3 The branch feeder breaker or disconnect shall be located as close as possible to the main power supply of the building and will be painted red and labelled "FIRE ALARM POWER". When available, source shall be Emergency Power
- .4 All addressable devices shall have their addresses clearly identified on them.
- .5 All wiring joints in the fire alarm system shall be identified on as-built drawings.

Fire Alarm Systems – Documentation

- .1 Documentation for the fire alarm system must include: an equipment list stating the type, catalogue number and quantity of each device installed/purchased including spares; all the manufacturers recommended operation and maintenance manuals; the complete verification report; accurate as-built floor plans showing the location and address of all devices and a riser diagram illustrating the network layout of the fire alarm system.

Intrusion Alarm Systems

- .1 Intrusion alarm systems will conform to all applicable codes and regulatory approvals
- .2 Intrusion alarm systems will be monitored internally by the Emergency Report Centre (ERC). Control panels shall be compatible with the ERC front end monitoring system (SurGuard MLR2).
- .3 Control panels shall be secured within a protected area (usually in the armed area). They shall be easily accessible for service work.

Materials

- .1 Monitoring
 - Mandatory features for digital / DVAC's controls communicating with the ERC front end:
 - Pulse / DTMF Dialing
 - Contact I.D. format
 - S/A Format
 - 1400 / 2300 HZ handshake / Kissoff
 - Universal Format
- .2 Detection Devices
 - All detection devices shall:
 - Be Motion Detectors
 - Have Form "A", "B" or "C" relay output for Grade C & B
 - Have form "C" with tamper, ULC certified for Grade A & ULC
 - Be Passive Infrared Type
 - Have dual technology (passive & microwave) in unstable environments
 - Have sensitivity adjustment
 - Be equipped with an independent tamper switch
 - Include Temperature Compensation circuit
 - Be Microprocessor Based
 - Provide Minimum 900 Sq. Ft. coverage
- .3 Magnetic Door Contacts Shall:
 - Be recessed type
 - Accommodate 3/4 , 7/8 or 1 inch wide gap for steel doors
 - Accommodate 1/4, 3/8 or 3/4 for wood doors and frames
 - Be installed on window surfaces to prevent accessibility (concealed)
 - Be suspended at the end of the line

.4 Panel Features

Intrusion alarm panels shall have the following features for each Grade noted:

| FEATURES | GRADE | | |
|---|-------|---|---|
| | A | B | C |
| AC Power Supervision | X | X | X |
| Low Battery Supervision | | | X |
| Loss of Communication Line Supervision | X | X | X |
| Static / Lightning Protection | X | X | |
| LCD Keypad | X | | |
| LED or LCD Keypad | | X | |
| LED Keypad | | | X |
| Keypad Tamper | X | | |
| Detector Supervision | X | X | |
| Keypad Supervision | X | | |
| Expansion module supervision | X | | |
| Multiplex expansion bus | X | | |
| Open / Short / Ground input supervision | X | X | |
| EOL supervised zones | X | X | |
| EOL supervised zones (end of line resistors) | | | X |
| Static Lighting Protection | | | X |
| Swinger shutdown | X | X | X |
| History Buffer | X | X | |
| Individual Zone Programming and Characteristics | X | | X |
| Minimum of six hardware zones | | | X |
| Minimum of eight hardware zones | | X | |
| Minimum of ninety-six hardware zones | X | | |
| Minimum of two partitions | | X | |
| Minimum of eight partitions | X | | |
| Minimum of six users | | | X |
| Minimum of sixteen users | | X | |
| Minimum of ninety-six users | X | | |
| Minimum of sixty-four relays | X | | |
| Uploadable / Downloadable Control Capabilities | X | | |
| Printer output | X | X | |
| Pulse / DTMF dialing | X | X | X |
| Test transmissions, Daily | X | X | X |
| Open / Closing by user | X | X | X |
| Alarm / Restore by Zone | X | X | X |
| Contact I.D. Format | X | X | X |
| SIA Format | X | X | X |
| Radionics Format | X | X | |
| 1400 / 2300 HZ Handshake / Kissoff | X | X | X |
| Universal Format | X | X | X |

.5 Batteries

All batteries shall be maintenance free, sealed, leak proof, gelled electrolyte, rechargeable:

Grade C:4 amp-hour (minimum)
Grade B:7 amp-hour (minimum)
ULC:7 amp-hour (minimum)
Grade A:14 amp-hour (minimum)

.6 Control Transformers

Transformers shall be CSA approved and meet OEM specifications.

.7 Preferred manufacturers

Panels (CPU): Napco, SurGuard, and DSC

Contacts: Sentrol or ADI

Wiring

- .1 All connecting wire used in the installation shall meet the original equipment manufacturers specification.
- .2 All wire used in the installation shall meet all respective fire and safety codes.
- .3 Each device wired to the control panel shall use an independent wire, which is free of joins and splices.
- .4 Wiring shall normally be in conduit to Queen's University's Standards.

Documentation

- .1 Intrusion alarm system shall include:
 - An equipment list stating the type, catalogue number and quantity of each device installed / purchased including spares.
 - All the manufacturers recommended operation, programmers and maintenance manuals.
 - Accurate as-built floor plans showing the location of all devices and a complete wiring diagram illustrating the interconnection of all field devices, power source and monitoring devices.

Maintenance

- .1 It is the end user's responsibility to ensure that their Intrusion Alarm Systems are maintained in good working order.
- .2 Routine maintenance is imperative on any intrusion detection system to ensure that it is operating as it was originally intended. It is recommended that all alarm systems should be serviced on a regular basis. The most economical way to ensure these tests are completed is for the user to enter into a service contract with a reputable alarm system contractor. The service contract should include:
 - Clean and test all motion and contact detectors
 - Test back up battery
 - Check that all peripheral devices are in good working order
 - Ensure all zones that are programmed to report an alarm signal are functional
 - Check that all keypads are in good working order
 - Two programming changes per year (code changes)
 - When the service is complete the end user should request a document stating the serviceability of the system.

- .3 In the event a user requires or requests repair work (non-warranty coverage) or upgrades to their existing system, a request in writing for system repair shall be completed by the user and sent to Physical Plant Services (PPS). The individual requesting the service will be financially responsible for any cost incurred due to the repair request. The aforementioned financial responsibility will be void if the request form indicates "Quote only".

Training

- .1 The contractor shall include in their quote adequate training for the end user.

Warranty

- .1 Installed parts: 3 year (minimum)
.2 Door Contacts: Lifetime Warranty
.3 Labour: 1 year (minimum)
.4 Access Control Systems conform to all applicable codes and regulatory approvals.

Materials

- .1 Access Control Panels
Access control panels (more commonly known as Intelligent Access Control Processors) should have the following features:
- Minimum of 500 transactions in buffer
 - Minimum of 6 site codes
 - Minimum of 2 readers
 - Minimum of 2 keypads
 - Capable of 7 reader technologies
 - Minimum of 16 NO/NC supervised zones on motherboard
 - Alarm points up to 2000 feet away
 - Minimum of 4 relays on motherboard
 - Metal cabinet with tamper
 - Buffered or non-buffered mode
 - 300 to 9600 baud communication speed
 - Internal memory retention
 - Up to 64 panels per communication loop
 - Fully distributed database
 - Computer enhanced not computer dependent
 - Dial up modem programming capabilities
 - Free egress, door ajar, door open to long outputs
 - Minimum of 3800 card user's
 - RS-485/RS-232/current loop, communication protocol
 - Hyper Terminal Diagnostics
 - .21 Minimum of 32 Times Zones

Locking Devices

- .1 Locking devices used in conjunction with any Access Control System shall be limited to either magnetic locks or electric strikes.
.2 New Magnetic locking device installations are not normally permissible because of Ontario Building Code restrictions. Magnetic locking devices shall only be used with the explicit approval of the Chief Building Official and Physical Plant Services.

- .3 Magnetic locking devices will supply a minimum holding force of 1,200 pounds and when in the released state shall supply no residual magnetism. All magnetic locks shall be equipped with built in surge protection and shall be held in place with tamper resistant mounting hardware.
- .4 Electric strikes shall be of the fail-safe (or fail unlock) type. Each strike shall be equipped with a surge suppression kit to ensure collapsing magnetic fields do not harm or interfere with the proper operation of the control panel. A minimum holding force of 1,400 pounds is required when the strike is in the locked position. The strike when installed shall operate in the same manner as the original mortise lock set.

Exit Devices

- .1 The "trail" requirements of the system determine what exit devices are required:
- .2 If an audit trail (entry/exit history) is required the exit device shall be the same as the installed entry device.
 - If the audit trail is required for entry only, several types of exit devices may be employed:
 - Pushbutton: Request exit button, located next to the latched side of the door. The button shall be a laminated type, clearly marked "EXIT".
 - Key Switch: When a key switch is used to override a magnetic lock or electric strike a signal shall be sent to the control panel to indicate that the locking device has been manually bypassed. The keyway on the switch should be a high security keyway and weather resistant.
 - Pull Station: When an auxiliary pull station is required to override the locking device it will be painted blue to distinguish it from fire alarm devices. A sign must be placed above the pull station which reads "IN CASE OF EMERGENCY PULL TO RELEASE DOOR". All signage must meet university stated signage policy. The pull station shall be fitted with a set of double contacts. One set will signal the control panel that the station has been activated and the other will interrupt the power to the locking device.

Signage

- .1 When magnetic locks or other devices are used to impede egress, proper signage shall be posted. The sign shall clearly indicate the proper procedure for exiting through the locked door. All signage must meet university stated signage policy.
- .2 When magnetic locking devices are used on doors released by fire alarm systems a sign which reads "EMERGENCY EXIT UNLOCKS BY FIRE ALARM" must be permanently mounted on the door. All signage must meet university stated signage policy.

Interior Room Requirements

- .1 When an access control system is installed on an interior room a telephone must be made available in that room to ensure users have direct access to the Emergency Report Centre (ERC). The phone may be a direct dial (to the ERC) lift set or regular office type with a posted number. Queen's telephone service is provided under the direction of the Information Technology Services Department (ITS). All installations must be coordinated and approved by ITS. The University's policy regarding the installation of telephones is to provide for the most flexible system possible. This is accomplished by providing conduit roughed in any and all office areas. The actual service installed in this conduit system will be determined later in the planning process.

Card Readers

- .1 Readers shall be proximity type, 4 inch read, and mullion style.

Batteries

- .1 Batteries shall be maintenance free, sealed, leak proof, gelled electrolyte, rechargeable.
- .2 14 amp-hour (minimum)

Wiring

- .1 All connecting wire used in the installation shall meet the original equipment manufacturers specification.
- .2 All wire used in the installation shall meet all respective fire and safety codes.
- .3 Each device wired to the control panel shall use an independent wire, which is free of joins and splices.
- .4 Harshness of the environment will determine if conduit is required.

Transformers

- .1 Shall be CSA approved and meet OEM specifications.

Documentation

- .1 Shall include:
- .2 Equipment list stating the type, catalogue number and quantity of each device installed/purchased including spares.
- .3 Manufacturer's operation, programming, and maintenance manuals.
- .4 Accurate as-built floor plans showing the location of all devices and a complete wiring diagram illustrating the interconnection of all field devices, power source and monitoring devices.

Maintenance

- .1 It is the end user's responsibility to ensure that their Access Control Systems are maintained in good working order.
- .2 Routine maintenance is imperative on any Access Control System to ensure that it is operating as it was originally intended. It is recommended that all systems should be serviced on a regular basis. The most economical way to ensure these tests are completed is for the user to enter into a service contract with a reputable alarm system contractor.
- .3 The service contract should include:
 - Clean and test all entry and exit devices.
 - Test back up battery.
 - Check that all peripheral devices are in good working order.
 - Ensure all zones that are programmed to report a signal and are functional.
 - Check that all keypads are in good working order.
 - Two programming changes per year (code changes).
 - When the service is complete the end user should request a document stating the serviceability of the system.
- .4 In the event a user requires or requests work (non-warranty coverage) or upgrades to their existing system, a request in writing for system repair shall be completed by the user and sent to Physical Plant Services (PPS). The individual requesting the service will be financially responsible for any cost incurred due to the repair request. The aforementioned financial responsibility will be void if the request form indicates "Quote

only".

Training

- .1 The contractor shall include in their quote adequate training for the end user.

Warranties

- .1 Installed parts: 3 years (minimum)
- .2 Card readers: 5 years (minimum)
- .3 Labour: 1 year (minimum)

Clocks

- .1 Independent clocks (not master/slave systems) shall be used. The operation and maintenance of clocks shall be the responsibility of the user.



Queen's
UNIVERSITY