9.4.2 Developing an IDS

9.4.2.1 Requirements

The primary requirements when developing an IDS are as follows:

- An IDS shall be used to identify a security breach of unauthorized entry for the exterior building perimeter, interior building security boundaries, and exterior site perimeter.
- Use of detection sensors, devices that monitor and detect forced and unauthorized entry into a protected area.
- Use of processor controllers, systems that receive and process outputs from connected sensors and use predefined parameters to generate alerts based on the information received from each sensor.
- Use of a notification console, a device that monitors events and system alerts that operators can use to make informed decisions as to the operational status of the entire IDS.
- Use of power source, low-voltage transformers and backup batteries.

9.4.2.2 Recommendations

The primary recommendations when developing an IDS are as follows:

- IDS panels should be monitored from a central monitoring station to provide enhanced security.
- IDS should be tied into a local alerting system and into a police station or a private security station.
- IDS should be capable of alerting homeowners and business owners via pager, telephone, or Internet.

9.4.3 System Connectivity

9.4.3.1 Requirements

Any telecommunications or ICT cabling required for an IDS shall meet the requirements of this standards and the AHJ, as applicable.

The use of wireless devices in an IDS shall meet AHJ requirements.

9.4.3.2 Recommendations

When selecting a wireless device with batteries, following properties should be preferred

- Devices that show battery levels
- Devices that generate warnings when battery levels are low

9.4.4 Sensors

9.4.4.1 Introduction

IDS detection sensors operate on the principle of sensing or detecting changes that occur to the operational conditions specified at the area under protection.

9.4.4.2 Recommendations

If detection sensors are used, they should be used to monitor:

- Perimeters – doors, windows, fences, and walls
- Area of space – office spaces, hallways, cabinets, and lobbies
- Points of interest – safes, paintings, and expensive artifacts

Detection sensors should be deployed considering the technology utilized and the basis of activation (see Table 9-4).

9.4.4.3 Motion Sensors

An IDS should have motion sensors used to detect motion in a room or area.

Motion sensors should be correctly placed in order to allow proper coverage of a given area. Power as recommended by the manufacturer, should be provided to motion sensors.

NOTE: For information about sensors, types and coverage capacity, refer to the manufacturer's literature.

Motion sensors should not be pointed toward heat registers or items hanging from the ceiling to reduce false alarm events.

Table 9-4 Detection Sensor Technology and Application

Technology	*Basis of Activation*	*Application*
Audio	Sound	Interior areas, vaults, and other low sound level areas
Capacitance	Proximity	Exterior areas
Electromechanical	Breaking of electrical circuit	Interior and exterior areas
Glass break	Vibration/audio	Windows
Infrared	Movement	Interior and any areas where the temperature remains fairly constant
Interfaces	Dry contact	Fire detection and alarm, HVAC, refrigeration, surveillance
Microwave	Movement	Interior and exterior areas
Photoelectric	Interrupting light beams	Interior and exterior areas with line of sight from transmitter to receiver
Pressure	Weight	Interior and exterior areas
Sonic/ultrasonic	Movement	Interior areas

9.4.4.4 Window Sensors

9.4.4.4.1 Recommendations

When appropriate, an IDS should have window sensors in order to detect breaches. The specification of window sensors is outside the scope of this standard. A wide variety of styles of window sensors should be considered as part of an IDS. Combinations of multiple sensor styles are allowed. The following styles may be considered:

- Glass break sensors
- Shock sensors
- Magnetic switches
- Security screens

9.4.4.4.2 Additional Information

A 7.5 m to 9 m (25 ft to 30 ft) radius is common for glass break sensors. Some units only detect a radius no larger than 3 m (10 ft). For accurate information about sensor operation, refer to its manufacturer's literature.

Many shock sensors are standalone active devices that have an internal processor, require power, and have contacts for signaling alarms to the control panel. Other types of shock sensors send signals to a remote processor that powers the units, interprets the signals, and passes alarms on the control panel. Refer to the manufacturer's installation instructions for further information.

9.4.4.5 Door Status Sensors

An IDS should have door status sensors used to report status on each door or latch that can offer access to a controlled area, space or property.

9.4.4.6 Perimeter Sensors

An IDS should have perimeter sensors to provide intrusion detection notification.

Outdoor motion sensors generally are mounted on the exterior of a building and have a detection range of 9 m to 15 m (30 ft to 50 ft). When connected to the building's structured cabling, cable length limits should be observed.

Photoelectric beam sensors (transmitter and receiver) may need external power and should be wired for power when used. When connected to the building's structured cabling, cable length limits should be observed.

Pan, tilt, and zoom (PTZ) cameras can be deployed as perimeter sensors, due to their ability to locate a target.

9.4.5 Notification Devices

9.4.5.1 Requirements

Notification devices, such as keypads, audible devices (e.g., speakers, sirens, bells), strobe lights, video monitors, relays, recording devices and power line carriers, shall be used as part of an IDS. A combination of more than one type of notification device in a given IDS is possible and permitted by this standard.

When active devices are used, power shall be provided to these devices.

9.4.5.2 Recommendations

An IDS should be monitored by an off-site facility or monitoring station to indicate alarms, or off-normal conditions so that necessary actions or responses will not be delayed. Communications to a remote site can be accomplished in many different ways.

9.4.6 Control Panel

9.4.6.1 Requirements

The control panel or controller shall be designed to analyze the various outputs from the detection sensors as well as monitor their own internal circuitry for abnormal operation of its internal devices.

Power limitations of the control panel shall be observed in order to not overload a power output or the entire power panel. The total current draw for an output shall never exceed its rated value. If either the maximum value of an output or the total panel will be exceeded, an external power supply shall be added to the system to power the additional load.

Battery sizing shall be determined by applying Equation 9-1.

$$B = (T_s \times I_s) + (T_a \times I_a) \qquad (9\text{-}1)$$

Where:

B = Battery size (ampere-hour, Ah)

T_s = Required battery run time (hour, h) during Standby

I_s = Current draw (ampere, A) during Standby

T_a = Required battery run time (hour, h) during Alarm

I_a = Current draw (ampere, A) during Alarm

The battery backup shall be correctly sized for the necessary runtime of the panel without external power. The control panel battery shall not be oversized, except when required to meet standby runtime criteria defined by codes or the AHJ.

9.4.6.2 Recommendations

When a standard battery backup size for a given total value determined (by applying Equation 9-1) is not available, battery size should be sized up (this information is usually available in the manufacturer's literature). When a required battery runtime is necessary while the panel is in alarm condition, additional calculations should be performed to verify battery size is sufficient.

Control panels should be installed in a secure area with limited or restricted access. Access to the control panels is usually only needed by installation or service personnel.

9.4.7 Keypads and Annunciators

9.4.7.1 Requirements

An IDS shall have keypads and annunciators in order to provide a means for the users and installers to input commands to the control panel as well as provide information to users, installers and managers.

9.4.8 Optional Integrated Equipment

9.4.8.1 Introduction

An IDS usually operates as a stand-alone system. However, most IDSs allow other systems to be incorporated into the control panel with integral expansion modules that are already built into the system, external expansion capability, or by replacement of the panel itself.

The following systems can be incorporated into an IDS:

- Access control (See Section 9.6)
- Fire detection and alarms, if approved by the AHJ (See Section 9.7)

9.4.8.2 Requirements

Addition of any fire alarm device to an IDS can change the classification of the system from IDS to fire alarm. Such additions or integrations shall comply with all applicable fire alarm codes, standards, and AHJ requirements.

9.5 Video Surveillance

9.5.1 Overview

Video surveillance is the extension of human vision to areas requiring surveillance. Discussions regarding surveillance system deployment, integration, monitoring, and convergence often lead to the determination of functional needs.

Video surveillance systems may include functions, such as:

- Remote video
- Facial Recognition
- Artificial Intelligence
- Advanced integrated surveillance systems
- Distributed integrated active remote multi-camera networks
- Database-integrated object recognition systems
- Binary change detection
- Active head tracking and face cataloging
- Video content analysis systems

Surveillance systems typically fall into one of the following categories: hardware control, digital video matrix, digital video management, and software as a service.

When planning video surveillance systems, like all ESS systems, device performance in unanticipated conditions and potential interdependencies with other external devices, systems, and infrastructure should be included, as elements to be addressed for achieving the highest level of fault tolerance possible.

9.5.2 VSS Elements

Video surveillance systems are composed of the following elements:

- DMC source
  - Video cameras
  - Encoders
- VSS physical infrastructure
  - Ethernet cable
  - Power over Ethernet
  - Power sourcing equipment
  - Wireless infrastructure
  - Media converters
- VSS logical infrastructure
  - Ethernet switches
  - Routers
  - Firewalls
- VSS control and analysis devices and applications
  - Video analytics algorithms and processing
  - Intelligent video search applications
  - Video synopsis applications
  - Positionable video camera control
  - Camera selection control
  - Video source to display control
- VSS video management devices and applications
  - Digital video recorder
  - Network video recorder
  - Video recording server
  - Video management system application
  - Physical security information management application
  - Digital data management,
  - Cloud-based video software-as-a-service

List continues on the next page

- DMC storage
  - Local storage within digital video recorders and network video recorders
  - Network attached storage
  - Cloud-based video infrastructure-as-a-service
- DMC display
  - Flat panel video monitors and walls
  - Mobile devices
  - Tablets and laptop computers

9.5.3 Design Recommendations

9.5.3.1 General

Designs should specify DMC storage to accommodate user compliance requirements. Facilities processing personally identifiable information (e.g., business transactions, government issued ID number, credit/banking account numbers) or conforming to the Payment Card Industry-Data Security Standard (PCI-DSS) and Statement on Auditing Standards 70 (SAS70) for physical and logical security should require a minimum of ninety (90) days DMC retention, unless otherwise directed by those standards or AHJ.

If the system requires remote viewing or if the solution is using managed or hosted video, qualified personnel should verify that the end user's connectivity (upstream bandwidth) can support these requirements. Mobile devices require lower resolution and network attached storage can accept a HDTV stream while a lower resolution stream is sent to the remote user or the managed video service.

The ability for the video camera or encoding device to render images that match the VSS primary function should be used.

The use of video cameras and encoding technology with built-in pixel counting can enhance the design process, measurement, and verification of pixels on target.

Smaller objects require higher resolution image capture. Video cameras with image capture characteristics complying with image quality standards are recommended, such as HDTV.

For subjects traveling at speeds of 40 mph and occupying greater than 10 percent of the viewing area, use of both MJPEG and H.264 compression encoding is recommended. For recording subjects exceeding the same relative speed on board a moving craft or vehicle, also use dual encoding.

NOTE: Additional guidance on achieving video quality is offered from a variety of resources (e.g., *Handbook of Video Quality in Public Safety and Security*, as administered by the US Dept. of Homeland Security and Public Safety Communications Research).

9.5.3.2 Use Case Related

For all use cases (see Section 9.5.7), designs should include a:

- DMC source
- VSS physical infrastructure
- VSS logical infrastructure
- VSS video management
- DMC storage

For a use case requiring greater than five (5) sites and low or non-existent VSS control and analysis, the VSS video management should be a network video recorder, video management system application or combined cloud-based video management and storage application/service.

For the use case where the jurisdiction requirements require DMC to not be stored on-site due to theft concerns, the design should specify a combined cloud-based video management and storage application/service.

For a use case requiring less than five (5) sites and medium to high VSS control and analysis, the VSS video management should be a video management system application, physical security information management system or digital data management system.

9.5.4 Testing

Testing shall include site testing for lighting and resolution with actual test objects or test charts developed from applicable standards and documents (e.g., ISO 12233, ISO 14524, HDTV test charts).

All VSS devices shall conform to an interoperability test as specified by the design. Where possible, devices conforming to the Open Network Video Interface Forum (ONVIF) shall be used, as long as the VSS device manufacturer can provide proof of the specification conformance test document.

Devices used that are not ONVIF conformant shall demonstrate interoperability via a manufacturer's application program interface (API), whose support for that API have been in place via an established partner program greater than five years and documented interoperability testing performed.

Qualified personnel shall verify the performance of the video camera or encoding device in production of suitable images for observation, forensic review or recognition functions.

9.5.5 Deployment Process

9.5.5.1 Requirements

Designs shall incorporate information from a video site survey, identify camera functions, and accommodate multiple VSS functions as applicable.

Qualified personnel shall assess the lighting conditions, measure the reflected light at the facility during various times of day and recommend DMC sources capable of rendering usable images with the available illumination and satisfying the primary VSS function. The designer shall also assess the DMC source device compatibility with the color temperature of the reflected light and color rendition index (CRI) of the illumination for compatibility. Use of illumination with as high a CRI is recommended.

Infrared illumination shall be used in the 850 nm wavelength where possible. Network cameras capable of rendering images illuminated by either 850 nm or 950 nm covert infrared illuminations to maintain maximum VSS flexibility shall be used.

VSS devices that utilize PoE shall be provisioned, powered and connected to cabling that conforms to IEEE 802.3. All PSE shall deliver the power on request from a compatible VSS powered device and maintain operation supervised by an external management system. Critical failures, such as PSE device failure, shall be monitored by the owner or end user's information management, information technology or systems solutions staff. PoE and high power PoE designations for powered devices and PSEs shall be considered manufacturer specific and not used where devices compliant with IEEE 802.3 are available. Deployments at higher power levels than these standards shall be accompanied with an analysis of cabling, cabling installation, supporting cabling accessories, local compliance, and dedicated data cabling, negating any temperature concerns and guaranteeing safe and consistent operation.

Qualified personnel (e.g., ESS designer) shall:

- Assess the existing or proposed infrastructure / system architecture / network topology / protocol support and determine the impact on the VSS.
- Recommend specific physical infrastructure improvements as part of the current design or separate project, capital project, or periodic expansion to accommodate the requirements of the VSS.
- Provide guidance for infrastructure lifecycle management, or the continuous assessment of the facility's network system to maintain compatibility with the VSS bandwidth, user access, infrastructure-delivered power, and scalability requirements.
- Consider systems external to the VSS to manage power and connectivity where possible.

  These systems shall be known as infrastructure management systems and shall provide intelligent patching and provision services, using the network to aggregate power usage reporting. The infrastructure management system shall be necessary for systems expected to exceed 20 percent expansion.
- Specify the resolution and image refresh rate for network cameras, according to the use case requirement.
- Provide the necessary data to make use of a user's existing network:
  - Estimate bandwidth using approved manufacturer tools and verify with average site conditions with scene motion.
  - Get individual values.
  - Prepare bandwidth use and overlay on network device map.

  NOTE: Verify expected protocol compliance and performance with user's network or IT professional (ensure sure bandwidth needs and protocol requirements match available infrastructure).

List continues on the next page

- Verify users are satisfied with the workstations' intended use and expected performance.
- Verify server performance and modify VSS as required.
- Finalize the equipment list with merging components into assemblies by function / purpose.
- Create a matrix of VSS uses and stakeholder responsibilities containing:
  - The person and group responsible
  - How the responsible group is informed
  - Identification of input and support to group responsible
- Make use of virtual local area networks (VLANs) and quality of service (QoS) as much as possible to ensure minimal impact on shared infrastructure (See Section 5).
- Dedicated infrastructure shall only be used when the shared infrastructure is over capacity or over-utilized for the use case or when the safety management program, security management program or risk assessment requires.
- Use these documents and define who is responsible for developing a commissioning statement.

9.5.5.2 Recommendations

Where illumination is unavailable or poor-quality images are rendered by the DMC source, designs should consider using infrared illumination and HDTV devices capable of supporting low light conditions. Network-based thermal imaging cameras of the uncooled sensor type, capable of multiple palette rendering, verifying compatibility with the VSS primary function, should be considered.

9.5.6 Authentication of Network Video Cameras for Improved ESS Network Security

9.5.6.1 Requirements

The non-person entity shall be a network camera capable of streaming DMC. The DMC shall also be known as digital video content, network video content or digital multimedia evidence. Each of these formats are capable of incorporating digital data representing audio content, video content, metadata information, location-based information, relevant IP addresses, recording time, and system time attached to a digital file.

Where applicable by user requirements, the DMC source shall be a network camera incorporating embedded memory, SD or MicroSD card media. The network camera shall be capable of running a cryptographic algorithm authenticating the network camera, DMC source originating from the network camera and the DMC user that consumes, stores or displays the DMC in accordance with an identity, credential, and access management (ICAM) policy. This ICAM policy shall incorporate a trustworthy process for assigning attributes to a digital identity (DMC source) and to connect that identity to an individual (DMC user) via a trusted framework.

9.5.7 Use Cases

9.5.7.1 Introduction

The video surveillance system (VSS) use case is defined by the scene characteristics and the specification of the VSS function(s).

9.5.7.2 Scene Requirements

The scene shall be identified to include one or more areas of interest or scene content. The VSS shall be designed to accomplish one or more specific tasks regarding a scene. The primary functions of the VSS shall be identified as one of the following:

- Observation
- Forensic review
- Recognition

9.5.7.2.1 Observation

Video surveillance systems designed for the observation function shall be optimized to provide continuous viewing of scene content captured by the video camera or encoding device, and displayed on local or remote monitors, or on remote display devices (e.g., smart-phones, tablets, laptop computers).

The minimum resolution as measured in ppm (ppf) shall be 65 ppm (20 ppf) to achieve a VSS observation function using imaging standards, such as HDTV.

9.5.7.2.2 Forensic Review

Video surveillance systems designed for the forensic review function shall be optimized to provide high resolution recording of scene content or digital multimedia content (DMC) captured by the video camera or encoding device. The DMC shall have resolution high enough to permit general identification of scene content or object(s) of interest, identification of object colors, specific identification of an object's characteristics, the time, and location of the objects in the DMC.

The minimum resolution shall be 131 ppm (40 ppf) using imaging standards, such as HDTV, to achieve a VSS forensic review function.

9.5.7.2.3 Recognition

Video surveillance systems designed for the recognition function shall be dependent on the specific recognition function required for the use case. Recognition functions shall include but not be limited to:

- Vehicle license plate recognition
- Facial recognition
- Face location
- Smoke and fire detection
- Object recognition
- Pattern recognition
- Cross-line detection
- Object temporal characteristics
- Color recognition
- Trajectory

Qualified personnel shall verify the performance of the video camera or encoding device, together with the recognition application to produce suitable data through site testing with actual test objects.

The minimum resolution as measured in pixels per linear distance shall be 262 ppm (80 ppf) using imaging standards such as HDTV to achieve a VSS recognition function.

Designs shall consider visual verification of image quality using normative resolution and visual acuity tools available where possible. In the case of public safety, homeland security, port security, critical infrastructure, video surveillance used for remote healthcare and all video surveillance applications used by first responders, designs shall incorporate any applicable codes, standards and regulations that offer global best practices.

Designs and component selection shall accommodate the following minimum image quality requirements to optimize recognition and identification:

- Audio, video, and metadata format
- Multiplex and transport protocol
- Data security and integrity

9.5.7.3 Content Criteria

The VSS scene content criteria shall incorporate resolution, object size, speed, trajectory, scene lighting level, and required refresh rate.

- Resolution—Resolution, as required by the VSS primary function, and shall be measured in pixels per meter (ppm) or pixels per foot (ppf). The pixels per meter or foot calculation shall be derived for both horizontal and vertical pixels and is equal to the imager's pixel dimensions divided by the corresponding field of view linear dimension (meter or feet).

  The use of video cameras and encoding technology with built-in pixel counting shall be considered as an enhancement to the design process, measurement and verification of pixels on target.
- Object Size—The size of the object(s) in the scene content, in conjunction with the VSS's primary function, shall be used in the design of the VSS. For all objects occupying 25 percent or less of the field of view, high definition television (HDTV) video cameras shall be required.
- Object Speed and Direction—HDTV video cameras shall be required in video surveillance systems where the moving object(s) of interest occupy 10 percent or less of the field of view. The imager orientation shall match the direction of movement (e.g., aspect ratios 16:9 horizontal, 9:16 vertical).

List continues on the next page

- Lighting Levels—The scene environment and the scene's light sources shall be used in evaluating the lighting of the VSS scene. Lighting levels shall be measured using resolution targets and reflected light.
- Display Refresh Rate—Refresh or display rate in frames (images) per second (fps) for the VSS function shall be matched for the display size. The refresh rate for the VSS function shall be matched to the percentage that the object(s) of interest occupy within the field of view, together with the object's speed and trajectory.

  NOTE: Mobile devices with smaller display resolution utilize a lower minimum refresh rate for the VSS function; larger displays utilize a higher refresh rate.

9.5.7.4 Additional Functions

In addition to the primary VSS use case, additional functions may be included. These functions include:

- Prosecution—The VSS shall incorporate recording of the object's time, location, and specific characteristics, considering the resolution minimum as forensic review function.
- Loss prevention and deterrence—The designer shall employ the use of public view monitors where possible, displaying entry activity and in prominent public view. Inactive camera shells or "dummy" cameras shall not be used.
- Intrusion detection and perimeter monitoring
- Access control identity
- Operations management and resource allocation
- Safety
- Security (object left behind)

9.6 Access Control Systems

9.6.1 Overview

Access control refers to the practice of controlling access to a property, building, or select space within a facility for authorized persons only. Currently, a wide variety of mechanical and electronic hardware devices are used to protect or prevent unauthorized access to important items or to restrict access to protected areas and valuable information. These devices vary from traditional physical keys and locks to elaborate electronic access systems capable of recognizing the biographical and biometric data of system users prior to granting access to secure spaces.

9.6.2 System Structure

9.6.2.1 Overview

The minimum of required components for an ACS include a computer, a control panel, and a peripheral device connected to the control panel. An ACS may be more complex, having multiple control panels and peripheral devices, and may use additional components, such as credentials.

The components of ACS may be classified into the following levels:

- Level 1 – Central equipment processing, recording, software, and database
- Level 2 – Controllers for intelligent field processing (e.g., data gathering panel)
- Level 3 – Peripheral devices (e.g., card reader, lock, door position switch)
- Level 4 – Credentials (e.g., cards, fobs, biometrics, personal identification numbers [PINs], passwords)

9.6.3 Peripheral Devices

9.6.3.1 Overview

Peripheral devices may be sensor equipment that monitors certain conditions (e.g., temperature) and reports the status back to the control panel. Peripheral devices also may be output devices that control passage through entryways or bells indicating shift change.

Peripherals in ACS are generally classified as being in one of the following categories:

- Door contacts—used for monitoring an open or closed door.
- Readers
- Electrified door hardware
- Request-to-exit devices

9.6.3.2 Readers

Readers shall be placed and installed in accordance to codes and the AHJ, in addition to any requirements pertaining to the accessibility or interaction by a person (e.g., *Americans with Disabilities Act*).

9.6.3.3 Electrified Door Hardware

9.6.3.3.1 Overview

Electrified door release hardware is a generic term for electromechanical locking hardware that is released upon an approval signal. This signal may originate from various sources, such as a simple remote button or the ACS software.

9.6.3.3.2 Requirements

Electrified door hardware shall meet all applicable codes and requirements of the AHJ.

9.6.3.4 Request to Exit Devices

9.6.3.4.1 Overview

A request to exit (REX, or also known as RX, RTE, or RQE) device is a device installed on the secure side of the door that allows egress without triggering an alarm. In most ACS, if the door opens from either side without a valid credential presented to the reader or REX, an alarm is activated. When activated, the REX device sends a REX signal to the ACS, communicating an authorized exit through the door.

9.6.3.4.2 Requirements

A REX may be used to unlock a door from the egress side to exit an area, which is commonly performed using magnetic locks. When a REX device is used for this purpose, its installation and use shall conform to applicable codes and the AHJ.

9.6.4 Fail-Secure/Fail-Safe/Fail Latched

9.6.4.1 Fail Secure

9.6.4.1.1 Overview

Fail-secure hardware goes to a locked state when power is removed from the hardware. It is sometimes referred to as power unlocked. Power is applied to unlock this type of device. This type of hardware is normally specified for security purposes as a device failure leaves the door secured.

9.6.4.1.2 Requirements

If a fail-secure device is kept unlocked for long periods of time, the device shall be rated for continuous duty.

9.6.4.1.3 Recommendations

Employing an inline power conditioner to minimize DC voltage surges also is recommended to extend the life of the device.

9.6.4.2 Fail Safe

9.6.4.2.1 Overview

Fail-safe hardware fails in the unlocked position when power is removed. It is sometimes referred to as power locked. Power is removed to unlock this type of device. This type of device is normally used in emergency situations when the door must fail unlocked for life safety egress.

9.6.4.2.2 Recommendations

Certain door release devices require power to lock (e.g., magnetic locks). When door release devices requiring power to lock are used solely for security purposes and there are no life safety issues, backup power is recommended.

9.6.4.3 Fail-Latched

9.6.4.3.1 Requirements

A related term to "fail-secure" is "fail-latched". Fire-rated door release devices shall be rated fail-secure to avoid unlatched egress doors. Doors that are fire rated and part of a fire separation (e.g., stairwell doors) shall remain latched even though they are unlocked.

9.6.4.4 Fail-Secure and Fail-Safe REXs

9.6.4.4.1 Overview

The installation and setup of REX devices that require power have to be carefully planned and performed. If the REX is set to the fail-secure configuration and power is lost, the REX will not change state, bypass the alarm, or open the door. If the REX is set to the fail-safe configuration and power is lost, the REX changes state, bypasses the alarm, and releases the door.

9.6.4.4.2 Requirements

The following items shall be verified when using fail-secure or fail-safe REXs:

- Does the PIR, door release button, or panic button unlock the door when activated?
- Does the door lock automatically on closure?
- Does the ACS detect that the door is open and display this condition?
- Does a local audible alarm sound when the door is opened?
- If required, is video coverage of the door adequate?
- Is an alarm generated if the door is open longer than the preset time?
- Is the fail-safe configuration for proper operation feasible?
- Does the door release when power is lost?

9.6.5 Power

9.6.5.1 Backup Power Recommendations

The ACS power supply should have a backup. All computers should be provided with an UPS that can provide the required length of operation. The minimum time recommended for an orderly shutdown and saving of all data with a software/hardware connection to the ACS computers should be fifteen minutes.

The card reader panels should have some type of battery backup for the electronics, and where possible, the doors controlled by the reader panel. A four-hour backup should be provided for door operation. Depending on the application and applicable codes, the AHJ may provide requirements for the reader panel back-up.

NOTE: AHJs may require that a door fail-safe when the batteries fail.

If emergency power is available, it may be advantageous to connect the ACS to this source as well as to the UPS.

In addition to backup power recommendations, the designer may request dedicated access control branch circuits for the primary power source for ACS equipment.

9.6.5.2 Peripheral Power Recommendations

Peripheral devices are typically powered by either 12 V_{DC} or 24 V_{AC} power supplies. Voltage drop should be considered when determining the distance from the device to the power source. Once the voltage drop is considered, the appropriate gauge wire size should be specified to ensure adequate voltage reaches the device.

Connecting the device to multi-fused 12–24 V_{DC}/V_{AC} power supply centralizes the power sources for multiple devices and accessories. This is in lieu of having AC outlets installed near each device. Voltage drop and wire size calculations should be considered for each individual device back to the multifused power supply.

The AC power input, the power transformer, and all fused power outputs should be enclosed in one lockable enclosure with tamper switches monitored by the alarm monitoring system. It is recommended that all outputs be individually fused. If a device or accessory is individually AC powered, more UPS circuits may be needed than when using a multi-fused power supply. A multi-fused power supply also simplifies placing a UPS circuit by having only one source for the multiple devices or accessories.

9.6.5.3 Power to Locks

9.6.5.3.1 Requirements

Power supplies shall be sized to provide adequate power for the connected devices and have a source of primary power at their location.

9.6.5.3.2 Recommendations

Having battery backup to allow uninterrupted operation for a selected period of time in the event of loss of primary power is desirable.

Certain types of release hardware require specific power supplies because of the initial power inrush necessary to activate the device. This power may be significantly different from the power necessary to keep the device seated in a normal operation.

NOTE: This type of power inrush is most commonly seen with electrified exit or panic hardware.