



First Revision No. 9-NFPA 731-2021 [Global Input]

Throughout the document remove “Standard for” from all UL standard Titles.

Submitter Information Verification

Committee:

Submittal Date: Tue Apr 13 12:22:57 EDT 2021

Committee Statement

Committee Statement: The Technical Committee deletes the term “Standard for” from all UL standard titles as it is redundant and unnecessary.

Response Message: FR-9-NFPA 731-2021

[Public Input No. 21-NFPA 731-2021 \[Global Input\]](#)



First Revision No. 17-NFPA 731-2021 [New Section after 1.2.1]

1.2.2

This standard addresses the cybersecurity protection of equipment or systems covered by this standard.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:12:39 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a standalone section for cyber security to address the growing need for cyber security protection.

Response Message: FR-17-NFPA 731-2021

Public Input No. 2-NFPA 731-2020 [New Section after 1.2.1]



First Revision No. 19-NFPA 731-2021 [Section No. 1.2.1]

1.2.1

The purpose of this standard is to define the means of signal initiation, transmission, notification, and annunciation; the levels of performance; and the reliability of premises security systems. ~~This standard addresses the integrity and reliability of cyber intrusion protection for equipment or systems network connected to the Internet of Things (IoT).~~

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:16:03 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision that accomplishes two things.

1. Comply with the NFPA Manual of Style
2. The requirement relating to cyber security needs a standalone section because of the growing concern and importance of cyber related issues

Response Message: FR-19-NFPA 731-2021

[Public Input No. 1-NFPA 731-2020 \[Section No. 1.2.1\]](#)



First Revision No. 21-NFPA 731-2021 [Section No. 1.3.1]

1.3.1 Premises Security Systems.

Premises security systems shall include one or more of the following system types:

- (1) Intrusion detection systems
- (2) Access control systems
- (3) Video surveillance systems
- (4) Asset protection systems
- (5) Environmental detection systems
- (6) Holdup and duress systems
- (7) Integrated systems
- (8) Monitoring services and systems

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:31:21 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision to add monitoring services and systems to the list of premises security system types.

Response Message: FR-21-NFPA 731-2021

[Public Input No. 3-NFPA 731-2020 \[Section No. 1.3.1\]](#)



First Revision No. 22-NFPA 731-2021 [Section No. 1.3.5.1]

1.3.5.1 Electronic Hardware Components.

This standard applies to new installations and alterations of premises security systems or their components installed for protection of building interiors, building perimeters, and surrounding property.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:49:26 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision to include renovation work to the scope of the Standard. The TC uses the the term alterations rather than renovations to add clarity.

Response Message: FR-22-NFPA 731-2021

[Public Input No. 4-NFPA 731-2020 \[Section No. 1.3.5.1\]](#)



First Revision No. 23-NFPA 731-2021 [Section No. 1.3.5.3]

1.3.5.3 Software.

In this standard, software includes ~~the system firmware~~ , but is not limited to, site-specific software, firmware, cybersecurity software, executive software, and associated software for system functionality .

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:59:22 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision that edits 1.3.5.3 to clarify the various types of software.

Response Message: FR-23-NFPA 731-2021

[Public Input No. 5-NFPA 731-2020 \[Section No. 1.3.5.3\]](#)



First Revision No. 25-NFPA 731-2021 [Section No. 1.4.2]

1.4.2

Unless otherwise noted, it is not intended that the provisions of this standard be applied to facilities, equipment, structures, or installations that were existing or approved for construction or installation prior to the adoption and effective date of this standard.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 15:20:11 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision that clarifies the provisions of the standard does not apply if a jurisdiction has not adopted the standard. The added language helps to clarify this.

Response Message: FR-25-NFPA 731-2021

[Public Input No. 7-NFPA 731-2020 \[Section No. 1.4.2\]](#)



First Revision No. 10-NFPA 731-2021 [Section No. 2.3.3]

Global FR-9

2.3.3 UL Publications.

Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

UL 50, ~~Standard for Enclosures for Electrical Equipment, Non-Environmental Considerations~~, 2015.

UL 50E, ~~Standard for Enclosures for Electrical Equipment, Environmental Considerations~~, 2015 2020.

UL 294, ~~Standard for Access Control System Units~~, 2013 2018.

UL 606, ~~Standard for Linings and Screens for Use with Burglar-Alarm Systems~~, 1999, revised 2006.

UL 634, ~~Standard for Connectors and Switches for Use with Burglar-Alarm Systems~~, 2007, revised 2014 2020.

UL 636, ~~Standard for Holdup Alarm Units and Systems~~, 2013.

UL 639, ~~Standard for Safety for Intrusion-Detection Units~~, 2007, revised 2011 2019.

UL 827, ~~Standard for Central-Station Alarm Services~~, 2014, revised 2016 2020.

UL 1076, ~~Standard for Proprietary Burglar Alarm Units and Systems~~, 2010 2018.

UL 2044, ~~Standard for Commercial Closed-Circuit Television Equipment~~, 2008, revised 2016 2019.

UL 2610, Commercial Premises Security Alarm Units and Systems, 2018, revised 2020.

UL 2802, ~~Standard for Performance Testing of Camera Image Quality~~, 2014 2013, revised 2019.

UL 2900-2-3, ~~Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems~~, 2017 2020.

UL 60065, ~~Standard for Audio, Video and Similar Electronic Apparatus~~, 2015 2020.

UL 60950-1, ~~Standard for Information Technology Equipment~~, 2007, revised 2013 2019.

UL 60950-22, ~~Standard for Information Technology Equipment — Equipment to Be Installed Outdoors~~, 2007 2017.

UL 62368, ~~Standard for Audio/Video, Information and Communication Technology Equipment~~, 2014 2019.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:35:40 EDT 2021

Committee Statement

Committee Statement: The Technical Committee updates all UL Standard edition dates and changes UL/ULC 2900 from an Outline of Investigation to a Standard and adds UL 2610 which has absorbed UL 636 and 1076.

UL 636 and UL 1076 will remain active standards, so they should continue to be referenced in Chapter 2 for this next edition of 731.

Response
Message: FR-10-NFPA 731-2021

[Public Input No. 22-NFPA 731-2021 \[Section No. 2.3.3\]](#)

[Public Input No. 8-NFPA 731-2020 \[Section No. 2.3.3\]](#)



First Revision No. 32-NFPA 731-2021 [Section No. 2.4]

2.4 References for Extracts in Mandatory Sections.

NFPA 72[®], National Fire Alarm and Signaling Code[®], 2019 2022 edition.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Jun 01 09:20:07 EDT 2021

Committee Statement

Committee Statement: Update date of NFPA 72 to 2022

Response Message: FR-32-NFPA 731-2021



First Revision No. 4-NFPA 731-2021 [Section No. 3.3.6]

3.3.32* ~~Closed Circuit Television (CCTV)~~ Video Surveillance System .

A video system in which an analog or digital video signal travels from the camera to video monitoring stations at the protected premises.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:00:09 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR to change Closed Circuit Television (CCTV) to "Video Surveillance System". Chapter 7 is titled Video Surveillance Systems. This language is added to better align with modern technology. The title of the chapter uses the term "video surveillance".

Response Message: FR-4-NFPA 731-2021



First Revision No. 20-NFPA 731-2021 [New Section after 3.3.8]

3.3.8 Cybersecurity.

The protection of systems from theft or damage of data, or damage to hardware or software, as well as from unauthorized command or control or access to any information of any services the systems provide. [72, 2022]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 14:20:44 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a new definition for "cyber security" by extracting the definition from the 2022 edition of NFPA 72 (see FR-5069).

Response Message: FR-20-NFPA 731-2021



First Revision No. 24-NFPA 731-2021 [New Section after 3.3.24.3]

3.3.25 Software.

Programs, instruments, procedures, data, and the like that are executed by a central processing unit of a product and that influences the functional performance of that product. For the purpose of this standard, software is one of two types: executive software and site-specific software. [72, 2022]

3.3.25.1 Executive Software.

Control and supervisory program that manages the execution of all other programs and directly or indirectly causes the required functions of the product to be performed. Executive software is sometimes referred to as firmware, BIOS, or executive program. [72, 2022]

3.3.25.2 Site-Specific Software.

Program that is separate from, but controlled by, the executive software that allows inputs, outputs, and system configuration to be selectively defined to meet the needs of a specific installation. Typically, it defines the type and quantity of hardware, customized labels, and the specific operating features of a system. [72, 2022]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 15:16:39 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision because there are different types of software as well as different requirements for each type of software. The Technical Committee adds definitions to clarify the various types of software.

Response Message: FR-24-NFPA 731-2021

Public Input No. 6-NFPA 731-2020 [New Section after 3.3.25]



First Revision No. 26-NFPA 731-2021 [Section No. 4.4.2.3]

4.4.2.3*

The location of the circuit disconnecting means shall be permanently identified by the required marking located on the inside of the protected ~~at the~~ premises security control unit.

A.4.4.2.3

The requirement seeks to prohibit the general public from knowing the location of the security control circuit disconnecting means.

Submitter Information Verification

Committee: PMM-AAA

Submission Date: Tue Apr 13 15:21:42 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision to ensure only authorized personnel will have knowledge to the location of the marking of the circuit disconnecting means. The TC adds annex text for clarity.

Response Message: FR-26-NFPA 731-2021

Public Input No. 9-NFPA 731-2021 [Section No. 4.4.2.3]



First Revision No. 27-NFPA 731-2021 [Section No. 4.4.3.4]

4.4.3.4

The secondary supply shall consist of one of the following:

- (1) A storage battery dedicated to the premises security system arranged in accordance with 4.4.4
- (2) An individual branch circuit of an automatic-starting engine-driven generator arranged in accordance with 4.4.5 and storage batteries dedicated to the premises security system with ~~15 minutes of capacity under~~ 4 hours of minimum capacity under maximum alarm standby and 15 minutes under full load
- (3) An emergency generating system as defined in *NFPA 70*, Article 700

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 15:35:32 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision to clarify the secondary capacity and increase the full load capacity to 4 hours. The reason for the 4 hour change is to align with NFPA 72.

Response Message: FR-27-NFPA 731-2021

[Public Input No. 10-NFPA 731-2021 \[Section No. 4.4.3.4\]](#)



First Revision No. 28-NFPA 731-2021 [Section No. 4.4.3.5]

4.4.3.5

Intrusion detection systems, video surveillance systems, and access control systems shall comply with 4.4.3.5.1 through 4.4.3.5.3 , as applicable.

4.4.3.5.1

Intrusion detection system control units shall have a backup capacity under quiescent load (system operating in a nonalarm condition) for a minimum of 24 hours.

4.4.3.5.2

Video surveillance systems shall have a backup capacity under quiescent load (system operating in normal condition) for a minimum of 4 hours.

4.4.3.5.3

Access control systems shall have a backup capacity under quiescent load (system operating in normal condition) for a minimum of 4 hours.

4.4.3.6*

The secondary supply of systems other than intrusion detection systems, video surveillance systems, and access control systems shall have the capacity to operate a premises security system for the longest time required by any of the following:

- (1) SVA (satisfies the needs determined)
- (2) System design
- (3) Manufacturer's published instructions
- (4) Other applicable standards

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 16:46:17 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision to require a minimum of secondary power to prevent unwanted alarms should there be a power failure or the power to the system is inadvertently turned off.

Response Message: FR-28-NFPA 731-2021

Public Input No. 11-NFPA 731-2021 [Section No. 4.4.3.5]



First Revision No. 29-NFPA 731-2021 [Section No. 5.3.3.1.9.4]

5.3.3.1.9.4

Motion detectors shall include, but not be limited to, the following:

- (1) Two or more technologies combined in a single device

~~Microwave~~

- (2) Passive infrared (PIR)

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 16:48:50 EDT 2021

Committee Statement

Committee Statement: The Technical Committee deletes microwave. Microwave by itself is not often used; dual technologies should be used. Microwave devices can cause unwanted alarms if not sited properly. They are also more prone to environmental stimuli which can cause unwanted alarms.

Response Message: FR-29-NFPA 731-2021

[Public Input No. 12-NFPA 731-2021 \[Section No. 5.3.3.1.9.4\]](#)



First Revision No. 1-NFPA 731-2021 [New Section after 6.1.4.7]

6.1.4.8

Where biometrics are used, they shall be implemented in accordance with local, state, and federal government data privacy provisions and laws.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 11:21:01 EDT 2021

Committee Statement

Committee Statement: The Technical Committee adds new text and creates a First Revision and adds the word "federal".

Response Message: FR-1-NFPA 731-2021

Public Input No. 16-NFPA 731-2021 [New Section after 6.1.5]



First Revision No. 2-NFPA 731-2021 [New Section after 6.3]

6.4* Access Control Software as a Service (SaaS).

The configuration of the service and system shall be compliant with a control framework that is in compliance with industry-recognized standards.

A.6.4

SaaS solutions should have audited data security controls based on established standards,

frameworks, and codes of practice such as the following:

- (1) CSA Security Trust Assurance and Risk (STAR) Program
- (2) Federal Risk and Authorization Management Program (FedRAMP)
- (3) ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
- (4) ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls
- (5) Service organization control (SOC) reports such as ISAE 3402, Assurance Reports on Controls at a Service Organization
- (6) UL 2900-2-3, Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 11:23:52 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates a First Revision. The TC deletes the majority of the PI-17 submission due to duplication of existing sections of chapter 6. A Task Group has been assigned to review the requirements. The TC edits section 6.4, 6.4.1, and A.6.4.1.

Response Message: FR-2-NFPA 731-2021

Public Input No. 17-NFPA 731-2021 [New Section after 6.3]



First Revision No. 3-NFPA 731-2021 [Section No. 7.1.1]

7.1.1

This section shall apply to the installation requirements for ~~closed circuit television (CCTV) systems~~ video surveillance systems (previously referred to as "CCTV") and digital imaging systems.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 11:54:48 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR in agreement with the proposed text. Technology has evolved to the point where viewing video is typically no longer "closed circuit". This language is added to better align with modern technology. The title of the chapter uses the term "video surveillance".

Response Message: FR-3-NFPA 731-2021

[Public Input No. 20-NFPA 731-2021 \[Section No. 7.1.1\]](#)



First Revision No. 5-NFPA 731-2021 [Section No. 7.1.5.1]

7.1.5.1

Control units, subcontrols, and devices that are used to interconnect the cameras to NIDs or CCTV video surveillance control units shall be located within a secured area.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:03:03 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR to change "CCTV" to "video surveillance". This language is added to better align with modern technology. The title of the chapter uses the term "video surveillance".

Response Message: FR-5-NFPA 731-2021



First Revision No. 11-NFPA 731-2021 [Section No. 8.1.1.1]

[Global FR-9](#)

8.1.1.1

The construction of holdup alarm initiating devices shall be in compliance with applicable standards, such as UL 636, ~~Standard for Holdup Alarm Units and Systems~~, or UL 2610, Commercial Premises Security Alarm Units and Systems.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:39:56 EDT 2021

Committee Statement

Committee Statement: The Technical Committee adds UL 2610. UL 2610 will supersede collateral standards such as UL 636.

Response Message: FR-11-NFPA 731-2021

[Public Input No. 23-NFPA 731-2021 \[Section No. 8.1.1.1\]](#)



First Revision No. 12-NFPA 731-2021 [Section No. 8.1.1.2]

8.1.1.2

The construction of private duress alarm initiating devices shall be in compliance with applicable standards, such as UL 636, ~~Standard for Holdup Alarm Units and Systems~~, or UL 2610, Commercial Premises Security Alarm Units and Systems .

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:44:27 EDT 2021

Committee Statement

Committee Statement: The Technical Committee adds UL 2610. UL 2610 will supersede collateral standards such as UL 636.

Response Message: FR-12-NFPA 731-2021

[Public Input No. 24-NFPA 731-2021 \[Section No. 8.1.1.2\]](#)



First Revision No. 15-NFPA 731-2021 [Section No. 9.4.1]

[Global FR-9](#)

9.4.1

Proprietary monitoring stations shall be physically configured and maintained in conformance with UL 1076, ~~Standard for Proprietary Burglar Alarm Units and Systems~~, Clause "Proprietary Burglar Alarm Service," or UL 2610, Commercial Premises Security Alarm Units and Systems.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 13:06:00 EDT 2021

Committee Statement

Committee Statement: The Technical Committee adds UL 2610. UL 2610 will supersede collateral standards such as UL 1076.

Response Message: FR-15-NFPA 731-2021



First Revision No. 6-NFPA 731-2021 [Section No. 10.4.3 [Excluding any Sub-Sections]]

Premises security systems and other systems and equipment that are associated with security systems and accessory equipment shall be tested according to Table 10.4.3(a), Table 10.4.3(b), and Table 10.4.3(c).

Table 10.4.3(a) Test Methods

<u>Devices</u>	<u>Test Methods</u>
Control equipment	
(1) Function	Verify correct receipt of alarm, supervisory, and trouble signals (inputs); operation of evacuation signals and auxiliary functions (outputs); circuit supervision, including detection of open circuits and ground faults; and power supply supervision for detection of loss of ac power and disconnection of secondary batteries.
(2) Fuses	Verify rating and supervision for field-removable fuses that are not integral to the control equipment.
(3) Interfaced equipment	Verify integrity of circuits providing interface between two or more control units. Test interfaced equipment connections by operating or simulating operation of the equipment being supervised. Verify signals required to be transmitted at the control unit.
(4) Lamps and LEDs	Illuminate lamps and LEDs.
(5) Primary (main) power supply	Test under maximum load, including all alarm appliances requiring simultaneous operation. Test redundant power supplies separately.
Engine-driven generator	If an engine-driven generator dedicated to the system is used as a required power source, verify operation of the generator in accordance with NFPA 110.
Secondary (standby) power source	Disconnect all primary (main) power supplies and verify the occurrence of required trouble indication for loss of primary power. Measure or verify the system's standby and alarm current demand and verify the ability of batteries to meet standby and alarm requirements using manufacturer's data. Operate general alarm systems a minimum of 5 minutes and sounders for a minimum of 15 minutes. Reconnect primary (main) power supply at end of test.
Uninterruptible power supply (UPS)	If a UPS system dedicated to the system is used as a required power source, verify operation of the UPS system in accordance with NFPA 111.
Batteries — general tests	Prior to conducting any battery testing, verify that all system software stored in volatile memory is protected from loss.
(1) Visual inspection	Inspect batteries for corrosion or leakage along with the tightness of connections. Clean the batteries if necessary and confirm the connections are tight and the levels of electrolyte are as specified by the manufacturer.
(2) Battery replacement	Replace batteries in accordance with the recommendations of the alarm equipment manufacturer or when the recharged battery voltage or current falls below the manufacturer's recommendations.
(3) Charger test	With the batteries fully charged and connected to the charger, place an ampere meter in series with the battery under charge. Verify the charging current is in accordance with the manufacturer's recommendations for the type of battery used. In the absence of specific information, use $\frac{1}{30}$ to $\frac{1}{25}$ of the battery rating.
(4) Discharge test	With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery.

<u>Devices</u>	<u>Test Methods</u>
(5) Load voltage test	With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the float voltage for the entire battery is 1.42 volts per cell, nominal, under load. If possible, measure cells individually. An artificial load equal to the full premises security system is permitted to be used in conducting this test.
Battery tests (specific types)	
(1) Lead-acid type	With the batteries fully charged and connected to the charger, measure the voltage across the batteries with a voltmeter. Verify the voltage is 2.30 volts per cell ± 0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the battery does not fall below 2.05 volts per cell under load. Measure as required the specific gravity of the liquid in the pilot cell or all of the cells. Verify the specific gravity is within the range specified by the manufacturer. Although the specified specific gravity varies from manufacturer to manufacturer, a range of 1.205–1.220 is typical for regular lead-acid batteries, while 1.240–1.260 is typical for high-performance batteries. Do not use a hydrometer that shows only a pass or fail condition of the battery and does not indicate the specific gravity; such a reading does not give a true indication of the battery condition.
(2) Nickel-cadmium type	With the batteries fully charged and connected to the charger, place an ampere meter in series with the battery under charge. Verify the charging current is in accordance with the manufacturer's recommendations for the type of battery used. In the absence of specific information, use $\frac{1}{30}$ to $\frac{1}{25}$ of the battery rating. With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the float voltage for the entire battery is 1.42 volts per cell, nominal, under load. If possible, measure cells individually.
(3) Sealed lead-acid type	With the batteries fully charged and connected to the charger, measure the voltage across the batteries with a voltmeter. Verify the voltage is 2.30 volts per cell ± 0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. Verify the battery performs under load, in accordance with the battery manufacturer's specifications.
Transient voltage surge suppression	Lightning protection equipment is to be inspected and maintained per the manufacturer's specifications. Additional inspections are required after any lightning strikes.
Sound and visual devices	
(1) Audible	Test in accordance with the manufacturer's published instructions.
(2) Visible	Test in accordance with the manufacturer's instructions.

<u>Devices</u>	<u>Test Methods</u>
Transmitting equipment	Verify receipt of the correct initiating device signal at the monitoring station.
Interface equipment	Verify integrity of single or multiple circuits providing interface between two or more control units. Test interfaced equipment connections by operating or simulating operation of the equipment being supervised. Verify signals required to be transmitted at the control unit.
Low-powered radio (wireless systems)	(1) Use the manufacturer's published instructions to verify correct operation after the initial testing phase has been performed by the supplier or by the supplier's designated representative. (2) Starting from the functional operating condition, initialize the system in accordance with the manufacturer's published instructions. Confirm that an alternative communications path exists between the wireless control unit and peripheral devices used to establish initiation, indication, control, and annunciation. Test the system for both alarm and trouble conditions. (3) Check batteries of all components in the system monthly unless the control unit checks the batteries and components daily.
Annunciators	Verify the correct operation and identification of annunciators. Verify the correct operation of the annunciator under a fault condition.
Conductors — metallic	
(1) Stray voltage	Test all installation conductors with a volt/ohmmeter to verify that there are no excessive stray (unwanted) voltages between installation conductors or between installation conductors and ground. Verify the maximum allowable stray voltage does not exceed 1 volt ac/dc, unless a different threshold is specified in the manufacturer's published instructions for the installed equipment.
(2) Ground faults	Test all installation conductors, other than those intentionally and permanently grounded, for isolation from ground per the installed equipment manufacturer's published instructions.
(3) Short-circuit faults	Test all installation conductors, other than those intentionally connected together, for conductor-to-conductor isolation per the manufacturer's published instructions for the installed equipment.
(4) Supervision	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices, sounders, and controlled devices on every initiating device circuit and sounder circuit.
Conductors — nonmetallic	
(1) Circuit integrity	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices, sounders, and controlled devices on every initiating device circuit and sounder circuit. Verify all circuits are monitored for integrity.
(2) Fiber optics	Test the fiber-optic transmission pathway by the use of an optical power meter or by an optical time domain reflectometer used to measure the relative power loss of the line. Test result data must meet or exceed ANSI/TIA 568.3-D, <i>Optical Fiber Cabling and Components Standard</i> , related to fiber-optic pathways and connection/splice losses and the control unit manufacturer's published specifications.
(3) Supervision	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices and sounders. Test each initiating device and sounder circuit for correct indication at the control unit.

Table 10.4.3(b) Test Methods of Initiating Devices

<u>Initiating Devices</u>	<u>Test Methods</u>
<i>Intrusion Detection Devices</i>	
Audio sensors	Using a sound level meter designed, constructed, and calibrated in accordance with ANSI/ASA S1.4, <i>American National Standard Electroacoustics — Sound Level Meters — Part 3: Periodic Tests</i> , determine that the average ambient sound does not exceed the manufacturer's recommendation for the ambient sound level during the period the intrusion detection system is armed. Ensure that the area covered by a single detector does not exceed the area of coverage specified by the detector manufacturer. Utilizing the method recommended by the manufacturer, test the operation of the system.
Contacts	
(1) Door	Open the door.
(2) Window	Open the window.
Exterior buried detectors	Test in accordance with manufacturer's published instructions
Glass break detectors	
(1) Audio	Test in accordance with manufacturer's published instructions
(2) Shock	Test in accordance with manufacturer's published instructions
Motion detection	
(1) Passive infrared (PIR)	Walk across the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
(2) Microwave	Walk into the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
(3) Dual technologies	Walk diagonally across the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
Photoelectric detection	Disrupt the channel of detection by passing an object through the channel.
Pressure and stress sensors	Test in accordance with manufacturer's published instructions
Protective cable	Test in accordance with manufacturer's published instructions
Proximity sensors	Test in accordance with manufacturer's published instructions
Shock sensors	Test in accordance with manufacturer's published instructions
Sound detection — vault	Test in accordance with manufacturer's published instructions
Holdup devices	
(1) Fixed in place	Simulate a holdup alarm condition by activating the device.
(2) Portable	Simulate a holdup alarm condition by activating the device at the maximum distance of the area of intended use.
Duress devices	
(1) Fixed in place	Simulate a duress condition by activating the device.
(2) Portable	Simulate a duress condition by activating the device at the maximum distance of the area of intended use.
Ambush devices	

<u>Initiating Devices</u>	<u>Test Methods</u>
(1) Fixed in place	Simulate an ambush alarm condition by activating the device.
(2) Portable	Simulate an ambush condition by activating the device at the maximum distance of the area of intended use.
<i>Access Control Components</i>	
Controller	Test in accordance with manufacturer's published instructions
Readers	
(1) Key	Test in accordance with manufacturer's published instructions
(2) Magnetic stripe	Test in accordance with manufacturer's published instructions
(3) Radio frequency identification (RFID) card	Test in accordance with manufacturer's published instructions
(4) Biometric	Test in accordance with manufacturer's published instructions
Position sensor	Test in accordance with manufacturer's published instructions
Electric latch	Test in accordance with manufacturer's published instructions
Electric lock	Test in accordance with manufacturer's published instructions
Electromagnetic lock	Test in accordance with manufacturer's published instructions
Request-to-exit (RTE) devices	
(1) Manual	Test in accordance with manufacturer's published instructions
(2) Motion	Test in accordance with manufacturer's published instructions
<i>CCTV Video Surveillance Devices</i>	
Video controller	Test in accordance with manufacturer's published instructions
Video switcher	Test in accordance with manufacturer's published instructions
Monitor	Test in accordance with manufacturer's published instructions
Camera	Test in accordance with manufacturer's published instructions
Enclosure	Test in accordance with manufacturer's published instructions

Table 10.4.3(c) Test Methods of Asset Protection Systems

<u>Asset Protection System</u>	<u>Test Method</u>
Tuning	Perform antenna placement, tuning, and measurements for optimal performance in accordance with the manufacturer's published instructions.
Verification	Use the manufacturer's published instructions manual provided by the system supplier to verify correct operation. Initialize the systems in accordance with the manufacturer's operation manual. Conduct a test to verify the presence of the exit lanes and simulate the event of an unauthorized removal of a tagged asset. Test the system for alarm, interference, and trouble conditions.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:09:14 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR to change CCTV Devices to Video Surveillance Devices. This language is added to better align with modern technology.

Response Message: FR-6-NFPA 731-2021



First Revision No. 7-NFPA 731-2021 [Section No. A.3.3.6]

A.3.3.32 ~~Closed-Circuit Television (CCTV~~ Video Surveillance System) .

The closed circuit signal can connect by, but is not limited to, coaxial, unshielded twisted pair (UTP), category cable (Cat 5, 5e, 6, etc.), fiber optics, microwave, radio frequency (RF), light (infrared or laser), local area networks (LANs), wide area networks (WANs), and Internet.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:11:35 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR to change Closed Circuit Television (CCTV) to "Video Surveillance System".

Response Message: FR-7-NFPA 731-2021



First Revision No. 8-NFPA 731-2021 [Section No. A.10.5]

A.10.5

Premises security systems and other systems and equipment that are associated with security systems and accessory equipment should be tested at the frequencies according to Table A.10.5.

Table A.10.5 Test Frequency

<u>System, Device, or Equipment</u>	<u>Frequency</u>
Intrusion detection system	Annually
(1) Exterior detectors	Annually
(2) Interior detectors	Annually
Holdup, duress, or ambush system	Annually
(1) Portable devices	Annually
(2) Exterior fixed devices	Annually
(3) Interior fixed devices	Annually
Access control system	Annually
(1) Readers	Annually
(2) Position switches	Annually
(3) Electric hardware	Annually
(4) Request-to-exit devices	Annually
CCTV <u>Video surveillance</u> system	Annually
(1) Camera enclosures	Annually and before adverse weather conditions
(2) Recorders	Annually
Sounding devices	Annually
Batteries — general tests	Annually
Off-premises transmission equipment	Quarterly or by automatic monthly test
Interface equipment	Annually

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:13:23 EDT 2021

Committee Statement

Committee Statement: The Technical Committee creates an FR to change “CCTV” to “Video surveillance” in Table A.10.5. This provides consistency with similar changes made elsewhere in the document.

Response Message: FR-8-NFPA 731-2021



First Revision No. 13-NFPA 731-2021 [Section No. G.4.4.1]

[Global FR-9](#)

G.4.4.1

The teller's holdup alarm in a bank is a common example of an emergency alarm. Based on a risk analysis, emergency alert alarms should be considered for use at medical treatment facilities, personnel counseling or interview offices, credit unions, cash-handling activities, and other high-risk areas. The type and location of the device should be selected carefully to ensure the device is readily available for surreptitious activation in an emergency. If there is a building security force, a silent alarm should annunciate at the dispatch point. If not, the alarms can be transmitted directly to a monitoring station location or directly connected to local police. Holdup alarm units should be listed to UL 636, *Standard for Holdup Alarm Units and Systems*, or UL 2610, *Commercial Premises Security Alarm Units and Systems*.
[730:E.4.4.1]

Submitter Information Verification

Committee: PMM-AAA

Submission Date: Tue Apr 13 12:46:04 EDT 2021

Committee Statement

Committee Statement: The Technical Committee updates the addition adds UL 2610. UL 2610 will supersede collateral standards such as UL 636.

Response Message: FR-13-NFPA 731-2021

[Public Input No. 25-NFPA 731-2021 \[Section No. G.4.4.1\]](#)



First Revision No. 30-NFPA 731-2021 [New Section after H.1.2.2]

H.1.2.3 CSA Publications.

Cloud Security Alliance Bellingham Office, 709 Dupont Street, Bellingham, WA 98225.
cloudsecurityalliance.org/star

CSA Security Trust Assurance and Risk (STAR) Program.

H.1.2.4 GSA Publications.

General Services Administration Technology Transformation Services, 1800 F Street NW,
Washington, DC 20405. fedramp.gov

Federal Risk and Authorization Management Program (FedRAMP).

H.1.2.5 IAASB Publications.

International Auditing and Assurance Standards Board, 529 5th Avenue, New York, NY
10017.

ISAE 3402, Assurance Reports on Controls at a Service Organization , 2011.

H.1.2.6 ISO Publications.

International Organization for Standardization, ISO Central Secretariat, Chemin de
Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland. iso.org

ISO/IEC 27001, Information technology — Security techniques — Information security
management systems — Requirements , 2013.

ISO/IEC 27002, Information technology — Security techniques — Code of practice for
information security controls , 2013.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed Apr 14 15:14:32 EDT 2021

Committee Statement

Committee Statement: The Technical Committee adds CSA, FedRAMP, IAASB and ISO Publications as these are now referenced in 6.4.

Response Message: FR-30-NFPA 731-2021



First Revision No. 31-NFPA 731-2021 [Section No. H.1.2.2]

H.1.2.2 BHMA Publications.

Builders Hardware Manufacturers Association, 355 Lexington Avenue, 15th Floor, New York, NY 10017.

ANSI/BHMA A156.1, *Butts and Hinges*, 2013 2016 .

ANSI/BHMA A156.2, *Bored and Preassembled Locks and Latches*, 2011 2017 .

ANSI/BHMA A156.4, *Door Controls — Closers*, 2013 2019 .

ANSI/BHMA A156.5, *Auxiliary Locks and Associated Products*, 2014 2020 .

ANSI/BHMA A156.12, *Interconnected Locks and Latches*, 2013 2018 .

ANSI/BHMA A156.13, *Mortise Locks and Latches Series 1000*, 2012 2017 .

ANSI/BHMA A156.16, *Auxiliary Hardware*, 2013 2018 .

ANSI/BHMA A156.17, *Self-Closing Hinges and Pivots*, 2014 2019 .

ANSI/BHMA A156.23, *Electromagnetic Locks*, 2010 2017 .

ANSI/BHMA A156.24, *Delayed Egress Locking Systems*, 2012 2018 .

ANSI/BHMA A156.25, *Electrified Locking Devices*, 2013 2018 .

ANSI/BHMA A156.26, *Continuous Hinges*, 2012 2017 .

ANSI/BHMA A156.28, *Recommended Practice for Keying Systems*, 2013 2018 .

ANSI/BHMA A156.30, *High Security Cylinders*, 2014 2020 .

ANSI/BHMA A156.31, *Electric Strikes and Frame Mounted Actuators*, 2013 2019 .

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed Apr 14 15:43:26 EDT 2021

Committee Statement

Committee Statement: The Technical Committee updates the document dates.

Response Message: FR-31-NFPA 731-2021

**First Revision No. 14-NFPA 731-2021 [Section No. H.1.2.6]**

Global FR-9

H.1.2.10 UL Publications.

Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

UL 294, ~~Standard for Access Control System Units~~, 2013, revised ~~2015~~2018.

UL 437, ~~Standard for Key Locks~~, 2013.

UL 606, ~~Standard for Linings and Screens for Use with Burglar-Alarm Systems~~, 1999, revised 2006.

UL 608, ~~Standard for Burglary Resistant Vault Doors and Modular Panels~~, 2004, revised 2012.

UL 634, ~~Standard for Connectors and Switches for Use with Burglar-Alarm Systems~~, 2007, revised ~~2015~~2020.

UL 636, ~~Standard for Holdup Alarm Units and Systems~~, 1996, revised 2013.

UL 639, ~~Standard for Intrusion-Detection Units~~, 2007, revised ~~2012~~2019.

UL 681, ~~Standard for Installation and Classification of Burglar and Holdup Alarm Systems~~, 2014.

UL 687, ~~Standard for Burglary-Resistant Safes~~, 2011.

UL 752, ~~Standard for Bullet-Resisting Equipment~~, 2005, revised 2013.

UL 768, ~~Standard for Combination Locks~~, 2006, revised ~~2013~~2018.

UL 827, ~~Standard for Central-Station Alarm Services~~, 2014, revised ~~2015~~2020.

UL 972, ~~Standard for Burglary Resisting Glazing Material~~, 2006, revised 2011.

UL 1034, ~~Standard for Burglary-Resistant Electric Locking Mechanisms~~, 2011, revised ~~2015~~2020.

UL 1037, ~~Antitheft Alarms and Devices~~, ~~1999~~2016, revised ~~2009~~2017.

UL 2058, ~~Outline of Investigation for High Security Electronic Locks~~, 2005.

UL 2610, ~~Commercial Premises Security Alarm Units and Systems~~, 2018, revised 2020.

UL 2900-2-3, ~~Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems~~, 2020.

UL 60950-1, ~~Standard for Information Technology Equipment — Safety — Part 1: General Requirements~~, 2007, revised ~~2013~~2019.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 12:48:44 EDT 2021

Committee Statement

Committee Statement: The Technical Committee updates the UL Standard editions and adds UL 2610 and UL 2900-2-3 which are added to the document.

Response FR-14-NFPA 731-2021

Message:

[Public Input No. 26-NFPA 731-2021 \[Section No. H.1.2.6\]](#)



First Revision No. 16-NFPA 731-2021 [Section No. H.2.2]

[Global FR-9](#)

H.2.2 UL Publications.

Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

UL 1076, ~~Standard for Proprietary Burglar Alarm Units and Systems~~, 1995, revised 2015.

UL 1610, ~~Standard for Central-Station Burglar-Alarm Units~~, 1998, revised 2015.

UL 1077, ~~Standard for General-Purpose Signaling Devices and Systems~~, 2008, revised 2011 2018.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue Apr 13 13:07:41 EDT 2021

Committee Statement

Committee Statement: The Technical Committee edits the date of the UL documents.

Response Message: FR-16-NFPA 731-2021

[Public Input No. 27-NFPA 731-2021 \[Section No. H.2.2\]](#)