



Second Revision No. 3-NFPA 731-2025 [Global Comment]

[NFPA 730 Extract updates to Annex G, see attached word document 731_F2025_NFPA_730_Extract_Updates_SR-3.docx]

Supplemental Information

<u>File Name</u>	<u>Description</u>	<u>Approved</u>
731_F2025_NFPA_730_Extract_Updates_SR-3.docx	731_F2025_NFPA_730_Extract_Updates_SR-3.docx	
731_Global_SR-3_For_Ballot.pdf		

Submitter Information Verification

Committee: PMM-AAA
Submittal Date: Thu May 08 09:55:49 EDT 2025

Committee Statement

Committee Statement: Extract updates in accordance with the NFPA Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document.
Response Message: SR-3-NFPA 731-2025

G.2.3.2 Fence-Mounted Sensors.

Fence-mounted sensors, in general, are intended for installation on chain-link fencing and are designed to detect either the presence of intruders as they approach or touch the fence or the mechanical vibrations caused by intruders climbing over, cutting through, or crawling under the fence. Since these devices are mounted directly to the fence, to reduce the potential for false alarms, it is important that the fence be installed according to ASTM F567, *Standard Practice for the Installation of Chain-Link Fence*. Fence signs should be securely mounted so that they do not rattle, and large bushes and tree limbs that grow along the fence line should be trimmed so that they do not rub against the fence. The primary advantage to the use of fence-mounted sensors is that installation is simplified, since the installer can follow the contour of the fence and the topography of the area. The major disadvantage to their use is that the intruder must come in contact with the fence to be detected. [730:E.2.3.2]

G.3.1.1

A door is a vulnerable point of the security of any building. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other physical weaknesses that would allow entry. A secure door is made of metal or solid wood. Steel doors produced to ANSI/SDI A250.8, *Recommended Specifications for Standard Steel Doors & Frames*, and tested to ANSI/SDI A250.4, *Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors, Frames, and Frame Anchors and Hardware Reinforcing*, and wood doors are tested for security. Door strength and reinforcement should be compatible with the locks used. [730:E.3.1.1]

G.3.4.2 Bullet-Resisting Glazing Materials.

UL 752, *Bullet-Resisting Equipment*, provides test criteria for glazing materials used to form bullet-resisting barriers that are designed to protect against robbery and holdups. The standard also includes test criteria for the devices and fixtures used in bullet-resisting enclosures. ASTM F1233, *Standard Test Method for Security Glazing Materials and Systems*, provides test criteria to evaluate the level of resistance of security glazing materials and systems to forced entry due to ballistic impact. [730:E.3.4.2]

Other types of composites use combinations of laminated glass, polycarbonate, and/or acrylic separated by an air gap. [730:E.3.4.2.1.1(D)]

G.3.5.2 Keys.

Keys and locks are often the first and only level of physical security control for many organizational assets. Consequently, key control or the lack of it can mean the difference between a relatively secure activity and extraordinary loss. Almost all organizations utilize some type of key access in everyday operations. Each day offers an opportunity for key mismanagement or unauthorized duplication, which can lead to mild annoyances, such as the replacement and cost for lost keys, or to more serious losses, such as theft or personal injury. A good key control system maintains a strict accountability for keys and limits both key duplication and distribution. Refer to ANSI/BHMA A156.28, *Recommended Practices for Mechanical Keying Systems*. Keys should comply with ANSI/BHMA A156.5, *Auxiliary Locks and Associated Products* *Cylinders and Input Devices for Locks* (section on cylinders), and ANSI/BHMA A156.30, *High Security Cylinders*, in the appropriate grade for the application. [730:E.3.5.2]

G.3.5.13 Mortise Locks.

These lock designs are typically used in institutional and high-rise residential applications. They can incorporate both a latch and a deadbolt in the same body. Mortise locks allow a deadbolt with latch in a path of egress because the latch and the deadbolt are retracted in a single motion. Mortise locks can be designed with a low-cost failure point, shear pin, spindle, and so forth, making their application attractive for locations that are apt to receive a lot of abuse. Mortise locks should meet ANSI/BHMA A156.13, *Mortise Locks & Latches and Latches Series 1000*, and UL 437, *Key Locks*, in the appropriate grade for the application. [730:E.3.5.13]

G.3.5.19 Deadbolts and Auxiliary Deadbolts.

These products provide an added degree of security due to their longer throw and positive deadlocking. Auxiliary deadbolts are used to protect perimeter doors where not prohibited by codes requiring single-motion egress and are also used on interior doors for forced-entry resistance. The use of auxiliary deadbolts is often prohibited in conjunction with another lock when in a path of egress, because that would require two separate motions and could be confusing to a person during an emergency. Double-cylinder auxiliary deadbolts provide a high level of security, particularly where there are glass panels in the vicinity of the lock, but local codes should be checked for allowable applications. Deadbolt exit locks and deadbolt exit devices provide a higher degree of resistance to forced entry and can be used on doors requiring single-motion egress. The only deadbolts permitted on fire-rated exit doors are those that are self-relocking. Mortise locksets that contain both a latch and a deadbolt can contain single-motion release for use on doors in the path of egress and fire-rated doors. Multipoint deadbolt locks are available in a wide variety of functions and types (surface-mounted, mortise, exit device) and provide the highest level of resistance to forced-entry attempts. Auxiliary deadbolts should comply with the deadbolt section of ANSI/BHMA A156.5, *Auxiliary Locks and Associated Products*, *Cylinders and Input Devices for Locks*, and the door locks section of UL 437, *Key Locks*, in the appropriate grade for the application. [730:E.3.5.19]

G.4.2.1

As a result of increased security awareness, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. The technology used in access control systems ranges from simple push-button locks to computerized access control systems integrated with video surveillance systems. Regardless of the technology used, all access control systems have one primary objective — to screen or identify people prior to allowing entry. Since identification is the foundation of all access control systems, they generally require that the user be in possession of a machine readable credential. Establishing a person's identity can be based on three methods: something known by a person (e.g., password), something possessed by a person (e.g., card or key), or something physically unique about the person (e.g., fingerprint). Electronic access control equipment should be listed to UL 294, *Access Control System Units*. [730:E.4.2.1]

G.4.2.3.2 Biometric Systems.

Establishing a person's identity can be based on three methods: something known by a person (a password), something possessed by a person (a card or key), and something physical about a person (a personal characteristic). Biometric access control devices, or personal characteristic verification locks, rely on the third method. Since duplication of individual physical characteristics is very rare, biometric devices, in theory, could offer the highest security possible. Biometric systems measure a unique characteristic of the person seeking access. These systems are classified as fingerprint, hand or palm geometry, handwriting, voice, and retinal verification systems. Typically, biometric readers are connected to a CPU but can also be used alone. The most readily available commercial systems for access control are fingerprint, palm, iris, and

facial systems. Additionally, legacy retina, handwriting, and voice systems may exist but have been deprecated and should not be considered for new access control purposes. [730:E.4.2.3.2]

G.4.2.3.2.1 Fingerprint Verification Systems.

Fingerprint verification systems ~~have been around for more than a decade. These systems~~ identify a person by matching stored fingerprints with live prints presented on an electro-optical scanner. [730:E.4.2.3.2.1]

G.4.2.3.2.5 Retinal Verification Systems.

Retinal verification systems use the pattern of blood vessels within the retina of the eye, which is unique in everyone, as a means of identifying a person. The user looks into an eyepiece that scans the retina with a safe low-level infrared light. The infrared light reflected back is converted into digital data that is compared to information stored in a computer. The limitation in retinal verification systems is that retinal patterns are not stable and can be altered by injury, illness, alcohol, or drugs. There also may be resistance on the part of a person to look into the device. Retinal scanners for access control have largely been deprecated and are no longer readily commercially available. [730:E.4.2.3.2.5]

G.4.2.3.2.6 Iris Verification Systems.

Iris verification systems use the unique pattern within the iris of the eye as a means of identifying a person. The user looks into an eyepiece that images the iris. The image is compared to information stored in a computer. [730:E.4.2.3.2.6]

G.4.3.1.2

A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected, such as a safe or a doorknob. When the image of an intruder or moving object enters the monitored window, the difference in contrast is detected and triggers an alarm. Such technology is largely deprecated and not applicable to contemporary installations. [730:E.4.3.1.2]

G.4.3.2.1 Equipment.

Video surveillance equipment should ~~provide appropriate resolution equal to or greater than the manufacturer's resolution specified in a marking on the equipment or in the literature packaged with the video equipment. Video surveillance equipment should be listed for its purpose and~~ comply with Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Year 2019, which prohibits the purchase of covered telecommunications equipment and services from vendors who sell products containing spyware. [730:E.4.3.2.1]

G.4.3.2.2.4

The signal can be recorded ~~by a video recorder for playback and analysis at a later time. Many recorders have a time-lapse mode for quick playback of lengthy periods of tape coverage. This system is often used in conjunction with a date-time generator that can project a continuous image of the date and time in the corner of the monitor screen. [730:E.4.3.2.2.4]~~



Second Revision No. 7-NFPA 731-2025 [Global Comment]

[New Chapter 12 Cybersecurity Provisions - see attached word document 731_F2025_New_Chapter 12_SR-7]

Supplemental Information

<u>File Name</u>	<u>Description</u>	<u>Approved</u>
731_F2025_New_Chapter_12_SR-7.docx	731_F2025_New_Chapter 12_SR-7	
731_F2025_New_Chapter_12_SR-7.docx	For prod use	
731_Global_SR-7_For_Ballot.pdf		

Submitter Information Verification

Committee: PMM-AAA
Submittal Date: Wed May 14 15:12:09 EDT 2025

Committee Statement

Committee Statement: This revision provides a new chapter on cybersecurity to provide clarity and guidance to the requirements for cybersecurity protection and is primarily extracted from NFPA 72. No minimum cybersecurity level is required for equipment that cannot be connected to via data ports of any kind. Where no connection is available cybersecurity is not required. The addition of requirements on remote software updates references UL 5500, which is specifically written to address remote software updates.

Response Message: SR-7-NFPA 731-2025

Public Comment No. 2-NFPA 731-2025 [Global Input]

Chapter 12 Cybersecurity Provisions

12.1 Application.

Where required by governing laws, codes, or standards, or other parts of this standard, cybersecurity shall be provided in accordance with Chapter 12 for equipment software, system support tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance. [72:11.1.1]

12.2 Security Levels for Non-Network Connectable Equipment.

No minimum cybersecurity level shall be required for systems that comply with the following conditions:

- (1) No network connectable equipment
- (2) No uploadable software configuration
- (3) *No data ports

A.12.2(3)

Examples of data ports include USB ports, Ethernet ports, HDMI ports, and serial ports.

12.3 Network Connectable Equipment Software Development and Production Environments.

Development and production environments used to develop and manufacture network connectable equipment shall employ cybersecurity safeguards that are consistent with one or more of the following:

- (1) NIST's "Framework for Improving Critical Infrastructure Cybersecurity"
- (2) ISO/IEC 27001, Information security management systems
- (3) IASME Consortium Cyber Essentials
- (4) Other equivalent standards acceptable to a nationally recognized testing laboratory
- (5) Other applicable laws and regulations

[72:11.2]

12.4 Security Levels for Network Connectable Equipment.

All interfaces used to communicate with network connectable equipment shall be protected in accordance with the following:

- (1) For non-internet-protocol wired interfaces, one of the following:
 - (a) Security Level 1 (SL1) in accordance with ANSI/ISA/IEC 62443-4-2, *Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components*
 - (b) Security Level 1 (SL1) in accordance with ANSI/ISA/IEC 62443-3-3, *Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements and Security Levels*

(c) Security Level 1 (SL1) in accordance with UL 2900-2-3, *Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems*

(d) Comparable level associated with Section 12.3(4)

(2) For non-internet-protocol wireless interfaces, or internet protocol wired and wireless interfaces that do not connect to publicly accessible networks, one of the following:

(a) Security Level 2 (SL2) in accordance with ANSI/ISA/IEC 62443-4-2

(b) Security Level 2 (SL2) in accordance with ANSI/ISA/IEC 62443-3-3

(c) Security Level 2 (SL2) in accordance with CAN/UL 2900-2-3

(d) Comparable level associated with Section 12.3(4)

(3) For internet protocol wired or wireless interfaces that connect to publicly accessible networks, one of the following:

(a) Security Level 3 (SL3) in accordance with ANSI/ISA/IEC 62443-4-2

(b) Security Level 3 (SL3) in accordance with ANSI/ISA/IEC 62443-3-3

(c) Security Level 3 (SL3) in accordance with CAN/UL 2900-2-3

(d) Comparable level associated with Section 12.3(4)

[72:11.3]

12.5 Interconnecting Conductors, Cables, or Other Physical Pathways.

Interconnecting conductors, cables, or other physical pathways for use in Security Level 2 or higher applications in locations accessible to the public shall be protected by metal raceways or metal armored cables. [72:11.4]

12.6 Unused Physical Data Ports.

All unused physical data ports shall be protected in at least one of the following ways:

(1) Physically protected from unauthorized access

(2) Administratively disabled

(3) Configured to require a token-based authentication, certificate-based authentication, password, or other method that is consistent with the security requirements of the system

[72:11.6]

12.7 Data Connections to External Networks.

When any data connection is made from the system to an external network, the connection shall be protected by a gateway or firewall that ensures that only trusted traffic is allowed to pass.
[72:11.7]

12.8 Network Connectable Equipment Cybersecurity Software Updates.

12.8.1 Remote Software Updates.

Remote software updates to equipment and systems that have a potential influence on safety and on compliance with the particular system and equipment safety standard shall be performed in accordance with UL 5500, *Remote Software Updates*.

12.8.2

At least quarterly, the equipment manufacturer(s) shall do the following until the equipment is no longer supported by the manufacturer:

- (1) Evaluate all relevant cybersecurity threats
- (2) Determine if a software update is required to maintain the cybersecurity level achieved in compliance with Section 12.4

[72:11.8.1]

12.8.3

The system installer shall provide the name and contact information of the system owner or their representative to the equipment manufacturer(s) at the time of system acceptance testing.

[72:11.8.2]

12.8.4

The equipment manufacturer(s) shall notify the system owner or their representative of all required software security updates required to maintain the cybersecurity level achieved in compliance with Sections 12.2, 12.3, and 12.4. [72:11.8.3]

12.8.5

Software for network connectable devices shall be maintained by installing software security updates as required by the equipment manufacturer(s) to maintain the cybersecurity level achieved in compliance with Sections 12.2, 12.3, and 12.4. [72:11.8.4]

12.8.6

Software security updates that are deemed necessary by the equipment manufacturer(s) for compliance with Section 12.3 shall be installed at least annually. [72:11.8.5]

12.8.7

Cybersecurity software updates applied to gateways or firewalls that do not affect the system site-specific or system executive software shall not be required to comply with 4.10.5.

[72:11.8.6]

12.8.8

Cybersecurity software updates to systems or system components shall be permitted to be made by remote access in compliance with Section 12.4. [72:11.8.7]

12.9 Notification of Termination of Cybersecurity Update Support.

The manufacturer shall notify the system owner or their representative of the termination of cybersecurity software update support required by Section 12.8 for any element of the system. [72:11.9]

12.10 Cybersecurity for System Support Tools.

A system support tool and the support tool interfaces shall comply with the requirements of Sections 12.2 through 12.9. [72:11.10]

12.11 Evidence of Compliance.

12.11.1

Evidence of cybersecurity compliance shall include one or more of the following:

- (1) Certification of compliance by a nationally recognized testing laboratory
- (2) Manufacturer certification for the specific type and brand of system provided by the manufacturer
- (3) An assessment or certification program acceptable to the authority having jurisdiction

[72:11.11.1]

12.11.2

The validity of cybersecurity certificates shall be verified annually by the person testing the system. [72:11.11.2]

12.11.3

The validity of the equipment manufacturer's contact information for the system owner shall be verified annually by the person testing the system. [72:11.11.3]

12.12 Documentation.

The standards used and security levels employed in complying with Chapter 12 shall be identified in the system documentation required by 4.12.2. [72:11.12]



Second Revision No. 1-NFPA 731-2025 [Section No. 2.3]

2.3 Other Publications.

2.3.1 ANSI Publications.

American National Standards Institute, Inc., ~~25 West 43rd Street, 4th Floor, 1180 6th Avenue, 10th floor,~~ New York, NY 10036.

~~ANSI/ASA/ANSI S1.4-2014/Part 3/IEC 61672-3:2013 (R2024),~~ *Electroacoustics — Sound Level Meters — Part 3: Periodic Tests*, ~~2022 2014, reaffirmed 2024~~.

~~ANSI/TIA 568.3-E~~, *Optical Fiber Cabling and Components Standard*, ~~2024 2022~~.

2.3.2 ISA Publications.

International Society of Automation, ~~67 T. W. Alexander Drive,~~ P.O. Box 12277, Research Triangle Park, NC 27709.

~~ANSI/ISA/IEC 62443-3-3,~~ *Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements and Security Levels*, 2013.

~~ANSI/ISA/IEC 62443-4-2,~~ *Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components*, 2018.

2.3.3 ISO Publications.

~~International Organization for Standardization, ISO Central Secretariat, BIBC II, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland.~~

~~ISO/IEC 27001,~~ *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements*, 2022.

2.3.4 NIST Publications.

~~National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-1070.~~

~~“Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, 2018.~~

2.3.5 SIA Publications.

Security Industry Association, 8405 Colesville Road, Suite 500, Silver Spring, MD 20910.

~~ANSI/SIA CP-01,~~ *Control Panel Standard — Features for False Alarm Reduction*, 2019.

~~ANSI/SIA PIR-01,~~ *Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity*, 2000.

2.3.6 UL Publications.

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

UL 50, *Enclosures for Electrical Equipment, Non-Environmental Considerations*, 2024.

UL 50E, *Enclosures for Electrical Equipment, Environmental Considerations*, 2020.

UL 294, *Access Control System Units*, 2023, revised 2024.

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

UL 634, *Connectors and Switches for Use with Burglar-Alarm Systems*, 2007, revised ~~2022~~ 2020.

UL 636, *Holdup Alarm Units and Systems*, 2018.

UL 639, *Intrusion-Detection Units*, 2007, revised ~~2019~~ 2024.

UL 827, *Central-Station Alarm Services*, 2022, revised 2023.

~~UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, 2011, revised 2020~~

UL 1076, *Proprietary Burglar Alarm Units and Systems*, 2018, revised 2021.

UL 2044, *Commercial Closed-Circuit Television Equipment*, 2019, revised 2024.

UL 2610, *Commercial Premises Security Alarm Units and Systems*, 2021, revised 2023.

UL 2802, *Performance Testing of Camera Image Quality*, 2013, 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, revised 2023.

UL 5500, *Remote Software Updates*, 2023.

UL 60065, *Audio, Video and Similar Electronic Apparatus*, 2015, revised 2020.

UL 60950-1, *Information Technology Equipment – Safety – Part 1: General Requirements*, 2007, revised 2019.

UL 60950-22, *Information Technology Equipment — Part 22: Equipment to Be Installed Outdoors*, 2017, revised 2022.

UL 62368, *Audio/Video, Information and Communication Technology Equipment*, 2019, revised 2021.

2.3.7 US Government Publications.

US Government Publishing Office, 732 North Capitol Street, NW, Washington, DC 20401.

ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).

Title 47, Code of Federal Regulations, Part 15, "Radio Frequency Devices."

2.3.8 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2020.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 08 08:30:46 EDT 2025

Committee Statement

Committee Statement: References updated in accordance with the NFPA Reference Policy.

Response Message: SR-1-NFPA 731-2025



Second Revision No. 9-NFPA 731-2025 [Section No. 2.4]

2.4 References for Extracts in Mandatory Sections.

NFPA 72[®], *National Fire Alarm and Signaling Code*[®], 2025 edition.

NFPA 730, *Guide for Premises Security*, 2026 edition.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed May 14 16:19:13 EDT 2025

Committee Statement

Committee Statement: Updates the extracted documents in accordance with the NFPA Extract Policy.
Adds NFPA 730 due to new definition extract.

Response Message: SR-9-NFPA 731-2025



Second Revision No. 6-NFPA 731-2025 [New Section after 3.3.23]

3.3.24* Security Vulnerability Assessment (SVA).

A systematic and methodical process for examining ways an adversary might exploit an organization's security vulnerabilities to produce an undesired outcome. [730, 2026]

A.3.3.24 Security Vulnerability Assessment (SVA).

A security vulnerability assessment (SVA) includes a risk assessment and threat assessment as well as other components that may be added to do a complete assessment of the vulnerabilities. The results of the SVA are used in developing countermeasures to address adversarial events. [730, 2026]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed May 14 10:47:30 EDT 2025

Committee Statement

Committee Statement: This revision extracts the definition of security vulnerability assessment (SVA) from NFPA 730 as it is used in NFPA 731 and is not currently defined.

Response Message: SR-6-NFPA 731-2025



Second Revision No. 4-NFPA 731-2025 [Section No. 3.3.25.3]

3.3.26.3* 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, 2025]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 08 10:06:05 EDT 2025

Committee Statement

Committee Statement: Extract updates in accordance with the NFPA Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document.

Response Message: SR-4-NFPA 731-2025



Second Revision No. 5-NFPA 731-2025 [Section No. 4.10.5]

4.10.5

Where required by the AHJ or SVA, ~~premises security equipment that is network connected shall be in compliance with one of the following standards: shall comply with the cybersecurity requirements of Chapter 12.~~

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

~~ANSI/ISA/IEC 62443-4-2, Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components~~

~~ANSI/ISA/IEC 62443-3-3, Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements and Security Levels~~

~~Other cybersecurity standards acceptable to the AHJ or SVA~~

Supplemental Information

<u>File Name</u>	<u>Description</u>	<u>Approved</u>
731_SR-5_4.10.5.docx		

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed May 14 10:41:12 EDT 2025

Committee Statement

Committee Statement: This revision points the user to the new Chapter 12 on Cybersecurity.

Response Message: SR-5-NFPA 731-2025

Public Comment No. 1-NFPA 731-2025 [Section No. 4.10.5]



Second Revision No. 8-NFPA 731-2025 [Section No. 6.1.1]

6.1.1* Equipment.

A.6.1.1

A critical part of an access or egress control system is the lock hardware that holds a door closed and opens or releases when initiated. Like many components of an integrated system, the locking mechanism can have various forms and functionalities, depending on the particular applications.

NFPA 101 includes requirements for a means of egress system to be provided that includes a continuous and unobstructed path of egress travel from any occupied point in a building, structure, or facility to a public way. However, there are specific situations in which these model codes allow access control equipment that limits the immediate and unobstructed egress travel under strict provisions.

Some factors in applicable fire and life safety codes that should be considered for the installation of electronic access control equipment include the following :

- (1) Integration with fire detection, fire suppression, or other life safety systems that release locked doors upon their activation, allowing immediate emergency egress
- (2) Fail safe features to release locks in the event of a loss of power
- (3) Fail secure features that intentionally maintain locked positions
- (4) Emergency planning and preparedness with staff training and required drills
- (5) Limitations on the delay time for delayed-egress doors
- (6) Special signage requirements
- (7) Security and resistance to unauthorized entry

Locks and locking systems can be tested for compliance with different end-product standards. Each end-product standard defines the scope of the application and includes construction and test compliance criteria for evaluation and certification.

Typical end uses for the locks and locking systems include integration into access control systems, fire-rated door assemblies, special locking arrangements, panic hardware, controlled exit panic devices, and burglary-resistant electric locks. Locks and locking systems used in these applications can take different forms depending on the design of a product or system. Some of these devices are purely mechanical and others may can include electronics to control or provide delayed release or audible alarm functions. Certified locks are investigated for safety from electric shock and mechanical hazards. Depending on the product type, they could also be tested for burglary resistance and/or fire resistance.

An end user or AHJ can see various configurations of equipment incorporated into a system. The equipment may can have different forms to suit a specific application. A very common scenario is the use of UL 294, *Access Control System Units*, certified access control systems units controlling locks certified to UL 1034, *Burglary-Resistant Electric Locking Mechanisms*.

Other prevalent applications include special locking arrangements that have dedicated system component equipment and certified locks connected to control a request to exit (REX) system. For this application, the REX system certification is specific to the system components submitted for investigation.

The various permutations of locking hardware and systems applications (see *Table A.6.1.1*) allows for the use of the devices in accordance with model building and life safety codes, with the common element of safety by design.

~~The table below summarizes the applicable standards for various locking devices and systems that are typically used on means of egress or controlled access areas.~~

Table A.6.1.1(a) Example Applicable Standard for Various Locking Devices and Systems

Standard	Category Title	Helpful Notes	Typical Door Hardware/Lock Form Factor
UL 294, <i>Access Control System Units</i>	Access control system units	Sec. 34.2 applies to single-point locking devices	Autonomous access control lock

Standard	Category Title	Helpful Notes	Typical Door Hardware/ Lock Form Factor
UL 294, <i>Access Control System Units</i>	Special locking arrangements	UL 294, Sec. 68 applies to controlled and delayed egress equipment and systems operation	Require to exit (REX) devices / systems and controlled or delayed egress locks
UL 1034, <i>Burglary-Resistant Electric Locking Mechanisms</i>	Burglary-resistant electric locking mechanisms	Performance based for static force, dynamic force, and endurance test factors	Electromagnetic locks, electric dead bolts, electric door strikes, electrically operated door locking mechanisms
UL 305, <i>Panic Hardware</i>	Panic or fire exit hardware	Generally mechanical devices only (no electronics)	Panic hardware, fire exit hardware
UL 294 and UL 305	Controlled exit panic devices	UL 294 and UL 305 apply	Electromechanical locking/latching mechanisms
UL 634, <i>Connectors and Switches for Use with Burglar Alarm Systems</i>	Connectors and switches for use in burglar alarm systems	Includes electric power transfers, door loops, and door position switches	Electric hinge and flexible connectors intended for burglar alarm applications
UL 10C, <i>Positive Pressure Fire Tests of Door Assemblies</i>	Positive pressure fire test of door assemblies	Also, UL 305 for card readers and components for use with locks sold separately	Electric cylindrical locks and mortise locks; electrically controlled single-point locks or latches; electromagnetic locks; fire exit hardware; electrified hinge; electric strikes; miscellaneous fire door accessories; positive pressure tested; accessories for use with single-point locks and latches and fire exit hardware

Maintaining Free Egress and Building Security.

Building safety and security is a balancing act when it comes to allowing free egress and securing a building. In most cases, national codes require free and unobstructed egress be achieved.

Locking configurations used for egress include the following four basic types:

- (1) Egress motion sensors equipment or systems
- (2) Delayed egress hardware
- (3) Push to exit hardware
- (4) Request to exit hardware and systems

Building, fire, and life safety codes prescribe a few elements that are common for achieving free egress. Some of these general elements are as follows:

- (1) Doors must be able to be opened readily from the occupant side to achieve egress.
- (2) Locking devices must not require the use of tools, special knowledge, or keys to operate from the egress side.
- (3) Hardware and fastening devices must be releasable without the use of special knowledge of operation.

- (4) Releasing devices must release the door leaf with no more than one motion.

Considerations for a Means of Egress System.

NFPA 101 includes requirements for a means of egress system to be provided, including a continuous and unobstructed path of egress travel from any occupied point in a building, structure, or facility to a public way. However, there are specific situations where locking arrangements that limit the immediate and unobstructed egress travel under strict provisions are permitted. Table A.6.1.1 provides a summary of these applications and identifies typical locking products and applicable BHMA and UL standards to certify products for egress or access control that allow for code-compliant installation and application.

Other factors that must also be considered for installation and in accordance with applicable codes include the following:

- (1) Integration with fire detection and suppression or other life safety systems that release locked doors upon their activation, allowing immediate emergency egress
- (2) Fail safe features to release locks in the event of a loss of power
- (3) Fail secure features that intentionally maintain locked positions
- (4) Emergency planning and preparedness with staff training and required drills
- (5) Limitations on the delay time for delayed-egress doors
- (6) Special signage requirements
- (7) Security and resistance to unauthorized entry

Categories for Certified Locks and Locking Systems.

Typical end uses for the locks and locking systems include integration into access control systems, fire-rated door assemblies, special locking arrangements, panic hardware, controlled exit panic devices, and burglary resistant electric locks. Locks and locking systems used in these applications can take different forms depending on the design of the product or system. Some of these devices are purely mechanical while others can include electronic circuits to control or provide delayed release or audible alarm functions. Certified locks are investigated for safety from electric shock and mechanical hazards and, depending on the product type, can also be tested for burglary resistance and/or fire resistance.

Table A.6.1.1 summarizes product types and the applicable standards for various locking devices and systems that are typically used on means of egress or controlled areas to comply with requirements in 6.1.1.1 and 6.1.1.2.

Table A.6.1.1 Example Applicable Standard for Various Locking Devices and Systems

<u>Category Title</u>	<u>UL Standard</u>	<u>Associated BHMA Standards</u>	<u>Helpful Notes</u>
<u>Access control system units</u>	<u>UL 294, Access Control System Units</u>	<u>ANSI/BHMA A156.2, Bored and Preassembled Locks and Latches</u> <u>ANSI/BHMA A156.3, Exit Devices</u> <u>ANSI/BHMA A156.13, Mortise Locks & Latches</u> <u>ANSI/BHMA A156.35, Power Supplies for Electronic Access Control</u>	<u>Access control systems can include a single point, multipoint, and mortise type locks.</u>

<u>Category Title</u>	<u>UL Standard</u>	<u>Associated BHMA Standards</u>	<u>Helpful Notes</u>
		ANSI/BHMA A156.37, Multipoint Locks	
Special locking arrangements	UL 294, Access Control System Units	ANSI/BHMA A156.24, Delayed Egress Locking Systems ANSI/BHMA A156.35, Power Supplies for Electronic Access Control	Special locking arrangements include delayed egress locking systems, where permitted.
Burglary resistant electric locking mechanisms	UL 1034, Burglary-Resistant Electric Locking Mechanisms	ANSI/BHMA A156.23, Electromagnetic Locks ANSI/BHMA A156.25, Electrified Locking Devices ANSI/BHMA A156.31, Electric Strikes and Frame Mounted Actuators	Burglary-resistant electric locking mechanisms can include burglary-resistant (BR) electromagnetic locks, BR electric dead bolts, BR electric door strikes, and BR electrically operated door locking mechanisms.
Panic or fire exit hardware	UL 305, Panic Hardware	ANSI/BHMA A156.3, Exit Devices	These are generally mechanical devices.
Controlled exit panic devices	UL 294, Access Control System Units , and UL 305, Panic Hardware	ANSI/BHMA A156.3, Exit Devices ANSI/BHMA A156.35, Power Supplies for Electronic Access Control	For controlled exit panic devices both UL 294 and UL 305 apply because these contain elements of access control systems and panic hardware. This includes electromechanical locking/latching mechanisms.
Connectors and switches for use in burglar alarm systems	UL 634, Connectors and Switches for Use with Burglar-Alarm Systems	ANSI/BHMA A156.1, Butts and Hinges ANSI/BHMA A156.26, Continuous Hinges	This includes electric power transfers, door loops, and door position switches. Electric hinge and flexible connectors are intended for burglar alarm systems.
Positive pressure fire test of door assemblies	UL 10C, Positive Pressure Fire Tests of Door Assemblies	All builders hardware items that are required to be listed are subject to the requirements of UL 10C.	Also, use UL 305 for GXHX. Card readers and components for use with locks sold separately and listed under GWVW.

<u>Category Title</u>	<u>UL Standard</u>	<u>Associated BHMA Standards</u>	<u>Helpful Notes</u>
			This includes <u>electric cylindrical locks and mortise locks (electrically controlled single-point locks or latches GYQS)</u> , <u>electromagnetic locks (GWXT)</u> , <u>fire exit hardware (GXHX)</u> , <u>electrified hinges (GWZQ)</u> , <u>electric strikes (GXAY)</u> , <u>miscellaneous fire door accessories, positive pressure tested (GVUY), and accessories that are for use with single-point locks and latches and fire exit hardware (GWVW)</u> .
<u>Power supplies</u>	<u>Various end product standards such as UL 294, <i>Access Control System Units</i>, UL 2610, <i>Commercial Premises Security Alarm Units and Systems</i>, and UL 864, <i>Control Units and Accessories for Fire Alarm Systems</i>.</u>	<u>ANSI/BHMA A156.35, <i>Power Supplies for Electronic Access Control</i></u>	

6.1.1.1

Electronic access control equipment shall ~~comply with UL 294, *Access Control System Units*~~ be listed for the intended purpose .

6.1.1.2

Electric locking equipment shall ~~comply with UL 1034, *Burglary-Resistant Electric Locking Mechanisms*~~ be listed for the intended purpose .

Supplemental Information

<u>File Name</u>	<u>Description</u>	<u>Approved</u>
731_Chapter_6_6.1.1_SR-8.docx	731_Chapter_6_6.1.1_SR-8.docx	
731_Chapter_6_6.1.1_SR-8.docx	For prod use	

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Wed May 14 15:35:31 EDT 2025

Committee Statement

Committee Statement: This revision clarifies that electronic access control equipment and electric locking equipment must be listed for the intended purpose. The annex was updated to include guidance to the user on possible listing standards for this equipment. The annex table was revised to provide the user with more detailed examples of applicable standards for this equipment. The annex is also updated to include information to ensure that when access control is provided the egress requirements are also considered such as when controlled access is provided on egress doors.

Response Message: SR-8-NFPA 731-2025



Second Revision No. 2-NFPA 731-2025 [Sections H.1, H.2]

H.1 Referenced Publications.

The documents or portions thereof listed in this annex are referenced within the informational sections of this standard and are not part of the requirements of this document unless also listed in Chapter 2 for other reasons.

H.1.1 NFPA Publications.

National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 1, *Fire Code*, 2024 edition.

NFPA 70[®], *National Electrical Code*[®], 2026 edition.

NFPA 72[®], *National Fire Alarm and Signaling Code*[®], 2025 edition.

NFPA 80, *Standard for Fire Doors and Other Opening Protectives*, 2025 edition.

NFPA 101[®], *Life Safety Code*[®], 2024 edition.

NFPA 730, *Guide for Premises Security*, 2026 edition.

NFPA 5000[®], *Building Construction and Safety Code*[®], 2024 edition.

H.1.2 Other Publications.

H.1.2.1 ASTM Publications.

ASTM International, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959.

ASTM F567, *Standard Practice for the Installation of Chain-Link Fence*, 2023.

ASTM F1090-45, *Standard Classification for Bank and Mercantile Vault Construction*, 2016 2024.

ASTM F1233-24, *Standard Test Method for Security Glazing Materials and Systems*, 2021.

ASTM F1247-89(2018), *Standard Specification for Intrusion Resistant Generic Vault Structures*, 1989, revised 2018.

H.1.2.2 BHMA Publications.

Builders Hardware Manufacturers Association, ~~355 Lexington Avenue, 15th Floor, New York, NY 10017~~ 529 14th Street, NW, Suite 1280, Washington, DC 20045 .

ANSI/BHMA A156.1, *Butts and Hinges*, 2021.

ANSI/BHMA A156.2, *Bored and Preassembled Locks and Latches*, 2022.

ANSI/BHMA A156.3, *Exit Devices* , 2025

ANSI/BHMA A156.4, *Door Control — Closers and Pivots* , ~~2019~~ 2024 .

ANSI/BHMA A156.5, *Cylinders and Input Devices for Locks*, 2020.

ANSI/BHMA A156.12, *Interconnected Locks*, 2022.

ANSI/BHMA A156.13, *Mortise Locks & Latches* , 2022.

ANSI/BHMA A156.16, *Auxiliary Hardware*, 2023.

ANSI/BHMA A156.17, *Self-Closing Hinges and & Pivots*, ~~2019~~ 2025 .

ANSI/BHMA A156.23, *Electromagnetic Locks*, ~~2017~~ 2022 .

ANSI/BHMA A156.24, *Delayed Egress Locking Systems* , 2022.

ANSI/BHMA A156.25, *Electrified Locking Devices*, 2023.

ANSI/BHMA A156.26, *Continuous Hinges*, 2021.

ANSI/BHMA A156.28, ~~Master~~ *Recommended Practices for Mechanical Keying Systems*, 2023.

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

ANSI/BHMA A156.31, *Electric Strikes and Frame Mounted Actuators*, ~~2019~~ 2024 .

ANSI/BHMA A156.35, *Power Supplies for Electronic Access Control* , 2020.

ANSI/BHMA A156.37, *Multipoint Locks* , 2020.

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.

US General Services Administration, 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, BIBC II, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland. iso.org/home.html

ISO/IEC 27001, *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements*, 2022.

ISO/IEC 27002, *Information security, cybersecurity, and privacy protection — Information security controls*, 2022.

H.1.2.7 NIST Publications.

National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899.
nist.gov/itl

Federal Information Processing Standards (FIPS) 140-3, *Security Requirements for Cryptographic Modules*, March 2019.

H.1.2.8 SDI Publications.

Steel Door Institute, ~~managed by Wherry Associates~~, 30200 Detroit Road,
 Cleveland ~~Westlake~~, OH 44145-1967.

ANSI/SDI A250.4, *Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors, Frames, and Frame Anchors*, ~~2022~~ 2024.

ANSI/SDI A250.8, *Specifications for Standard Steel Doors & Frames*, ~~2017~~ 2023.

H.1.2.9 SIA Publications.

Security Industry Association, 8405 Colesville Road, Suite 500, Silver Spring, MD 20910.

ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, 2019.

H.1.2.10 UL Publications.

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

UL 10C, *Positive Pressure Fire Tests of Door Assemblies*, 2016, revised 2021.

UL 294, *Access Control System Units*, 2023.

UL 305, *Panic Hardware*, 2012, revised 2022.

UL 437, *Key Locks*, 2013, revised 2023.

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

UL 608, *Burglary Resistant Vault Doors and Modular Panels*, 2004, revised 2022.

UL 634, *Connectors and Switches for Use with Burglar-Alarm Systems*, 2007, revised ~~2022~~ 2020.

UL 636, *Holdup Alarm Units and Systems*, 2018.

UL 639, *Intrusion-Detection Units*, 2007, revised ~~2019~~ 2024.

UL 681, *Installation and Classification of Burglar and Holdup Alarm Systems*, 2014, revised 2021.

UL 687, *Burglary-Resistant Safes*, 2011, revised 2020.

UL 752, *Bullet-Resisting Equipment*, 2023.

UL 768, *Combination Locks*, 2006, revised 2023.

UL 827, *Central-Station Alarm Services*, 2022, revised 2023.

UL 864, *Control Units and Accessories for Fire Alarm Systems*, 2023, revised 2024.

UL 972, *Burglary Resisting Glazing Material*, 2011, revised 2020.

UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, 2011, revised 2020.

UL 1037, *Antitheft Alarms and Devices*, 2016, revised 2023.

UL 2058, *Outline of Investigation for High Security Electronic Locks*, 2005, ~~revised 2013~~.

UL 2610, *Commercial Premises Security Alarm Units and Systems*, 2021, revised 2023.

UL 2900-2-3, *Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems*, 2020, revised 2023.

UL 60950-1, *Information Technology Equipment — Safety — Part 1: General Requirements*, 2007, revised 2019.

H.1.2.11 US Government Publications.

US Government Publishing Office, 732 North Capitol Street, NW, Washington, DC 20401.

Americans with Disabilities Act, 42 U.S.C. § 12101 , 1990.

Title 12, Code of Federal Regulations, Part 326, "Minimum Security Devices and Procedures and Bank Secrecy Act Compliance."

Title 47, Code of Federal Regulations, Part 15, "Radio Frequency Devices."

S/N 0-635-034/1069. "Physical Security." US Army Field Manual 19-30, March 1979.

H.2 Informational References.

The following documents or portions thereof are listed here as informational resources only. They are not a part of the requirements of this document.

H.2.1 SIA Publications.

Security Industry Association, 8405 Colesville Road, Suite 500, Silver Spring, MD 20910.

PASS Safety and Security Guidelines for K-12 Schools, 2023. <https://passk12.org/guidelines-resources/pass-school-security-guidelines>

H.2.2 UL Publications.

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

UL 1610, *Central-Station Burglar-Alarm Units*, 2016, revised 2021.

UL 2017, *General-Purpose Signaling Devices and Systems*, 2008, revised 2024.

Submitter Information Verification

Committee: PMM-AAA

Submission Date: Thu May 08 08:44:21 EDT 2025

Committee Statement

Committee Statement: Reference updates in accordance with the NFPA Reference Policy.

Response Message: SR-2-NFPA 731-2025