

Educational Session

Merton Bunker, PE
Coffman Engineers

Automatic Fire Alarm Association

1

Disclaimer

Any of the proposed changes identified herein are subject to change at the NFPA Tech Session on June 20, 2024.

Not all changes made during the revision cycle are shown in this presentation.

Any opinions expressed by the presenter is solely his own and do not reflect the position of any other party.

This presentation should not be used as a substitute for professional consultation.

Automatic Fire Alarm Association

2

Thanks to Staff, TC Members, and TC Chairs

Staff: Patrick Bakaj
SIG-FUN: David Lowrey (Chapters 7 and 10)
SIG-PRO: Jack Poole (Chapters 12, 21 and 23)
SIG-TMS: David Kerr (Chapter 14)
SIG-IDS: L. J. Dallaire (Chapter 17)
SIG-NAS: Drew Poole (Chapter 18)
SIG-ECS: Bill Koffel (Chapter 24)
SIG-SSS: Dan O'Connnor (Chapter 26)
SIG-PRS: Leo Martin (Chapter 27)
SIG-HOU: Cory Ogle (Chapter 29)

Automatic Fire Alarm Association

3

3

The Annual 2025 Revision Process

- ✓ Technical Committee First Draft Meetings: July 2022, Indianapolis
- ✓ Correlating Committee First Draft Meetings: January 2023, Orlando
- ✓ Technical Committee Second Draft Meetings: July 2023, Kansas City/Virtual
- ✓ Correlating Committee Second Draft Meetings: December 2023 Virtual
- ✓ NITMAM Closing Date: March 27, 2024
- ✓ NITMAM Posting: May 8, 2024
- ✓ NFPA Annual Meeting Adoption: June 2024, Orlando
- ✓ Standards Council Approval: August 2024
- ✓ Issue: September 2024



Automatic Fire Alarm Association

4

Manual Of Style Changes

Many changes in this cycle were made to comply with the NFPA Manual Of Style.

- Eliminated exceptions.
- Cleaned up sections with multiple requirements.

Eliminated some requirements for obsolete technology.

Automatic Fire Alarm Association

5

Chapter 2

Referenced Publications — NFPA 1225, *Standard for Emergency Services Communications,* 2022 edition.

FR 5205

Automatic Fire Alarm Association

6

Chapter 3

Definitions

3.3.293.3 Cybersecurity Software.

Software that is included in a system element and arranged such that its inclusion or exclusion in no way affects the executive or site-specific software execution and whose purpose is to reduce the vulnerability of the system and/or equipment to cybersecurity attacks. (SIG-FUN)

FR 5363 and SCR4

Automatic Fire Alarm Association

7

Chapter 3

Definitions

3.3.303 Subsidiary Stations or Intermediary Service Provider.

A means of signal transport and processing between a protected premise and a public safety answering point (PSAP) that is owned, operated, and maintained by a private for-profit entity. (SIG-SSS)

FR 5116

Automatic Fire Alarm Association

8

Chapter 3

Definitions

3.3.328* Unconditioned Area. An enclosed area, room, or space without climate or HVAC controls. (SIG-IDS)

A.3.3.328 Unconditioned Area. Unconditioned areas are different from outdoor installations that are exposed to outside weather and environmental conditions. Examples of unconditioned areas include warehouses, attics, garages, and storage areas without HVAC systems.

FR 5267

Automatic Fire Alarm Association

9

Chapter 7

Documentation

7.3.4.7 Design documentation for restricted audible mode operation (RAMO) notification, including the definition of the protected space, sound pressure levels, and staff requirements, shall comply with 18.4.8.

SCR 5

Automatic Fire Alarm Association

10

Chapter 10

Fundamentals

10.5.7 Gateway Reporting System Personnel Qualification. (SIG-SSS)

10.5.7.1 Gateway Personnel. Gateway personnel shall be qualified in the service, inspection, maintenance, and testing of gateway alarm reporting systems.

10.5.7.2 Qualification.

10.5.7.2.1 Personnel shall demonstrate qualification by being trained and certified in gateway alarm reporting system design, installation, or service (as appropriate).

FR 5102

Automatic Fire Alarm Association

11

Chapter 10

Fundamentals

10.5.7.2.2 Personnel who are trained and certified for the specific type of subsidiary station or intermediary services provider system and comply with one the following shall be considered qualified:

(1) Personnel who are licensed or certified by a state or local authority, if applicable.

(2) Personnel who are certified by a nationally recognized certification organization acceptable to the authority having jurisdiction.

(3) Personnel who are employed and qualified by an organization listed by a nationally recognized testing laboratory for the design, installation, or servicing of systems within the scope of this chapter.

(4) Personnel who are employed and certified by an equipment manufacturer for the specific type of system.

FR 5102

Automatic Fire Alarm Association

12

Chapter 11

Cybersecurity

11.1.2* No minimum cybersecurity level shall be required for systems that meet both of the following conditions:

(1) No network connectable equipment.

(2) No uploadable software configuration.

A.11.1.2 An example of a system that requires no cybersecurity is a dip-switch configurable control unit with no network connection.

FR 5188

Automatic Fire Alarm Association

14

Chapter 11

Cybersecurity

11.2* 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 ~~standards~~:

(1) NIST's ~~Cybersecurity~~ "Framework for Improving Critical Infrastructure Cybersecurity"

(2) ISO/IEC 27001,*Information ~~Security Management~~ security management systems*

(3) IASME Consortium Cyber Essentials

(4) Other equivalent standards acceptable to a ~~Nationally Recognized Testing Laboratory~~ nationally recognized testing laboratory

(5)* Other applicable laws and regulations

Automatic Fire Alarm Association

15

Chapter 11

Cybersecurity

11.3* Security Levels for Network Connectable Equipment.

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

FR 5188 and SR 5079

Automatic Fire Alarm Association

17

Chapter 11

Cybersecurity

(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 CAN/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 11.2(4)

FR 5188 and SR 5079

Automatic Fire Alarm Association

18

Chapter 11

Cybersecurity

(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~~/3-3~~

(b) Security Level 2 (SL2) in accordance with ANSI/ISA/IEC 62443-~~4-2/~~3-3

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

(d) Comparable level associated with Section 11.2(4)

FR 5188 and SR 5079

Automatic Fire Alarm Association

19

Chapter 11

Cybersecurity

(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 11.2(4)

FR 5188 and SCR 23

Automatic Fire Alarm Association

20

Chapter 11

Cybersecurity

11.4* 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.

A.11.4 An assumption is often made that attacks are launched remotely from the internet. However, there are many examples of attackers gaining access to a facility to enable an attack. For example, a system that has no networking capability, with only a RS-232 serial port can be connected to an RS-232-to-Ethernet adapter. This could be intended benignly, as a way of enabling remote monitoring or remote service, but it is a risk that should be considered nonetheless.

The protection by metal raceways or metal armored cables of interconnecting conductors, cables, or other physical pathways is also recommended for use in Security Level 1 applications. For improved physical security in systems where control units and data access points are not installed in restricted areas, using security tamper switches to produce a tamper signal for notification when an enclosure is opened should be considered. Tamper resistant fasteners can be employed on junction box covers to provide additional physical protection.

FR 5188

Automatic Fire Alarm Association

21

Chapter 11

Cybersecurity

11.5 Network Connectable Equipment Using Shared Pathways.

11.5.1 Network connectable equipment using the security levels required by Section 11.3(2) through Section 11.3(4) shall comply with 23.6.3.3 through 23.6.3.5 and 7.6.7.

11.5.2 Network connectable equipment using Shared Pathway Level 0, Shared Pathway Level 1, or Shared Pathway Level 2 shall comply with 23.6.3.3 through 23.6.3.5 and 7.6.7.

FR 5188 and SR 5082

Automatic Fire Alarm Association

22

Chapter 11

Cybersecurity

11.6 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

FR 5188 and SR 5154

Automatic Fire Alarm Association

23

Chapter 11

Cybersecurity

11.7 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 only trusted traffic is allowed to pass.

FR 5188

Automatic Fire Alarm Association

24

Chapter 11

Cybersecurity

11.8 Network Connectable Equipment Cybersecurity Software Updates.

11.8.1 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 11.2.

FR 5188 and SR 5095

Automatic Fire Alarm Association

25

Chapter 11

Cybersecurity

11.8.2 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 acceptance testing.

11.8.3 The equipment manufacturer(s) shall notify the system owner or their representative of all required software security updates required to maintain the cybersecurity achieved in compliance with Sections 11.2, 11.3, and 11.4

FR 5188 and SR 5095

Automatic Fire Alarm Association

26

Chapter 11

Cybersecurity

11.8.4 Software for network connectable devices shall be maintained by installing software security updates as required by the equipment manufacturer(s) to maintain the cybersecurity achieved in compliance with Sections 11.2, 11.3, and 11.4.

11.8.5 Software security updates that are deemed necessary by the equipment manufacturer(s) for compliance with Section 11.3 shall be installed at least annually.

FR 5188 and SR 5095

Automatic Fire Alarm Association

27

Chapter 11

Cybersecurity

11.8.6 Cybersecurity software updates applied to gateways or firewalls that do not affect the system site-specific or executive software shall not be required to comply with Section 14.4.2.

11.8.7 Cybersecurity software changes to systems or system components shall be permitted to be made by remote access in accordance with Section 23.8.2.11.3.

FR 5188 and SR 5087

Automatic Fire Alarm Association

28

Chapter 11

Cybersecurity

11.9 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 11.8 for any element of the system.

FR 5188 and SR 5096

Automatic Fire Alarm Association

29

Chapter 11

Cybersecurity

11.10 Cybersecurity for System Support Tools.

A system support tool and the support tool interfaces shall comply with the requirements of Sections 11.2 through 11.8.

FR 5188

Automatic Fire Alarm Association

30

Chapter 11

Cybersecurity

11.11 Evidence of Compliance.

11.11.1 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

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

FR 5188

Automatic Fire Alarm Association

31

Chapter 11

Cybersecurity

11.12 Documentation. The standards used and security levels employed in complying with Chapter 11 shall be identified in the system documentation required by Chapter 7.

FR 5188

Automatic Fire Alarm Association

32

Chapter 11

Cybersecurity

Building systems are increasingly networked and/or accessible to public facing networks. Evidence has been identified in multiple case studies including the Fire Protection Research Foundation (FPRF) report. The FPRF conducted research that has identified gaps and assessed the appropriateness of the existing provisions and guidance related to cybersecurity. Gaps include:

–Interconnection of external systems (call centers, service providers)

-Interconnection with other building systems with no access/restriction to prevent unintended communications.

-Systems that have remote access for maintenance or monitoring

-The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.

-Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable.

The revised chapter addresses the above gaps by requiring industry accepted cybersecurity practices.

FR5188, SR5082, 5154, 5095, 5096, 5086, 5087, 5089, and SCR23



Automatic Fire Alarm Association

33

Chapter 14

Inspection, Testing and Maintenance

Item 9 VRLA Battery Tests

A load test per Table 14.4.3.2 Item 9(5) is permitted as an acceptable alternative to an Ohmic test (Semiannually).

FR 5349



Automatic Fire Alarm Association

36

Chapter 14

Inspection, Testing and Maintenance

Table 14.4.3.2 Item 17(7)(a) revised to indicate that magnets are not acceptable for smoke entry tests.

FR 5349



Automatic Fire Alarm Association

37

Chapter 14

Inspection, Testing and Maintenance

14.4.3.4 Thermal image fire detectors shall be inspected, tested, and maintained in accordance with the manufacturer's published instructions.

FR 5336

Automatic Fire Alarm Association

38

Chapter 17

Initiating Devices

17.6.3.3.3 Girders.

17.6.3.3.3.1 A girder shall be considered a beam where the top of the girder is within 4 in. (100 mm) of the ceiling.

17.6.3.3.3.2 A girder shall not be a factor in detector location where the top of the girder is more than 4 in. (100 mm) from the ceiling.

SR 5031 and SR 5027

Automatic Fire Alarm Association

40

Chapter 17

Initiating Devices

17.7.2* Protection During Construction.

17.7.2.1 Detectors installed for signal initiation during new construction or building alterations shall comply with one of the following:

(1) Detectors shall be cleaned and verified to be operating in accordance with the listed sensitivity prior to the final acceptance test of the system.

(2) Detectors shall be replaced prior to the final acceptance test of the system.

17.7.2.2 Detectors installed but not operational during building alterations shall comply with one of the following:

(1) Detectors shall be protected from construction debris, dust, dirt, and damage in accordance with the manufacturer's recommendations and verified to be operating in accordance with the listed sensitivity prior to the final acceptance test of the system.

(2) Detectors shall be replaced prior to the final acceptance test of the system.

17.7.2.3 Where detection is not required during new construction, detectors shall not be installed until after all other construction trades have completed cleanup.

SR 5024

Automatic Fire Alarm Association

41

Chapter 17

Initiating Devices

17.7.4.2.3.1*

In the absence of specific performance-based design criteria, detectors on ceilings up to 40 ft (12.2 m) in height shall be spaced in accordance with either of the following:

(1) The detectors shall comply with the following:

(a) The distance between detectors shall not exceed a nominal spacing of 30 ft (9.1 m).

(b) There shall be detectors within a distance of one-half the nominal spacing, measured at right angles from all walls or partitions extending upward to within the top 15 percent of the ceiling height.

(2) *All points on the ceiling shall have a detector within a distance equal to or less than 0.7 times the nominal 30 ft (9.1 m) spacing (0.7*S*).

SR 5025

Automatic Fire Alarm Association

42

Chapter 17

Initiating Devices

17.11 Acoustic Leak Detection.

17.11.1 General.

17.11.1.1 The design documentation for an acoustic leak detector shall state the required performance objective of the system.

17.11.1.2 The purpose and scope of Section 17.11 shall be to provide requirements for the selection, location, and spacing of acoustic leak detectors.

….

Note: This slide shows only the first section.

FR 6360, SR 5034 and SR 5035

Automatic Fire Alarm Association

44

Chapter 17

Initiating Devices

17.12 Thermal Image Fire Detection.

17.12.1 Thermal image fire detection systems and all the components thereof, including hardware and software, shall be listed for the purpose of fire detection.

…

Note: This slide shows only the first section.

FR 5331

Automatic Fire Alarm Association

45

Chapter 17

Initiating Devices

17.14.1* Where carbon monoxide protection of a building is required by laws, codes, or standards, carbon monoxide detectors shall be sited in accordance with all of the following, unless a performance-based design in accordance with Section 17.3 is used:

(1) *On the ceiling or on the wall with the top of the detector within 12 in. (300 mm) of the ceiling, where installed in the same room as the permanently installed carbon monoxide source

(2) *Centrally located in every HVAC zone of the areas required by laws, codes, or standards

(3) Outside of each separate sleeping area, guest room, and guest suite within 21 ft (6.4 m) of any door to a sleeping room, with the distance measured along a path of travel

(4) Other locations where required by applicable laws, codes, or standards

(5) In accordance with the manufacturer's published instructions

FR 5333

Automatic Fire Alarm Association

46

Chapter 18

Notification Appliances

Section 18.3.7 was heavily revised and expanded.

Notification Appliance Circuits

- Modifications to DC Powered NACs
- Modifications to AC Powered NACS

Reference SCR31

SCR 31

Automatic Fire Alarm Association

47

Chapter 18

Notification Appliances



18.4.8* Restricted Audible Mode Operation (RAMO) Notification.

18.4.8.1 The requirements of 18.4.8.1.1 through 18.4.8.1.4 shall apply where RAMO is required either by the risk analysis of a notification zone or by the authority having jurisdiction, governing laws, codes, or standards, or other parts of this Code.

18.4.8.1.1 RAMO areas shall be indicated on the project drawings.

18.4.8.1.2 RAMO shall be permitted to be used only where trained, awake, and mobile staff are present in the notification zone.

18.4.8.1.3* All audible signals within a RAMO notification zone shall comply with 18.4.6.3.

18.4.8.2 All audible notification signals in a RAMO notification zone shall be synchronized in accordance with 18.4.2.5.

18.4.8.3 All visual notification signals in a RAMO notification zone shall be synchronized in accordance with 18.5.5.7.2.

FR 5352 and SR 5065

Automatic Fire Alarm Association

48

Chapter 18

Notification Appliances

18.4.6.4

For the purposes of 18.4.6, sleeping areas shall include bedrooms as well as living rooms, spare rooms, dens, and other spaces where sleeping could occur.

FR 5330

Automatic Fire Alarm Association

49

Chapter 21

Emergency Function Controls

21.2.4 Emergency Control Interface devices

21.2.4.1 Emergency control function interface devices shall be located as follows:

(1) Within 3 ft (0.9 m) of the component controlling the emergency control function where conductors are not installed in metal raceway or metal armored cables

(2) Within 20 ft (6 m) of the component controlling the emergency control function where conductors are installed in metal raceway or metal armored cables

21.2.4.2 Where configured as a Class D circuit, control circuits shall not be required to meet the requirements of 21.2.4.1(1) or 21.2.4.1(2).

FR 5005

Automatic Fire Alarm Association

50

Chapter 23

Protected Premises Systems

23.8.2.11.3 Remote access shall be permitted for testing and maintenance activities, including resetting, silencing, or operation of emergency control functions provided all of the following are met:

(1) *The system shall provide a means to manually terminate the remote access connection at the remote device and at the fire alarm or signaling system control unit at any time.

(2) *Remote access shall be automatically terminated within a maximum of 1 hour of inactivity in the remote access mode.

(3) Resetting, silencing, or operation of emergency control functions shall be limited to portion(s) of the system taken out of service.

(4) ~~Qualified~~Authorized service personnel shall be on-site to enable resetting, silencing, and operation of emergency control functions at the affected system(s) by password or limited access.

FR 5055

Automatic Fire Alarm Association

51

Chapter 24

Emergency Communications Systems

24.4.8.3.2* When the message is recorded, the repeated message sequence of 24.4.8.3.1 shall itself be repeated after a pause in accordance with one of the following:

(1) A pause of up to 180 seconds.

(2) A pause in accordance with the emergency response plan and with approval from the authority having jurisdiction.

FR 5262

Automatic Fire Alarm Association

52

Chapter 26

Supervising Station Systems

Section 26.6.5.1 is deleted.

Two-way radio technology removed from the Code.

No listed 2-way radio technology products are currently listed.

Simplifies "radio" to one-way only.

SR 5138 and SR 5127

Automatic Fire Alarm Association

54

Chapter 26

Supervising Station Systems

Subsidiary Stations

Moved in second draft meeting to 26.2.11 and renamed Intermediary Stations

NOTE: Changed (again!) with TIA 1770 approved in January 2024. Will apply to 2025 edition of NFPA 72.

SR 5150 and SR 5142

Automatic Fire Alarm Association

55

Chapter 29

Single- and Multiple-Station Alarms and Household Signaling Systems

29.1.2 Fuel gas detection and warning equipment shall be installed in accordance with NFPA 715.

SR 5129

Automatic Fire Alarm Association

56

Questions

Merton Bunker, PE
Merton.Bunker@coffman.com

Automatic Fire Alarm Association

58