Public Input No. 493-NFPA 72-2022 [Global Input]

Type your content here ...

Replace all references to NFPA 1221 with 1225 throughout the document.

Delete: NFPA 1221, Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems, 2019 edition.

Replace with: NFPA 1225, Standard for Emergency Services Communications, 2022 Edition.

Statement of Problem and Substantiation for Public Input

A global change throughout the document is that 1221 no longer exist and should reference 1225.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 14:06:32 EDT 2022
Committee: SIG-FUN

Public Input No. 55-NFPA 72-2022 [Global Input]

Change all references to NFPA 1221 to the newly published NFPA 1225, Standard for Emergency Services Communications.

Statement of Problem and Substantiation for Public Input

NFPA 1225 has replaced NFPA 1221 as of its publication in 2021.

Submitter Information Verification

Submitter Full Name: Richard Kluge
Organization: Ericsson
Affiliation: ATIS
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 10 12:50:19 EST 2022
Committee: SIG-FUN

Public Input No. 69-NFPA 72-2022 [Section No. 1.4.1]

1.4.1

~~Unless otherwise noted, it is not intended that the~~ The provisions of this document shall not be required to be applied to facilities, equipment, structures, or installations that were existing or approved for construction or installation prior to the effective date of the document.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.1.1 requires chapter 1 to be written in mandatory language. The proposed revised text from the task group includes mandatory language.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 11:33:51 EST 2022
Committee: SIG-FUN

Public Input No. 70-NFPA 72-2022 [Section No. 1.6.1]

1.6.1

The units of measure in this Code ~~are presented~~ shall be presented in U.S. Customary Units (inch-pound units).

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.3.3 requires Chapter 1 written in mandatory language. The task group proposed text includes mandatory language.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 12:22:20 EST 2022
Committee: SIG-FUN

Public Input No. 71-NFPA 72-2022 [Section No. 1.6.2]

1.6.2

Where presented, the International System of Units (SI) ~~of Units~~ shall follow the inch-pound units in parentheses.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.3.3 requires Chapter 1 written in mandatory language. The task group proposed text which includes mandatory language.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 12:28:25 EST 2022
Committee: SIG-FUN

Public Input No. 72-NFPA 72-2022 [Section No. 1.6.4]

1.6.4

Where both systems of units are presented, users of this Code shall ~~apply~~ comply with both of the following:

(1) Shall utilize only one set of units consistently~~ and shall~~

(2) Shall not alternate between units~~.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 12:32:45 EST 2022
Committee: SIG-FUN

Public Input No. 73-NFPA 72-2022 [Section No. 1.6.5]

1.6.5*

The values presented for measurements in this Code ~~are~~ shall be expressed with a degree of precision appropriate for practical application and enforcement~~. It is not intended that the application or enforcement of these values be more precise than the precision expressed.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.3.3 requires Chapter 1 written in mandatory language. The task group proposed text includes mandatory language. Also note that the second sentence of the existing paragraph is proposed to be appended to the existing annex in an associated PI-74 for A.1.6.5

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 12:47:15 EST 2022
Committee: SIG-FUN

Public Input No. 75-NFPA 72-2022 [Section No. 1.6.6]

1.6.6

Where extracted text contains values expressed in only one system of units, the values in the extracted text ~~have been~~ shall be retained without conversion to preserve the values established by the responsible technical committee in the source document.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.3.3 requires Chapter 1 written in mandatory language. The task group proposed text which includes mandatory language.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 13:17:39 EST 2022
Committee: SIG-FUN

Public Input No. 333-NFPA 72-2022 [Section No. 2.2]

2.2 NFPA Publications.

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

NFPA 10, *Standard for Portable Fire Extinguishers,* 2022 edition.

NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2022 edition.

NFPA 25, *Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems,* 2020 edition.

NFPA 37, *Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines,* 2021 edition.

NFPA 70®, National Electrical Code®, 2020 edition.

NFPA 75, *Standard for the Fire Protection of Information Technology Equipment,* 2020 edition.

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems,* 2021 edition.

NFPA *101®, Life Safety Code®,* 2021 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2022 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2022 edition.

NFPA 170, *Standard for Fire Safety and Emergency Symbols,* 2021 edition.

NFPA 601, *Standard for Security Services in Fire Loss Prevention,* 2020 edition.

NFPA 855, *Standard for the Installation of Stationary Energy Storage Systems,* 2020 edition.

NFPA 1031, *Standard for Professional Qualifications for Fire Inspector and Plan Examiner,* 2014 edition.

~~NFPA 1221~~ NFPA 1225 , Standard for ~~the Installation, Maintenance, and Use of~~ Emergency Services Communications ~~Systems~~ , ~~2019~~ 2022 edition ~~.~~

NFPA 1600®, Standard on Continuity, Emergency, and Crisis Management, 2019 edition.

NFPA 1620, *Standard for Pre-Incident Planning,* 2020 edition.

Statement of Problem and Substantiation for Public Input

A global change throughout the document to reflect that 1221 no longer exists and should reference 1225.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:

Zip:	
Submittal Date:	Mon May 23 15:15:56 EDT 2022
Committee:	SIG-FUN

Public Input No. 455-NFPA 72-2022 [Section No. 2.2]

2.2 NFPA Publications.

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

NFPA 10, *Standard for Portable Fire Extinguishers,* 2022 edition.

NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2022 edition.

NFPA 25, *Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems,* 2020 edition.

NFPA 37, *Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines,* 2021 edition.

NFPA 70®, National Electrical Code®, 2020 edition.

NFPA 75, *Standard for the Fire Protection of Information Technology Equipment,* 2020 edition.

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems,* 2021 edition.

NFPA *101®, Life Safety Code®,* 2021 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2022 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2022 edition.

NFPA 170, *Standard for Fire Safety and Emergency Symbols,* 2021 edition.

NFPA 601, *Standard for Security Services in Fire Loss Prevention,* 2020 edition.

NFPA 855, *Standard for the Installation of Stationary Energy Storage Systems,* 2020 edition.

NFPA 1031, *Standard for Professional Qualifications for Fire Inspector and Plan Examiner,* 2014 edition.

~~NFPA 1221,~~ NFPA 1225 Standard for ~~the Installation, Maintenance, and Use of~~ Emergency Services Communications ~~Systems~~ , ~~2019~~ 2022 edition ~~.~~

NFPA 1600®, Standard on Continuity, Emergency, and Crisis Management, 2019 edition.

NFPA 1620, *Standard for Pre-Incident Planning,* 2020 edition.

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_2_2_comments.docx		

Statement of Problem and Substantiation for Public Input

A global change throughout the document is that 1221 no longer exists and should reference 1225.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)

Street Address:	
City:	
State:	
Zip:	
Submittal Date:	Fri May 27 08:33:28 EDT 2022
Committee:	SIG-FUN

Public Input No. 550-NFPA 72-2022 [Section No. 2.2]

2.2 NFPA Publications.

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

NFPA 10, *Standard for Portable Fire Extinguishers,* 2022 edition.

NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2022 edition.

NFPA 25, *Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems,* 2020 edition.

NFPA 37, *Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines,* 2021 edition.

NFPA 70®, National Electrical Code®, 2020 edition.

NFPA 75, *Standard for the Fire Protection of Information Technology Equipment,* 2020 edition.

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems,* 2021 edition.

NFPA *101®, Life Safety Code®,* 2021 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2022 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2022 edition.

NFPA 170, *Standard for Fire Safety and Emergency Symbols,* 2021 edition.

NFPA 601, *Standard for Security Services in Fire Loss Prevention,* 2020 edition.

NFPA 855, *Standard for the Installation of Stationary Energy Storage Systems,* 2020 edition.

NFPA 1031, *Standard for Professional Qualifications for Fire Inspector and Plan Examiner,* 2014 edition.

~~NFPA 1221~~ NFPA 1225 , *Standard for ~~the Installation, Maintenance, and Use of~~ Emergency Services Communications ~~Systems~~* , ~~2019 edition~~ *2022* edition .

NFPA 1600®, Standard on Continuity, Emergency, and Crisis Management, 2019 edition.

NFPA 1620, *Standard for Pre-Incident Planning,* 2020 edition.

Statement of Problem and Substantiation for Public Input

As part of the Emergency Response and Responder Safety Document Consolidation Plan (consolidation plan) as approved by the NFPA Standards Council, NFPA 1225 is a combination of Standards NFPA 1061 and NFPA 1221. For consolidated Standard and revision cycle information, see the Next Edition tab.

Submitter Information Verification

Submitter Full Name: Sagiv Weiss-Ishai
Organization: San Francisco Fire Department
Affiliation: SFFD
Street Address:
City:

State:	
Zip:	
Submittal Date:	Tue May 31 17:39:24 EDT 2022
Committee:	SIG-FUN

Public Input No. 551-NFPA 72-2022 [Section No. 2.3.3]

2.3.3 ASME Publications.

American Society of Mechanical Engineers, Two Park Avenue, New York, NY 10016-5990.

ASME A17.1/CSA B44, *Safety Code for Elevators and Escalators*, ~~2019~~ 2022 .

Statement of Problem and Substantiation for Public Input

the 2022 Edition of the A17.1/B44 was already completed and estimated to be published at the end of 2022 or beginning of 2023. Therefore the A17.1/B44 2022 edition should be referenced in the 2025 Edition of NFPA 72 as the most updated and recent elevator code.

Submitter Information Verification

Submitter Full Name: Sagiv Weiss-Ishai
Organization: San Francisco Fire Department
Affiliation: SFFD
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 31 17:42:22 EDT 2022
Committee: SIG-FUN

Public Input No. 559-NFPA 72-2022 [Section No. 2.3.9]

2.3.9 UL Publications.

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

UL 38, *Manual Signaling Boxes for Fire Alarm Systems,* 2008, revised 2018.

UL 217, *Smoke Alarms*, ~~8th edition~~ 2020 , ~~2015,~~ revised ~~2016~~ 2021 .

UL 268, *Smoke Detectors for Fire Alarm Systems*, ~~7th edition~~ 2016 , ~~2016~~ revised 2021 .

UL 521, *Heat Detectors for Fire Protective Signaling Systems*, 1999, revised ~~2017~~ 2021 .

UL 827, *Central-Station Alarm Services*, 2014, revised ~~2019~~ 2021 .

UL 864, *Control Units and Accessories for Fire Alarm Systems*, 2014, revised ~~2018~~ 2020 .

UL 985, *Household Fire Warning System Units*, 2015, revised 2018.

UL 1484, *Residential Gas Detectors*, 2016, revised ~~2017~~ 2022 .

UL 1638, *Visible Signaling Devices for Fire Alarm and Signaling Systems, Including Accessories*, 2016.

UL 1730, *Smoke Detector Monitors and Accessories for Individual Living Units of Multifamily Residences and Hotel/Motel Rooms*, 2006, revised 2017.

UL 1971, *Signaling Devices for the Hearing Impaired*, 2002, revised 2018.

UL 1981, *Central Station Automation Systems*, 2014, revised ~~2015~~ 2019 .

UL 2017, *General-Purpose Signaling Devices and Systems*, 2008, revised 2018.

UL 2034, *Single and Multiple Station Carbon Monoxide Alarms,* 2017, revised 2018.

UL 2075, *Gas and Vapor Detectors and Sensors,* 2013, revised ~~2017~~ 2021 .

UL 2525, *Two-way Emergency Communications Systems for Rescue Assistance*, 2020.

UL 2572, *Mass Notification Systems*, 2016, revised 2018.

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

UL 62368-1, *Audio/Video, Information and Communication Technology Equipment — Part 1: Safety Requirements,* 2019, revised 2021 .

Statement of Problem and Substantiation for Public Input

Changes are updates to edition or revision dates and are submitted reference updates.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 560-NFPA 72-2022 [Section No. K.1.2.15]	

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL LLC
Street Address:

City:	
State:	
Zip:	
Submittal Date:	Wed Jun 01 10:41:58 EDT 2022
Committee:	SIG-FUN

Public Input No. 552-NFPA 72-2022 [Section No. 2.4]

2.4 References for Extracts in Mandatory Sections.

NFPA 13, *Standard for the Installation of Sprinkler Systems,*~~2022 edition~~ 2025 edition .

NFPA 70®, National Electrical Code®, 2020 edition.

NFPA *101®, Life Safety Code®,* 2021 edition.

NFPA 654, *Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids,* 2020 edition.

~~NFPA 1221~~ NFPA 1225 , *Standard for ~~the Installation, Maintenance, and Use of~~ Emergency Services Communications ~~Systems~~ ,*~~2019 edition~~ 2022 edition .

NFPA 5000®, Building Construction and Safety Code®, 2021 edition.

Statement of Problem and Substantiation for Public Input

As part of the Emergency Response and Responder Safety Document Consolidation Plan (consolidation plan) as approved by the NFPA Standards Council, NFPA 1225 is a combination of Standards NFPA 1061 and NFPA 1221. For consolidated Standard and revision cycle information, see the Next Edition tab.

Submitter Information Verification

Submitter Full Name: Sagiv Weiss-Ishai
Organization: San Francisco Fire Department
Affiliation: SFFD
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 31 17:45:33 EDT 2022
Committee: SIG-FUN

Public Input No. 498-NFPA 72-2022 [New Section after 3.3.63]

3.3. X Gateway.

A means of signal transport between a protected premise and a Public Safety Answering Point (PSAP) which is owned, operated and maintained by a private for profit entity. May be part of the communications cloud. The pathway is governed under the scope of NFPA 72.

Statement of Problem and Substantiation for Public Input

This is a definition for a new means of signal transport that has emerged since the last cycle of NFPA 72 (2022). In this case the equipment is not maintained or owned by a public utility and the exception for public utilities that is described within Chapter 26 should be excluded.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 495-NFPA 72-2022 [Chapter 25]	New Chapter
Public Input No. 497-NFPA 72-2022 [New Section after 10.5.6.4.3]	New qualifications
Public Input No. 499-NFPA 72-2022 [Section No. A.26.6.2.4]	Revised Exception
Public Input No. 501-NFPA 72-2022 [Section No. A.26.6.2.4]	New Fig
Public Input No. 495-NFPA 72-2022 [Chapter 25]	
Public Input No. 497-NFPA 72-2022 [New Section after 10.5.6.4.3]	
Public Input No. 499-NFPA 72-2022 [Section No. A.26.6.2.4]	
Public Input No. 501-NFPA 72-2022 [Section No. A.26.6.2.4]	

Submitter Information Verification

Submitter Full Name: Shane Clary
Organization: Bay Alarm Company
Affiliation: Bay Alarm Company
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 15:03:38 EDT 2022
Committee: SIG-FUN

Public Input No. 319-NFPA 72-2022 [Section No. 3.3.65.1.3]

3.3.65.1.3* Supervisory Condition.

An abnormal condition in connection with the supervision ~~of~~ , operation, or status of other systems, processes, or equipment. (SIG-FUN)

Statement of Problem and Substantiation for Public Input

This PI is intended to prompt a discussion around the age-old definitions of supervisory and trouble conditions, particularly how they relate to current and future sensors and devices which perhaps were not contemplated when these definitions were developed. Accurate guidance from NFPA 72 is critical as other technical committees attempt to apply these conditions to those found in other standards. Information gathered during a presentation on this topic at the '22 NFPA C&E will be forwarded to SIG-FUN for consideration.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 320-NFPA 72-2022 [Section No. 3.3.65.1.4]	
Public Input No. 320-NFPA 72-2022 [Section No. 3.3.65.1.4]	

Submitter Information Verification

Submitter Full Name: Jason Webb
Organization: Potter Electric Signal Company
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 20 09:48:57 EDT 2022
Committee: SIG-FUN

Public Input No. 320-NFPA 72-2022 [Section No. 3.3.65.1.4]

3.3.65.1.4* Trouble Condition.

An abnormal condition in a system, sensor, or device due to a fault. (SIG-FUN)

Statement of Problem and Substantiation for Public Input

This PI is intended to prompt a discussion around the age-old definitions of supervisory and trouble conditions, particularly how they relate to current and future sensors and devices which perhaps were not contemplated when these definitions were developed. Accurate guidance from NFPA 72 is critical as other technical committees attempt to apply these conditions to those found in other standards. Information gathered during a presentation on this topic at the '22 NFPA C&E will be forwarded to SIG-FUN for consideration.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 319-NFPA 72-2022 [Section No. 3.3.65.1.3]	
Public Input No. 319-NFPA 72-2022 [Section No. 3.3.65.1.3]	

Submitter Information Verification

Submitter Full Name: Jason Webb
Organization: Potter Electric Signal Company
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 20 10:00:33 EDT 2022
Committee: SIG-FUN

Public Input No. 334-NFPA 72-2022 [New Section after 3.3.65.2]

3.3.66 Network Connectable Equipment

System components that connect to the internet or each other through wired or wireless pathways using various protocols.

Statement of Problem and Substantiation for Public Input

The term “Network Connectable Equipment” is now used as part of the cybersecurity changes and the definition should be added to 72 to help the reader understand how the new term is being used.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 23 15:48:58 EDT 2022
Committee: SIG-FUN

Public Input No. 494-NFPA 72-2022 [Section No. 3.3.66]

3.3.66 Constantly Attended.

Attended 24 hours a day and 365 days a year. (SIG-PRO)

3.3.66 Network Connectable Equipment

System Components that connect to the internet or each other through wired or wireless pathways using various protocols.

Statement of Problem and Substantiation for Public Input

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.
Their report lists gaps that include:

- Configuration – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
- Implementation – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
- Security – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.
- Access – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment

The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here.

- https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
- Researchers Hack Building Control System at Google Australia Office | WIRED

Target Hackers Broke in Via HVAC Company – Krebs on Security

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 14:24:49 EDT 2022
Committee: SIG-FUN

Public Input No. 337-NFPA 72-2022 [New Section after 3.3.288.2]

Cybersecurity-related Only Software

Software that is included in a system element that is 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 to cybersecurity attacks.

Statement of Problem and Substantiation for Public Input

Defining term added to types of software in section 3.3.288.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 335-NFPA 72-2022 [Section No. 3.3.288]	added subsection to 3.3.288

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 23 16:21:52 EDT 2022
Committee: SIG-FUN

Public Input No. 579-NFPA 72-2022 [Chapter 4]

Chapter 4 ~~Reserved~~ **~~Noncombustible material [101: 4.6.13]~~**

4.1 *

A material that complies with any one of the following shall be considered a noncombustible material:

(1) *

The material, in the form in which it is used, and under the conditions anticipated, will not ignite, burn, support combustion, or release flammable vapors when subjected to fire or heat.

(2)

The material is reported as passing ASTM E136, *Standard Test Method for Assessing Combustibility of Materials Using a Vertical Tube Furnace at 750°C.*

(3)

The material is reported as complying with the pass/fail criteria of ASTM E136 when tested in accordance with the test method and procedure in ASTM E2652, *Standard Test Method for Assessing Combustibility of Materials Using a Tube Furnace with a Cone-shaped Airflow Stabilizer, at 750°C.* [101:4.6.13]

A.4.1 The provisions of 4.1 do not require inherently noncombustible materials to be tested in order to be classified as noncombustible materials. [101: A.4.6.13.1]

A.4.1 (1) Examples of such materials include steel, concrete, masonry, and glass.

The provision of 4.1(1) recognizes that some materials are inherently noncombustible and do not require testing to receive a classification of noncombustible. The text of A.4.1(1) provides examples of such materials. [101:A.6.6.13.1(1)]

Also, add ASTM E136 (2019a) and ASTM E2652 (2018) into section 2 on referenced ASTM standards.

ASTM E136, *Standard Test Method for Assessing Combustibility of Materials Using a Vertical Tube Furnace at 750°C* , 2019.

ASTM E2652, *Standard Test Method for Assessing Combustibility of Materials Using a Tube Furnace with a Cone-shaped Airflow Stabilizer, at 750°C* , 2018.

Statement of Problem and Substantiation for Public Input

NFPA 72 requires the use of noncombustible materials in two instances but does not describe what that means. This text, extracted from NFPA 101, describes the requirements for a noncombustible material. Note that US codes and standards typically require materials to "pass" ASTM E136 in order to be classified as noncombustible. That means that this requirement is slightly less severe than the requirement that the material "will not ignite, burn, support combustion, or release flammable vapors when subjected to fire or heat", since the requirements of ASTM E136 allow a material to have some minimal flaming and mass loss and temperature increase, as shown below. Having discussed the criteria in ASTM E136 it is important to note that some materials will be classified as combustible or noncombustible depending on the amount (typically very small) of combustible resin or binder included to ensure the material has appropriate cohesion.
ASTM E136 acceptance criteria:
ASTM E136 - Standard Test Method for Assessing Combustibility of Materials Using a Vertical Tube Furnace at 750°C

15.1 Report the material as passing the test if at least three of the four test specimens tested meet the individual test specimen criteria detailed in 15.2 or 15.3. The three test specimens do not need to meet the same individual test specimen criteria.

15.2 If the weight loss of the test specimen is 50 % or less, the material passes the test when the criteria in 15.2.1 and in 15.2.2 are met:
15.2.1 The recorded temperatures of the surface and interior thermocouples do not at anytime during the test rise more than 30°C (54°F) above the stabilized furnace temperature measured at T2 prior to the test.
15.2.2 There is no flaming from the test specimen after the first 30 s.
15.3 If the weight loss of the specimen exceeds 50 %, the material passes the test when the criteria in 15.3.1 and in 15.3.2 are met:
15.3.1 The recorded temperatures of the surface and interior thermocouples do not at anytime during the test rise above the stabilized furnace temperature measured at T2 prior to the test.
15.3.2 No flaming from the test specimen is observed at any time during the test.
15.4 Report the option that was used.

Submitter Information Verification

Submitter Full Name: Marcelo Hirschler
Organization: GBH International
Street Address:
City:
State:
Zip:
Submittal Date: Wed Jun 01 18:43:10 EDT 2022
Committee: SIG-FUN

Public Input No. 224-NFPA 72-2022 [Section No. 7.2.1]

7.2.1*

Where documentation is required by the authority having jurisdiction, the following list shall represent the minimum documentation required for new systems and additions or alterations to existing systems:

(1) * Written narrative providing intent and system description

(2) Riser diagram

(3) Floor plan layout showing locations of all devices, control equipment, and supervising station and shared communications equipment with each sheet showing the following:

(4) Point of compass (north arrow)

(5) A graphic representation of the scale used

(6) Room use identification

(7) Building features that will affect the placement of initiating devices and notification appliances

(8) Sequence of operation in either an input/output matrix or narrative form

(9) Equipment technical data sheets

(10) Manufacturers' published instructions, including operation and maintenance instructions

(11) Battery capacity and safety margin calculations (where batteries are provided)

(12) Voltage drop calculations for notification appliance circuits

(13) Mounting height elevation for wall-mounted devices and appliances

(14) Where occupant notification is required, minimum sound pressure levels that must be produced by the audible notification appliances in applicable covered areas

(15) Locations of alarm notification appliances, including candela ratings for visual alarm notification appliances

(16)* Pathway diagrams between the control unit and shared communications equipment within the protected premises

(17) Completed record of completion in accordance with 7.5.6

(18) For software-based systems, a copy of site-specific software, including specific instructions on how to obtain the means of system and software access (password)

(19) Record (as-built) drawings

(20) Records, record retention, and record maintenance in accordance with Section 7.7

(21) Completed record of inspection and testing in accordance with 7.6.6

(22) Verification of fire alarm activation on suppression system activation (all initiating devices)

(23) Central Station notification of suppression system activation

(24) Make up air shut down (operation and identificatoin of location of devices)

(25) Exhaust air activation (if not in operation) - operation and identification of location of devices

(26) Cooking appliance shut down

Statement of Problem and Substantiation for Public Input

Fire suppression systems installed in accordance with other NFPA standards are rarely if ever documented in this matrix of requirements. Additionally, the fire suppression system activation and associated fan operations and power disconnect as well as signals to monitoring are likewise not documented. Testing of the activation of fire suppression systems and integration with the fire alarm system is necessary for full system reliability. Locations of all of the related devices also need to be included in the documentation.

Submitter Information Verification

Submitter Full Name: Scott Futrell
Organization: Futrell Fire Consult & Design, Inc.
Street Address:
City:
State:
Zip:
Submittal Date: Thu Apr 14 13:35:25 EDT 2022
Committee: SIG-FUN

Public Input No. 225-NFPA 72-2022 [Section No. 7.2.1]

7.2.1*

Where documentation is required by the authority having jurisdiction, the following list shall represent the minimum documentation required for new systems and additions or alterations to existing systems:

(1) * Written narrative providing intent and system description

(2) Riser diagram

(3) Floor plan layout showing locations of all devices, control equipment, and supervising station and shared communications equipment with each sheet showing the following:

(4) Point of compass (north arrow)

(5) A graphic representation of the scale used

(6) Room use identification

(7) Building features that will affect the placement of initiating devices and notification appliances

(8) Sequence of operation in either an input/output matrix or narrative form

(9) Equipment technical data sheets

(10) Manufacturers' published instructions, including operation and maintenance instructions

(11) Battery capacity and safety margin calculations (where batteries are provided)

(12) Voltage drop calculations for notification appliance circuits

(13) Mounting height elevation for wall-mounted devices and appliances

(14) Where occupant notification is required, minimum sound pressure levels that must be produced by the audible notification appliances in applicable covered areas

(15) Locations of alarm notification appliances, including candela ratings for visual alarm notification appliances

(16) Pathway diagrams between the control unit and shared communications equipment within the protected premises

(17) Completed record of completion in accordance with 7.5.6

(18) For software-based systems, a copy of site-specific software, including specific instructions on how to obtain the means of system and software access (~~password~~ passwords for all levels of access)

(19) Record (as-built) drawings

(20) Records, record retention, and record maintenance in accordance with Section 7.7

(21) Completed record of inspection and testing in accordance with 7.6.6

Statement of Problem and Substantiation for Public Input

The passwords for all levels of access need to be available to the building owner or manager. This is very important for emergency service or when the installer is not available. It is understood by the author that the proprietary system sellers, installers, and dealers will be against this change. They do not have a relevant argument because the passwords are necessary for use by the owner or

manager's when they need additional assistance from other contractors. Fire and life safety is the goal and cannot be assured or guaranteed without access to the required passwords.

Submitter Information Verification

Submitter Full Name: Scott Futrell
Organization: Futrell Fire Consult & Design, Inc.
Street Address:
City:
State:
Zip:
Submittal Date: Thu Apr 14 14:45:43 EDT 2022
Committee: SIG-FUN

Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]

7.2.1*

Where documentation is required by the authority having jurisdiction, the following list shall represent the minimum documentation required for new systems and additions or alterations to existing systems:

(1) * Written narrative providing intent and system description

(2) Riser diagram

(3) Floor plan layout showing locations of all devices, control equipment, and supervising station and shared communications equipment with each sheet showing the following:

(4) Point of compass (north arrow)

(5) A graphic representation of the scale used

(6) Room use identification

(7) Building features that will affect the placement of initiating devices and notification appliances

(8) Sequence of operation in either narrative form, a logic diagram, or an input/output matrix ~~or narrative form~~

(9) Equipment technical data sheets

(10) Manufacturers' published instructions, including operation and maintenance instructions

(11) Battery capacity and safety margin calculations (where batteries are provided)

(12) Voltage drop calculations for notification appliance circuits

(13) Mounting height elevation for wall-mounted devices and appliances

(14) Where occupant notification is required, minimum sound pressure levels that must be produced by the audible notification appliances in applicable covered areas

(15) Locations of alarm notification appliances, including candela ratings for visual alarm notification appliances

(16) Pathway diagrams between the control unit and shared communications equipment within the protected premises

(17) Completed record of completion in accordance with 7.5.6

(18) For software-based systems, a copy of site-specific software, including specific instructions on how to obtain the means of system and software access (password)

(19) Record (as-built) drawings

(20) Records, record retention, and record maintenance in accordance with Section 7.7

(21) Completed record of inspection and testing in accordance with 7.6.6

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document

the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

See PI 463-NFPA 72-2022 uploaded logic diagram.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 344-NFPA 72-2022 [Section No. 7.4.9]	
Public Input No. 345-NFPA 72-2022 [Section No. 7.5.4]	
Public Input No. 346-NFPA 72-2022 [Section No. 7.5.5.2]	
Public Input No. 352-NFPA 72-2022 [Section No. 10.14.7.4]	
Public Input No. 353-NFPA 72-2022 [Section No. 10.15.10.5]	
Public Input No. 368-NFPA 72-2022 [Section No. 14.4.3.2]	
Public Input No. 375-NFPA 72-2022 [Section No. A.7.3.2]	
Public Input No. 376-NFPA 72-2022 [Section No. A.14.4.3]	
Public Input No. 379-NFPA 72-2022 [Section No. A.24.3.9]	
Public Input No. 451-NFPA 72-2022 [Section No. A.7.4.9]	
Public Input No. 456-NFPA 72-2022 [Section No. A.7.5.5.2]	
Public Input No. 463-NFPA 72-2022 [Section No. A.14.6.1.1]	
Public Input No. 344-NFPA 72-2022 [Section No. 7.4.9]	
Public Input No. 345-NFPA 72-2022 [Section No. 7.5.4]	

Public Input No. 346-NFPA 72-2022 [Section No. 7.5.5.2]
Public Input No. 352-NFPA 72-2022 [Section No. 10.14.7.4]
Public Input No. 353-NFPA 72-2022 [Section No. 10.15.10.5]
Public Input No. 375-NFPA 72-2022 [Section No. A.7.3.2]
Public Input No. 376-NFPA 72-2022 [Section No. A.14.4.3]
Public Input No. 379-NFPA 72-2022 [Section No. A.24.3.9]
Public Input No. 451-NFPA 72-2022 [Section No. A.7.4.9]
Public Input No. 463-NFPA 72-2022 [Section No. A.14.6.1.1]

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 18 15:29:56 EDT 2022
Committee: SIG-FUN

Public Input No. 76-NFPA 72-2022 [Section No. 7.4.3]

7.4.3

Shop drawings for fire alarm or emergency communications systems shall provide ~~basic information and shall provide the~~ both of the following:

(1) Basic information

(2) The basis for the record (as-built) drawings required in accordance with 7.5.~~2~~ 5 .

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.
Also, the 2022 edition has the section for Record Drawings (As-Builts) in section 7.5.5, not 7.5.2. Changed the section of reference to be most relevant.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 13:20:54 EST 2022
Committee: SIG-FUN

Public Input No. 33-NFPA 72-2021 [Section No. 7.4.4]

7.4.4

Shop drawings shall include the following information:

(1) Name of protected premises, owner, and occupant (where applicable)

(2) Name of installer or contractor

(3) Location of protected premises

(4) Device legend and symbols in accordance with NFPA 170, or other symbols acceptable to the authority having jurisdiction

(5) Date of issue and any revision dates

(6) Edition year of NFPA 72 to which the system is designed

Statement of Problem and Substantiation for Public Input

This is an important piece of information to include on the drawing . The text was modelled after current NFPA 13 requirements.

Submitter Information Verification

Submitter Full Name: Chase Browning
Organization: Medford Fire Department
Affiliation: Southern Oregon Fire Code Officials
Street Address:
City:
State:
Zip:
Submittal Date: Wed Dec 01 12:11:49 EST 2021
Committee: SIG-FUN

Public Input No. 145-NFPA 72-2022 [New Section after 7.4.7]

7.4.7.1

Control Unit diagrams shall be provided for all control equipment (i.e., equipment listed as either a control unit or a control unit accessory), power supplies, battery chargers, and annunciators.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new section with separate paragraphs for the multiple requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 144-NFPA 72-2022 [Section No. 7.4.7]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 17:27:52 EST 2022
Committee: SIG-FUN

Public Input No. 146-NFPA 72-2022 [New Section after 7.4.7]

7.4.7.2

Control unit diagrams shall include the following information:

(1) Identification of the control equipment depicted

(2) Location(s) of control equipment

(3) All field wiring terminals and terminal identifications

(4) All circuits connected to field wiring terminals and circuit identifications

(5) All indicators and manual controls

(6) Field connections to supervising station signaling equipment, releasing equipment, or emergency safety control interfaces, where provided

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new section with separate paragraphs for the multiple requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 144-NFPA 72-2022 [Section No. 7.4.7]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 17:30:32 EST 2022
Committee: SIG-FUN

Public Input No. 144-NFPA 72-2022 [Section No. 7.4.7]

7.4.7

Control ~~unit diagrams shall be provided for all control equipment (i.e., equipment listed as either a control unit or control unit accessory), power supplies, battery chargers, and annunciators and shall include the following information:~~

(1) ~~Identification of the control equipment depicted~~

(2) ~~Location(s) of control equipment~~

(3) ~~All field wiring terminals and terminal identifications~~

(4) ~~All circuits connected to field wiring terminals and circuit identifications~~

(5) ~~All indicators and manual controls~~

(6) ~~Field connections to supervising station signaling equipment, releasing equipment, or emergency safety control interfaces, where provided~~

Unit Diagrams.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new section with separate paragraphs for the multiple requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 145-NFPA 72-2022 [New Section after 7.4.7]	
Public Input No. 146-NFPA 72-2022 [New Section after 7.4.7]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 17:23:29 EST 2022
Committee: SIG-FUN

Public Input No. 344-NFPA 72-2022 [Section No. 7.4.9]

7.4.9*

A ~~narrative description or~~ description of the sequence of operation shall be provided in narrative form, a logic diagram,

or an input/output matrix~~ of operation shall be provided to describe the sequence of operation~~ .

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 13:57:34 EDT 2022
Committee: SIG-FUN

Public Input No. 575-NFPA 72-2022 [Section No. 7.4.9]

7.4.9*

A narrative description or input/output matrix of operation shall be provided to describe the sequence of operation, including all of the following as applicable:

(1) All inputs individually or grouped by type, floor, and/or function

(2) All outputs individually or grouped by type, floor, and/or function

(3) All conditions reported to a central station, remote supervising station, proprietary supervising station or public emergency alarm reporting system, including whether reporting is via grouped condition type or point identification type

(4) Use of public mode and/or private mode notification by area per 23 . 8.6.1.1

(5) Use of relocation and partial evacuation by floor or area per 24.4.8

(6) Use of presignal features per 23.8.1.1

(7) Use of positive alarm sequence per 23.8.1.2

(8) Use of alarm verification features per 23.8.5.4.1

(9) Use of detector cross-zoning per 23.8.5.4.3 and 23.8.5.4.4

(10) Inputs and outputs for each elevator interface per Chapter 21

(11) Detailed input and output matrix for OEO operation per 21.6.2

(12) Inputs and outputs for each HVAC interface per Chapter 21

(13) All inputs and outputs for activation of a fire fighter's smoke control station (FSCS) or integration with a smoke control system per 21.7.7

(14) Inputs and outputs, including notification sequence, for carbon monoxide or other gas detection

(15) Inputs and outputs for dry pipe and preaction sprinkler systems per 17.17.2.2.2 and 23.11

(16) Inputs and outputs, including abort switches, for integrated releasing systems per 23.8.5.10 and 23.11

(17) Identification and sequence for all selective signaling and manual activation buttons/switches on a control unit and/or annunciator, including bypass activations

(18) Where prerecorded voice messages are used per 24.3.6, the content (i.e., text) of the messages and message sequence, including pre-tones and post-tones shall be detailed

(19) Inputs and outputs for all mass notification system (MNS) features, including MNS override of fire alarm signals allowed by 24.5.13 and text of messages used per 24.3.6

(20) Sequence of operation shall include details on acknowledge, silence, and reset functions as applicable

Statement of Problem and Substantiation for Public Input

Fire investigations continue to reveal that existing owner documentation and shop drawings are not providing detailed sequence of operations, especially for unique situations like positive alarm sequence, presignal, detector cross-zoning and releasing systems. NFPA 72 has multiple provisions allowing uniquely programmed sequences, including selective signaling, partial evacuation sequences,

and the like, but rarely are these detailed in the sequence of operation. This list can be applied by a designer, almost like a checklist, to verify that all unique sequences are detailed in the shop drawings, allowing the Owner to receive documentation of how there system is programmed as required by 7.5.5.2 and 14.6.1.1. This list of requirements is scalable based on the size of the project, as only those items that apply need to be included in the sequence of operation. Also, the list allows both a matrix or a written narrative to meet the objectives of the items in the list.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 576-NFPA 72-2022 [Section No. A.7.5.5.2]	
Public Input No. 577-NFPA 72-2022 [Section No. A.14.6.1.1]	
Public Input No. 580-NFPA 72-2022 [New Section after 21.6.2]	

Submitter Information Verification

Submitter Full Name: Larry Rietz
Organization: Jensen Hughes
Street Address:
City:
State:
Zip:
Submittal Date: Wed Jun 01 17:30:50 EDT 2022
Committee: SIG-FUN

Public Input No. 32-NFPA 72-2021 [New Section after 7.4.10]

7.4.11

A narrative description or diagram shall be provided to describe the chosen communications method for Supervising Station Alarm Systems, where applicable.

Statement of Problem and Substantiation for Public Input

A common issues we see is the transmission method is deferred to the end of the project, which was not an issue when only POTS lines were used, however, with newer technologies, we have seen not only proprietary conflicts but secondary power issues along with delays late on in the projects. Having the communications method described on the shop drawings will ensure that the design is coordinated early on and will be beneficial to all parties involved.

Submitter Information Verification

Submitter Full Name: Chase Browning
Organization: Medford Fire Department
Affiliation: Southern Oregon Fire Code Officials
Street Address:
City:
State:
Zip:
Submittal Date: Wed Dec 01 12:00:41 EST 2021
Committee: SIG-FUN

Public Input No. 345-NFPA 72-2022 [Section No. 7.5.4]

7.5.4

For new emergency communications systems, an owner's manual shall be provided and shall contain the following documentation:

(1) Detailed narrative description of the system inputs, evacuation signaling, ancillary functions, annunciation, intended sequence of operations, expansion capability, application considerations, and limitations

(2) Written sequence of operation for the system including a logic diagram or an operational input/output matrix

(3) Operator instructions for basic system operations, including alarm acknowledgment, system reset, interpretation of system output (LEDs, CRT display, and printout), operation of manual evacuation signaling and ancillary function controls, and change of printer paper

(4) Detailed description of routine maintenance and testing as required and recommended and as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed, which includes the following:

(5) Listing of the individual system components that require periodic testing and maintenance

(6) Step-by-step instructions detailing the requisite testing and maintenance procedures, and the intervals at which those procedures shall be performed, for each type of device installed

(7) Schedule that correlates the testing and maintenance procedures that are required by this section

(8) Service directory, including a list of names and telephone numbers of those who provide service for the system

(9) Product data sheets for all system equipment

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the

sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 14:08:33 EDT 2022
Committee: SIG-FUN

Public Input No. 78-NFPA 72-2022 [Section No. 7.5.4]

7.5.4 ~~–~~

~~For~~

N ew Emergency Communications Systems Documentation.

7.5.4.1 An owner’s manual shall be provided for new emergency communications systems

~~, an owner’s manual shall be provided and shall~~

~~.~~

7.5.4.2 The owner's manual shall contain the following documentation:

(1) Detailed narrative description of the system inputs, evacuation signaling, ancillary functions, annunciation, intended sequence of operations, expansion capability, application considerations, and limitations

(2) Written sequence of operation for the system including an operational input/output matrix

(3) Operator instructions for basic system operations, including alarm acknowledgment, system reset, interpretation of system output (LEDs, CRT display, and printout), operation of manual evacuation signaling and ancillary function controls, and change of printer paper

(4) Detailed description of routine maintenance and testing as required and recommended and as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed, which includes the following:

(5) Listing of the individual system components that require periodic testing and maintenance

(6) Step-by-step instructions detailing the requisite testing and maintenance procedures, and the intervals at which those procedures

~~shall~~

(a) are to be performed, for each type of device installed

(b) Schedule that correlates the testing and maintenance procedures that are required by this section

(7) Service directory, including a list of names and telephone numbers of those who provide service for the system

(8) Product data sheets for all system equipment

Additional Proposed Changes

File Name	Description	Approved
72_7.5.4_PI-78_proposed_text.docx	PI-78 list view since list view for 'c' is not showing properly in Terra View preview.	

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue.

Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new section with separate paragraphs for the multiple requirements. The task group also recommended editorial change in list item (b) from 'shall' to 'are to'.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 13:36:36 EST 2022
Committee: SIG-FUN

7.5.4 N

~~For n~~ew Eemergency ~~communications~~ Communications Ssystems Documentation.
7.5.4.1 A~~, a~~n owner's manual shall be provided for new emergency communications systems.
7.5.4.2 The owner's manual ~~and~~ shall contain the following documentation:

(1) Detailed narrative description of the system inputs, evacuation signaling, ancillary functions, annunciation, intended sequence of operations, expansion capability, application considerations, and limitations

(2) Written sequence of operation for the system including an operational input/output matrix

(3) Operator instructions for basic system operations, including alarm acknowledgment, system reset, interpretation of system output (LEDs, CRT display, and printout), operation of manual evacuation signaling and ancillary function controls, and change of printer paper

(4) Detailed description of routine maintenance and testing as required and recommended and as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed, which includes the following:

(a) Listing of the individual system components that require periodic testing and maintenance

(b) Step-by-step instructions detailing the requisite testing and maintenance procedures, and the intervals at which those procedures ~~shall~~ are to be performed, for each type of device installed

(c) Schedule that correlates the testing and maintenance procedures that are required by this section

(5) Service directory, including a list of names and telephone numbers of those who provide service for the system

(6) Product data sheets for all system equipment

Public Input No. 346-NFPA 72-2022 [Section No. 7.5.5.2]

7.5.5.2*

A sequence of operations ~~in~~ in narrative form, a logic diagram, or an input/output matrix ~~or narrative form~~ shall be provided with the record drawings to reflect actual programming at the time of completion.

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 14:13:07 EDT 2022
Committee: SIG-FUN

Public Input No. 79-NFPA 72-2022 [Section No. 7.5.6.2]

7.5.6.2*– Record of Completion Documentation.

7.5.6.2.1 The record of completion documentation shall be completed by the installing contractor and submitted to the authority having jurisdiction and the owner at the conclusion of the job.

7.5.6.2.2 The record of completion documentation shall be permitted to be part of the written statement required in 7.5.2 and part of the documents that support the requirements of 7.5.8 .

7.5.6.2.3 When more than one contractor has been responsible for the installation, each contractor shall complete the portions of the documentation for which that contractor has responsibility.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text creates a new section and provides new paragraphs for each requirement.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 14:18:31 EST 2022
Committee: SIG-FUN

Public Input No. 82-NFPA 72-2022 [Section No. 7.5.6.6.1]

7.5.6.6.1

All modifications made after the initial installation shall be recorded on a revised version of the original completion documents~~, which shall~~ .

7.5.6.6.2

The revised version of the original completion documents shall serve as a supplement to the original, unaltered completion documents.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text creates a new section and provides new paragraphs for each requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 83-NFPA 72-2022 [Section No. 7.5.6.6.2]	
Public Input No. 84-NFPA 72-2022 [Section No. 7.5.6.6.3]	
Public Input No. 85-NFPA 72-2022 [Section No. A.7.5.6.6.3]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 19:52:37 EST 2022
Committee: SIG-FUN

Public Input No. 83-NFPA 72-2022 [Section No. 7.5.6.6.2]

7.5.6.6.~~2~~ 3

The revised record of completion document shall include a revision date.

Statement of Problem and Substantiation for Public Input

This PI links with PI-82. If accepted/revised, this paragraph requires renumbering.
Substantiation from that PI: NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue.
Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text creates a new section and provides new paragraphs for each requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 82-NFPA 72-2022 [Section No. 7.5.6.6.1]	renumbering

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 20:06:33 EST 2022
Committee: SIG-FUN

Public Input No. 84-NFPA 72-2022 [Section No. 7.5.6.6.3]

7.5.6.6.~~3~~ 4 *

Where the original or the latest overall system record of completion cannot be obtained, a new system record of completion shall be provided that documents the system configuration as discovered during the current project's scope of work.

Statement of Problem and Substantiation for Public Input

This PI links with PI-82. If accepted/revised, this paragraph and associated annex will require renumbering.
Substantiation from PI-82: NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue.
Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text creates a new section and provides new paragraphs for each requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 82-NFPA 72-2022 [Section No. 7.5.6.6.1]	renumber

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 20:08:22 EST 2022
Committee: SIG-FUN

Public Input No. 86-NFPA 72-2022 [Section No. 7.5.6.7.2]

7.5.6.7.2

If filed electronically, the record of completion document shall be ~~accessible~~ both:

(1) Accessible with standard software and ~~shall be backed up.~~

(2) Backed up

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 20:18:38 EST 2022
Committee: SIG-FUN

Public Input No. 513-NFPA 72-2022 [Section No. 7.5.7.1 [Excluding any Sub-Sections]]

For software-based systems, a copy of the site-specific software shall be provided to ~~the system owner or owner's designated representative.~~ authorized personnel only

Statement of Problem and Substantiation for Public Input

The definition for Authorized Personnel in Section 3.3.24 indicates: "The property owner, or designated representative appointed or selected by the property owner,,," The term "property owner" as indicated in 3.3.24 could also cover the term "system owner" and it also includes the designated person by the owner. Therefore, it is proposed to use a defined term to be consistent with the Code definitions. The word "only" is proposed to be added to clarify that only authorized personnel should have access to the site-specific software and not any other personnel.

Submitter Information Verification

Submitter Full Name: Sagiv Weiss-Ishai
Organization: San Francisco Fire Department
Affiliation: SFFD
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 19:38:34 EDT 2022
Committee: SIG-FUN

Public Input No. 89-NFPA 72-2022 [New Section after 7.5.8.3]

7.5.8.4

Verification for new supervising stations, the verification shall comply with both of the following:

(1) Ascertain proper arrangement, transmission, and receipt of all signals required to be transmitted off-premises

(2) Installation to meet the requirements of 14.4.1 and 14.4.2

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items. The original paragraph list items (1),(2), and (5) were kept in the first paragraph in PI-88. Since Paragraphs (3) and (4) contained multiple requirements, they were split out into their own sections with lists for them. This PI is the (3) with a list for the 2 requirements. PI-89 is for (4).

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 87-NFPA 72-2022 [Section No. 7.5.8.3]	Moving (3) of original text to a new section with list

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 15:21:57 EST 2022
Committee: SIG-FUN

Public Input No. 90-NFPA 72-2022 [New Section after 7.5.8.3]

7.5.8.5

Verification on existing supervising station systems that are extended, modified, or reconfigured shall comply with both of the following:

(1) Ascertain proper arrangement, transmission, and receipt of all signals required to be transmitted off-premises for the new work only

(2) Complete reacceptance testing in accordance with Chapter 14

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items. The original paragraph list items (1),(2), and (5) were kept in the first paragraph in PI-88. Since Paragraphs (3) and (4) contained multiple requirements, they were split out into their own sections with lists for them. PI-89 is for (3). This PI is for (4) with a list for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 87-NFPA 72-2022 [Section No. 7.5.8.3]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 15:53:44 EST 2022
Committee: SIG-FUN

Public Input No. 87-NFPA 72-2022 [Section No. 7.5.8.3]

7.5.8.3

Verification shall ensure that:

(1) All components and functions are installed and operate per the approved plans and sequence of operation.

(2) All required system documentation is complete and is archived on site.

(3) ~~For new supervising station systems, the verification shall also ascertain proper arrangement, transmission, and receipt of all signals required to be transmitted off-premises and shall meet the requirements of 14.4.1 and 14.4.2 .~~

(4) ~~For existing supervising station systems that are extended, modified, or reconfigured, the verification shall be required for the new work only, and reacceptance testing in accordance with Chapter 14 shall be acceptable.~~

(5) Written confirmation has been provided that any required corrective actions have been completed.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items. The original paragraph list items (1),(2), and (5) were kept in the first paragraph. Since Paragraphs (3) and (4) contained multiple requirements, they were split out into their own sections with lists for them. See PI-88 and PI-89 for those.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 89-NFPA 72-2022 [New Section after 7.5.8.3]	
Public Input No. 90-NFPA 72-2022 [New Section after 7.5.8.3]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 20:24:45 EST 2022
Committee: SIG-FUN

Public Input No. 80-NFPA 72-2022 [Section No. 7.6.6]

7.6.6* Record of Inspection and Testing.

~~The record of all~~ All inspections, testing, and maintenance as required by 14.6.2.4 shall be documented using ~~either the record of~~ an inspection and testing ~~forms, Figure 7.8.2(g) through Figure 7.8.2(l) , or an alternative record that includes all the applicable information shown in Figure 7.8.2(g) through Figure 7.8.2(l) .~~ record that includes, at a minimum, the results of all applicable visual inspection and/or testing methods outlined in Chapter 14.

Statement of Problem and Substantiation for Public Input

This PI is related to PI-67 and PI-81 proposing the relocation of the Inspection and Testing forms to the Annex. Therefore, the link to 7.8.2 has been removed and the connection to the true source of the form is strengthened by making reference to Chapter 14 rather than to the Inspection and Testing forms that were never intended to be mandated. Related PIs indicate those proposed changes to 7.8.2 as well as the relocation of the Inspection and Testing forms to an annex note related to Section 7.6.6. See further substantiation in PI 81.

The committee rejected a related PC last cycle stating that the Code already states in the Annex that the I&T is a sample form. That statement is true. However, the presence of the I&T form in the body of the Code as a sample is not correct. As a sample form, it belongs in the Annex. Its presence in the body of the Code is contradictory to the Code's intent and to the Annex note that the committee referenced in their previous substantiation. It belongs in the Annex. The concern of the committee over not having the form in Chapter 7 is not valid since it's still related to Chapter 7 by way of the annex note linked to 7.6.6.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 81-NFPA 72-2022 [New Section after A.7.7.1.2]	
Public Input No. 67-NFPA 72-2022 [Section No. 7.8.2]	
Public Input No. 67-NFPA 72-2022 [Section No. 7.8.2]	
Public Input No. 68-NFPA 72-2022 [Section No. A.7.8.2(2)]	
Public Input No. 81-NFPA 72-2022 [New Section after A.7.7.1.2]	

Submitter Information Verification

Submitter Full Name: Joe Scibetta
Organization: BuildingReports
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 16:40:58 EST 2022
Committee: SIG-FUN

Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]

7.7.1.3
Archiving of records by any means shall be permitted if hard copies of the records can be provided promplty when requested.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text in PI-91 removed the 2nd requirement. This PI adds a new paragraph for the 2nd requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 91-NFPA 72-2022 [Section No. 7.7.1.2]	directly related
Public Input No. 93-NFPA 72-2022 [Section No. 7.7.1.3]	
Public Input No. 94-NFPA 72-2022 [Section No. 7.7.1.4]	
Public Input No. 95-NFPA 72-2022 [Section No. 7.7.1.5]	
Public Input No. 96-NFPA 72-2022 [Section No. 7.7.1.6]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 16:02:15 EST 2022
Committee: SIG-FUN

Public Input No. 91-NFPA 72-2022 [Section No. 7.7.1.2]

7.7.1.2*

The records shall be available for examination and, if required, reported to the authority having jurisdiction. ~~Archiving of records by any means shall be permitted if hard copies of the records can be provided promptly when requested.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new paragraph for the 2nd requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 15:59:13 EST 2022
Committee: SIG-FUN

Public Input No. 93-NFPA 72-2022 [Section No. 7.7.1.3]

7.7.1.~~3~~ 4

If off-premises monitoring is provided, records of all signals, tests, and operations recorded at the supervising station, including the public emergency alarm reporting system, shall be maintained by the off-premise monitoring service provider for not less than 1 year unless more stringent requirements are required elsewhere in this Code.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new paragraph for the 2nd requirement. Due to the added paragraph, this paragraph will required renumbering.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 16:06:15 EST 2022
Committee: SIG-FUN

Public Input No. 94-NFPA 72-2022 [Section No. 7.7.1.4]

7.7.1.4 5

Required documents regarding system design and function shall be maintained for the life of the system.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new paragraph for the 2nd requirement. Due to the added paragraph, this paragraph requires renumbering

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]	Directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 16:08:46 EST 2022
Committee: SIG-FUN

Public Input No. 95-NFPA 72-2022 [Section No. 7.7.1.5]

7.7.1.~~5~~ – 6 .

The emergency communications system and fire alarm system as-built plans and other related documentation shall be permitted to be maintained together, including the appearance of both systems on the same drawings.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new paragraph for the 2nd requirement, which requires renumbering of this section.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]	Directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 16:23:13 EST 2022
Committee: SIG-FUN

Public Input No. 96-NFPA 72-2022 [Section No. 7.7.1.6]

7.7.1.~~6~~ 7

Revisions and alterations to systems shall be recorded and records maintained with the original system design documents.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text adds a new paragraph for the 2nd requirement, which requires this paragraph to be renumbered.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 92-NFPA 72-2022 [New Section after 7.7.1.2]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 16:37:56 EST 2022
Committee: SIG-FUN

Public Input No. 97-NFPA 72-2022 [Section No. 7.7.2.3]

7.7.2.3*

All record documentation shall ~~be stored~~ comply with the following:

(1) Stored in the documentation cabinet~~. No record documentation shall be stored~~

(2) Not stored in the control unit~~.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 17:51:32 EST 2022
Committee: SIG-FUN

Public Input No. 370-NFPA 72-2022 [Chapter 8]

Chapter 8 ~~Reserved~~ ~~**Responsibility of the Owner or Designated Representative**~~

8.1 Scope

This chapter shall highlight owner requirements. It does not take the place of other parts of this code.

8.2 Owner requirements

The owner shall comply with all the following requirements:

(1) **The owner shall maintain the fire alarm system in accordance with Chapter 14.**

(2) **The owner shall maintain the documents and site-specific software provided by Chapter 7.**

(3) **The owner shall respond to impairment notifications per chapter 10.**

Statement of Problem and Substantiation for Public Input

Some owners may not be familiar with all requirements of NFPA 72. The purpose here is to further clarify their responsibility for the overall fire alarm and signaling system of an occupancy. Pointing to specific requirements of the document will allow the owner to have one reference point.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 10:17:01 EDT 2022
Committee: SIG-FUN

Public Input No. 462-NFPA 72-2022 [Chapter 8]

Chapter 8 ~~Reserved~~

Chapter 8 - Responsibility of the Owner or Designated Representative

8.1 Scope

This chapter shall highlight owner requirements. It does not take the place of other parts of this code.

8.2 Owner requirements

The owner shall comply with all the following requirements:

a) The owner shall maintain the fire alarm system in accordance with Chapter 14.

b) The owner shall maintain the documents and site-specific software provided by Chapter 7.

c) The owner shall respond to impairment notifications per chapter 10.

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_8-1_comments.docx		

Statement of Problem and Substantiation for Public Input

Some owners may not be familiar with all requirements of NFPA 72 and the purpose is to further clarify their responsibility for the overall fire alarm and signaling system of an occupancy. Pointing to specific requirements of the document will allow the owner to have one reference point.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 09:47:09 EDT 2022
Committee: SIG-FUN

Public Input No. 503-NFPA 72-2022 [Chapter 8]

Chapter 8 Reserved

8.1 Scope

This scope shall highlight owner requirements. It does not take the place of other parts of this code.

8.2 Owner requirements

The owner shall comply with all the following requirements:

a) The owner shall maintain the fire alarm system in accordance with Chapter 14,

b) The owner shall maintain the documents and site-specific software provided by Chapter 7,

c) The owner shall respond to impairment notifications per Chapter 10.

Statement of Problem and Substantiation for Public Input

Some owners may not be familiar with all requirements of NFPA 72 and the purpose is to further clarify their responsibility for the overall fire alarm and signaling system of an occupancy. Pointing to specific requirements of the document will allow the owner to have one reference point.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 15:25:55 EDT 2022
Committee: SIG-FUN

Public Input No. 377-NFPA 72-2022 [Section No. 10.3.1]

10.3.1*

Equipment ~~constructed and installed in conformity with this Code shall be listed~~ shall meet all of the following requirements:

a) Equipment shall be designed for the purpose for which it is used.

b) Equipment shall be listed as complying with one or more of the standards in Chapter 2.

c) Equipment shall be compatible for use with the system.

Statement of Problem and Substantiation for Public Input

The modified text clarifies the intended listing requirements. Products must be listed to compatible standards as identified in Chapter 2.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 378-NFPA 72-2022 [Section No. A.10.3.1]	

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:36:03 EDT 2022
Committee: SIG-FUN

Public Input No. 464-NFPA 72-2022 [Section No. 10.3.1]

10.3.1*

~~Equipment constructed and installed in conformity with this Code shall be listed~~

10.3.1 Equipment shall meet all of the following requirements:

a) Equipment shall be designed for the purpose for which it is used.

b) Equipment shall be listed as complying with one or more of the standards in Chapter 2.

c) Equipment shall be compatible for use with the system.

A10.3.1

Just noting that a piece of equipment is listed is not sufficient. Listing involves evaluation of the equipment to determine its suitability for a specific purpose for use. The evaluation is usually accomplished using product testing standards developed to demonstrate that specific performance requirements have been met. Many of these performance requirements are based on specific requirements in the Code and go far beyond requirements used only to demonstrate electrical safety.

While most equipment would be listed for fire alarm system use, some equipment may have a different listing. For example, routers and modems that may be used with some transmission methods in the signal transmission path between a protected premises and a supervising station might be listed as general communications equipment (see 26.6.3.12).

Equipment listings generally contain information pertaining to the permitted use, required ambient conditions, mounting orientation, voltage tolerances, compatibility, and so on. Equipment must be installed, tested, and maintained in conformance with the listing and the manufacturer's published instructions to meet the requirements of the Code. Conformance with the listing and the manufacturer's instructions has been a long-standing requirement, originating in the requirements of NFPA 70.

Another aspect to equipment listing is the compatibility with the other parts of the system. This is key as it is designed to ensure system functionality and reliability.

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_10-3-1_comments.docx		

Statement of Problem and Substantiation for Public Input

The text as modified further clarifies the intended listing requirements. Products must be listed to compatible standards as identified in Chapter 2.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)

Affiliation:	Automatic Fire Alarm Association (AFAA)
Street Address:	
City:	
State:	
Zip:	
Submittal Date:	Fri May 27 09:52:25 EDT 2022
Committee:	SIG-FUN

Public Input No. 504-NFPA 72-2022 [Section No. 10.3.1]

10.3.1*

Equipment constructed and installed in conformity with this Code shall be listed for the purpose for which it is used.

10.3.1 Equipment shall meet all of the following requirements:

a) Equipment shall be designed for the purpose for which it is used,

b) Equipment shall be listed as complying with one or more of the standards in Chapter 2,

c) Equipment shall be compatible for use with the system.

A10.3.1

Just noting that a piece of equipment is listed is not sufficient. Listing involves evaluation of the equipment to determine its suitability for a specific purpose for use. The evaluation is usally accomplished using product testing standards developed to demonstrate that specifc performance requirements have been met. Many of these performance requirements are based on specific requirements in the Code and go far beyond requirements used only to demonstrate slectrical safety.

While most equipment would be listed for fire alarm system use, some equipment may have a different listing. For example, routers and modems that may be used with some transmission methods in the signal transmission path between a protected premiises and a supervising station might be listed as general communications equipment (see 26.6.3.12).

Equipment listings generally contain information pertaining to the permitted use, required ambient conditions, mounting orientation, voltage tolerances, compatibility, and so on. Equipment must be installed, tested, and maintained in conformance with the listing and the manufacturer's published instructions to meet the requirements of the Code. Conformance with the listing and the manfacturer's instructions has been a long-standing requirement, originating in the requirements of NFPA 70.

Another aspect to equipment listing is the compatibility with the other parts of the system. This is key as it is designed to ensure system functionality and reliability.

Statement of Problem and Substantiation for Public Input

The text as modified further clarifies the intended listing requirements. Products must be listed to compatible standards as identified in Chapter 2.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 15:31:46 EDT 2022
Committee: SIG-FUN

Public Input No. 283-NFPA 72-2022 [Section No. 10.4.4]

10.4.4*

Unless ~~otherwise permitted~~ otherwise required by the authority having jurisdiction, control unit displays, visible indicators, or controls shall be mounted such that the distance to the highest switch, lamp, or textual display does not exceed 6 ft (1.8 m) above the finished floor, and the lowest switch, lamp, or textual display shall not be less than 15 in. (375 mm) above the finished floor.

Additional Proposed Changes

File Name	Description	Approved
low_panel_20220512154432.pdf	Example of Currently Permitted FACU mounting height.	

Statement of Problem and Substantiation for Public Input

The proposer of this Public Input again requests that the SIG-FUN consider my proposal to revise the permitted mounting height requirement for control unit displays, visible indicators or controls.

As stated in my previous attempts to have this requirement revised, the use of the word "permitted" does not carry the same power of enforcement for the AHJ as the word "required". An AHJ may "permit" the control unit displays, visible indicators or controls to be located at a user friendly height for firefighters but an installer is not "required" to mount the FACU and its control unit displays, visible indicators or controls at the height required by the AHJ. The attached picture shows a FACU, and its control unit displays, visible indicators or controls, mounted at a height that meets the requirements of 10.4.4 The current control unit displays, visible indicators or controls are located +/- 28-inches AFF. Based on 10.4.4 the entire panel could be lowered another +/- 13-inches and still be in compliance with the current code language.

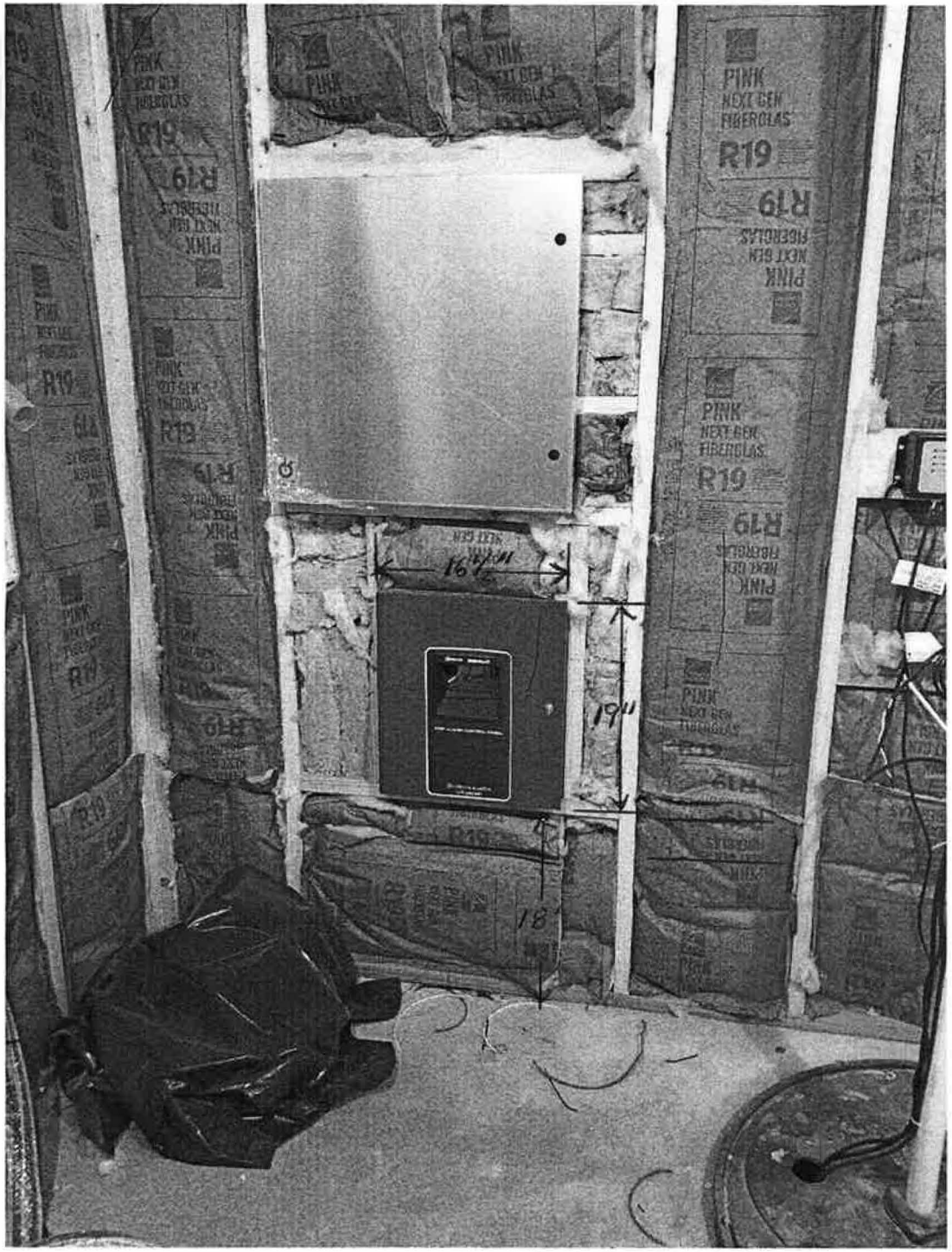
It should be clear from the picture that even at the current mounting height of the FACU, the viewability and operability of the control unit displays, visible indicators or controls is not ideal for firefighters. Now lower the FACU another 13-inches. The Annex material for 10.4.4 implies that the intent of the section is for the system owner and first responders. Clearly, the mounting height is not beneficial for first responders who would need to get on their hands and knees to view the display and operate the switches and controls.

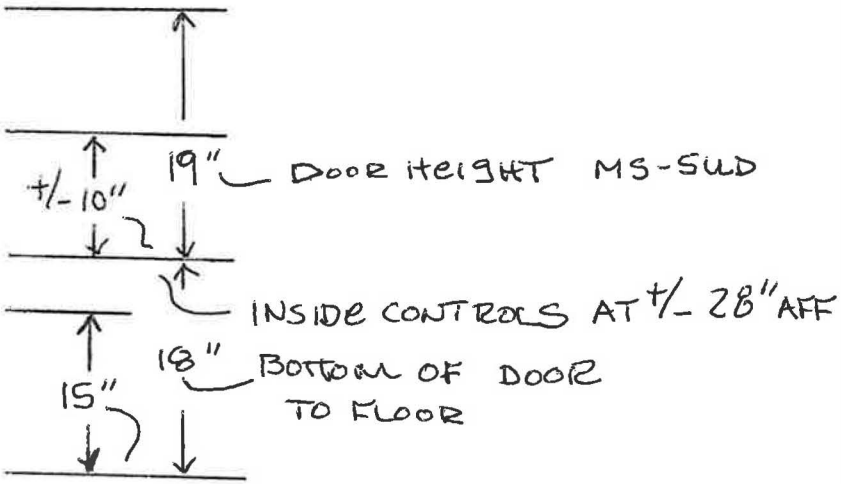
I request that the technical committee consider my proposed word change so AHJ's, if desired, could require a user friendly mounting height for control unit displays, visible indicators or controls.

Submitter Information Verification

Submitter Full Name: Warren Olsen
Organization: Fire Safety Consultants, Inc.
Affiliation: Illinois Fire Inspectors Association
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 13 11:31:01 EDT 2022

Committee: SIG-FUN





CODE PERMITTED LEVEL OF INSIDE CONTROLS - +/- 13" LOWER THAN THEY ARE IN THIS PICTURE. 10.4.4

Public Input No. 98-NFPA 72-2022 [Section No. 10.4.4]

10.4.4*

Unless otherwise permitted by the authority having jurisdiction, control unit displays, visible indicators, or controls shall be mounted ~~such that the~~ to comply with both of the following:

(1) The distance to the highest switch, lamp, or textual display does not exceed 6 ft (1.8 m) above the finished floor~~, and~~ .

(2) The distance to the lowest switch, lamp, or textual display ~~shall~~ is not ~~be less than~~ within 15 in. (375 mm) ~~above the~~ of the finished floor.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 17:53:58 EST 2022
Committee: SIG-FUN

Public Input No. 380-NFPA 72-2022 [Section No. 10.5.1.3]

10.5.1.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction

(3) ~~Manufacturer's certification~~ Certification by the manufacturer for the specific type and brand of the system provided

Statement of Problem and Substantiation for Public Input

Revised wording to be consistent with #2 and to clarify that certification by the manufacturer is specifically for the systems that the manufacturer provides.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:47:34 EDT 2022
Committee: SIG-FUN

Public Input No. 465-NFPA 72-2022 [Section No. 10.5.1.3]

10.5.1.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction

(3) ~~Manufacturer's certification for~~ ~~the~~ Certification by the manufacturer of the specific type and brand

~~of~~

(4) of the system provided

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_10-5-1-3_comments.docx		

Statement of Problem and Substantiation for Public Input

Revised the format to be consistent with (2) and to clarify that certification by a manufacturer is specifically for the systems that manufacturer provides.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 09:58:38 EDT 2022
Committee: SIG-FUN

Public Input No. 505-NFPA 72-2022 [Section No. 10.5.1.3]

10.5.1.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction
~~Manufacturer's certification for the~~

(3) Certification by the manufacturer of the specific type and brand of the system provided

Statement of Problem and Substantiation for Public Input

Revised the format to be consistent with (2) and to clarify that certification by a manufacturer is specifically for the systems that manufacturer provides.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 16:06:30 EDT 2022
Committee: SIG-FUN

Public Input No. 99-NFPA 72-2022 [Section No. 10.5.2.1]

10.5.2.1

Installation personnel shall be ~~qualified or shall be supervised~~ at least one of the following:

(1) Qualified

(2) Supervised by persons who are qualified in the installation, inspection, and testing of the systems~~.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:03:16 EST 2022
Committee: SIG-FUN

Public Input No. 382-NFPA 72-2022 [Section No. 10.5.2.3]

10.5.2.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction

(3) ~~Manufacturer's certification for the~~ Certification by the manufacturer of the specific type and brand of the system provided

Statement of Problem and Substantiation for Public Input

Revised wording format to be consistent with #2 and to clarify that certification by a manufacturer is specific to systems that the manufacturer provides.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:51:23 EDT 2022
Committee: SIG-FUN

Public Input No. 466-NFPA 72-2022 [Section No. 10.5.2.3]

10.5.2.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction

(3) ~~Manufacturer's certification for~~ ~~the~~ Certification by the manufacturer of the specific type and brand

~~of~~

(4) of the system provided

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_10-5-2-3_comments.docx		

Statement of Problem and Substantiation for Public Input

Revised the format to be consistent with (2) and to clarify that certification by a manufacturer is specifically for the systems that manufacturer provides.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 10:03:22 EDT 2022
Committee: SIG-FUN

Public Input No. 506-NFPA 72-2022 [Section No. 10.5.2.3]

10.5.2.3

Personnel shall provide documentation of their qualification by one or more of the following:

(1) Registration, licensing, or certification by a state or local authority

(2) Certification by an organization acceptable to the authority having jurisdiction

(3) ~~Manufacturer's certification for the~~ Certification by the manufacturer of the specific type and brand of the system provided

Statement of Problem and Substantiation for Public Input

Revised the format to be consistent with (2) and to clarify that certification by a manufacturer is specifically for the systems that manufacturer provides.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 16:10:41 EDT 2022
Committee: SIG-FUN

Public Input No. 101-NFPA 72-2022 [New Section after 10.5.3.2]

10.5.3.2.1

Testing personnel shall have knowledge and experience of the testing requirements contained in this Code, of the equipment being tested and of the test methods.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized two paragraphs for the two requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 100-NFPA 72-2022 [Section No. 10.5.3.2]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:07:59 EST 2022
Committee: SIG-FUN

Public Input No. 102-NFPA 72-2022 [New Section after 10.5.3.2]

10.5.3.2.2

Knowledge and experience of testing personnel shall be acceptable to the authority having jurisdiction or meet the requirement of 10.5.3.4

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 100-NFPA 72-2022 [Section No. 10.5.3.2]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:11:15 EST 2022
Committee: SIG-FUN

Public Input No. 100-NFPA 72-2022 [Section No. 10.5.3.2]

10.5.3.2* Testing Personnel.

~~Testing personnel shall have knowledge and experience of the testing requirements contained in this Code, of the equipment being tested, and of the test methods. That knowledge and experience shall be acceptable to the authority having jurisdiction or meet the requirement of 10.5.3.4 .~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text Provides two separate paragraphs for the two requirements in the section.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 101-NFPA 72-2022 [New Section after 10.5.3.2]	
Public Input No. 102-NFPA 72-2022 [New Section after 10.5.3.2]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:05:28 EST 2022
Committee: SIG-FUN

Public Input No. 104-NFPA 72-2022 [New Section after 10.5.3.3]

10.5.3.3.1

Service personnel shall have knowledge and experience of the maintenance and servicing requirements contained in this Code, of the equipment being serviced or maintained, and of the servicing or maintenance methods.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text provides 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 103-NFPA 72-2022 [Section No. 10.5.3.3]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:15:49 EST 2022
Committee: SIG-FUN

Public Input No. 105-NFPA 72-2022 [New Section after 10.5.3.3]

10.5.3.3.2

Knowledge and experience of service personnel shall be acceptable to the authority having jurisdiction or meet the requirement of 10.5.3.4.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 103-NFPA 72-2022 [Section No. 10.5.3.3]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:19:00 EST 2022
Committee: SIG-FUN

Public Input No. 103-NFPA 72-2022 [Section No. 10.5.3.3]

10.5.3.3 Service Personnel.

~~Service personnel shall have knowledge and experience of the maintenance and servicing requirements contained in this Code, of the equipment being serviced or maintained, and of the servicing or maintenance methods. That knowledge and experience shall be acceptable to the authority having jurisdiction or meet the requirement of 10.5.3.4 .~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 104-NFPA 72-2022 [New Section after 10.5.3.3]	
Public Input No. 105-NFPA 72-2022 [New Section after 10.5.3.3]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Thu Jan 20 18:14:25 EST 2022
Committee: SIG-FUN

Public Input No. 282-NFPA 72-2022 [New Section after 10.5.3.5.1]

10.5.3.5.2

If certification is not offered or required by the manufacturer, the requirements of 10.5.3.5.1 shall not apply.

Statement of Problem and Substantiation for Public Input

This proposal would move what is currently in A.10.5.3.5 from the appendix into the body of the code. There are many older systems that are still in operation across the country where the manufacturer no longer offers certification for programming. As many certifications expire over time, and as technicians retire, it is becoming more and more difficult to meet 10.5.3.5 for these older systems, and it will eventually become impossible to meet the requirement for these systems without requiring the building owner to pay for an upgrade or an entirely new system.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 343-NFPA 72-2022 [Section No. A.10.5.3.5]	

Submitter Information Verification

Submitter Full Name: Jason Dupuis
Organization: Cintas Fire Protection F19
Street Address:
City:
State:
Zip:
Submittal Date: Thu May 12 16:56:40 EDT 2022
Committee: SIG-FUN

Public Input No. 109-NFPA 72-2022 [New Section after 10.5.5.2]

10.5.5.2.1

Evidence of qualifications and/or certification shall be provided when requested by the authority having jurisdiction.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 108-NFPA 72-2022 [Section No. 10.5.5.2]	directly associated

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:28:26 EST 2022
Committee: SIG-FUN

Public Input No. 110-NFPA 72-2022 [New Section after 10.5.5.2]

10.5.5.2.2
A license or qualification listing shall be current in accordance with the requirements of the issuing authority or organization.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 108-NFPA 72-2022 [Section No. 10.5.5.2]	directly relates

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:31:07 EST 2022
Committee: SIG-FUN

Public Input No. 108-NFPA 72-2022 [Section No. 10.5.5.2]

10.5.5.2

Evidence of qualifications and/or certification~~. shall be provided when requested by the authority having jurisdiction .. A license or qualification listing shall be current in accordance with the requirements of the issuing authority or organization.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 109-NFPA 72-2022 [New Section after 10.5.5.2]	
Public Input No. 110-NFPA 72-2022 [New Section after 10.5.5.2]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:27:13 EST 2022
Committee: SIG-FUN

Public Input No. 112-NFPA 72-2022 [New Section after 10.5.6.4.3]

10.5.6.4.3.1

Evidence of qualifications and/or certification shall be provided when requested by the authority having jurisdiction.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 111-NFPA 72-2022 [Section No. 10.5.6.4.3]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:34:47 EST 2022
Committee: SIG-FUN

Public Input No. 113-NFPA 72-2022 [New Section after 10.5.6.4.3]

10.5.6.4.3.2

A license or qualification listing shall be current in accordance with the requirements of the issuing authority or organization.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 111-NFPA 72-2022 [Section No. 10.5.6.4.3]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:36:42 EST 2022
Committee: SIG-FUN

Public Input No. 497-NFPA 72-2022 [New Section after 10.5.6.4.3]

10.5.7 Gateway Reporting System Personnel Qualification.

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).

10.5.7.2.2

Personnel who are trained and certified for the specific type of public emergency alarm reporting 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

10.5.7.2.3

Evidence of qualifications and/or certification shall be provided when requested by the authority having jurisdiction. A license or qualification listing shall be current in accordance with the requirements of the issuing authority or organization.

Statement of Problem and Substantiation for Public Input

A new chapter for systems that pass through a gateway between a protected premise and a Public Safety Answering Point (PSAP) is being proposed. This PI is for the qualifications of those that would work within the gateway facility.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 495-NFPA 72-2022 [Chapter 25]	New Chapter on Gateways
Public Input No. 498-NFPA 72-2022 [New Section after 3.3.63]	New Definition
Public Input No. 499-NFPA 72-2022 [Section No. A.26.6.2.4]	Revised Exception
Public Input No. 501-NFPA 72-2022 [Section No. A.26.6.2.4]	New Fig.
Public Input No. 495-NFPA 72-2022 [Chapter 25]	
Public Input No. 498-NFPA 72-2022 [New Section after 3.3.63]	
Public Input No. 499-NFPA 72-2022 [Section No. A.26.6.2.4]	

Public Input No. 501-NFPA 72-2022 [Section No. A.26.6.2.4]

Submitter Information Verification

Submitter Full Name: Shane Clary
Organization: Bay Alarm Company
Affiliation: Bay Alarm Company
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 14:53:14 EDT 2022
Committee: SIG-FUN

Public Input No. 111-NFPA 72-2022 [Section No. 10.5.6.4.3]

10.5.6.4.3

Evidence of qualifications and/or certification~~.~~ ~~shall be provided when requested by the authority having jurisdiction~~ .~~ A license or qualification listing shall be current in accordance with the requirements of the issuing authority or organization.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 112-NFPA 72-2022 [New Section after 10.5.6.4.3]	
Public Input No. 113-NFPA 72-2022 [New Section after 10.5.6.4.3]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:33:39 EST 2022
Committee: SIG-FUN

Public Input No. 467-NFPA 72-2022 [Section No. 10.6.3.1]

10.6.3.1*

Power shall be supplied in ~~accordance~~ accordance ~~with~~ ~~either~~ ~~either~~ with 10.6.3.2 ~~or~~ ~~or~~ , 10.6. ~~4.~~ 4 or 23.16.2

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_10-6-3-1_and_10-6-3-2_comments.docx		

Statement of Problem and Substantiation for Public Input

Revised to include the use of primary batteries as the power supply for low-power radio (wireless) systems permitted by 23.16.2.

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 10:09:51 EDT 2022
Committee: SIG-FUN

Public Input No. 383-NFPA 72-2022 [Sections 10.6.3.1, 10.6.3.2]

Sections 10.6.3.1, 10.6.3.2

10.6.3.1*

Power shall be supplied in accordance with ~~either~~ 10.6.3.2 ~~or~~ , 10.6.4 or 23 . 16.2 .

10.6.3.2

Unless configured in compliance with 10.6.4 or 23.16.2 , at least two independent and reliable power supplies shall be provided, one primary and one secondary.

Statement of Problem and Substantiation for Public Input

Revised to include the use of primary batteries as the power supply for low-power radio (wireless) systems permitted by 23.16.2.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:55:31 EDT 2022
Committee: SIG-FUN

Public Input No. 507-NFPA 72-2022 [Sections 10.6.3.1, 10.6.3.2]

Sections 10.6.3.1, 10.6.3.2

10.6.3.1*

Power shall be supplied in accordance ~~with either~~ with 10.6.3.2 ~~or~~ , 10.6.4, or 23 . 16.2.

10.6.3.2

Unless configured in compliance with 10.6.4 ~~, at~~ or 23.16.2 at least two independent and reliable power supplies shall be provided, one primary and one secondary.

Statement of Problem and Substantiation for Public Input

Revised to include the use of primary batteries as the power supply for low-power radio (wireless) systems permitted by 23.16.2.

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 16:13:54 EDT 2022
Committee: SIG-FUN

Public Input No. 555-NFPA 72-2022 [New Section after 10.6.5.1.2]

Sprinkler Bell

The dedicated power for the fire alarm system shall be allowed to power the sprinkler suppression system bell or other notification appliance.

...

Statement of Problem and Substantiation for Public Input

The 120 VAC sprinkler bell that is required by others may be powered by the same dedicated branch circuit that provides power to the FACU and/or remote power supply. This is intended to keep the cost down for the building owner.

Submitter Information Verification

Submitter Full Name: Shane Clary
Organization: Bay Alarm Company
Affiliation: Bay Alarm Company
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 31 23:37:18 EDT 2022
Committee: SIG-FUN

Public Input No. 514-NFPA 72-2022 [Section No. 10.6.5.2.5]

10.6.5.2.5

The circuit disconnecting means shall only be accessible ~~only to authorized~~ to service, emergency or authorized personnel.

Statement of Problem and Substantiation for Public Input

The circuit disconnecting means should also be accessible to Service Personnel or emergency personnel and not only to authorized personnel.
Service and Emergency personnel are Specifically defined terms in chapter 3 and they are not included under the authorized personnel definition. Therefore, this section is proposed to be expanded to include additional access to the disconnecting means by Service Personnel or Emergency Personnel.

Submitter Information Verification

Submitter Full Name: Sagiv Weiss-Ishai
Organization: San Francisco Fire Department
Affiliation: SFFD
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 19:52:26 EDT 2022
Committee: SIG-FUN

Public Input No. 114-NFPA 72-2022 [Section No. 10.6.7.2.17]

10.6.7.2.17

Where carbon monoxide detection is monitored by a supervising station, the secondary power supply shall have sufficient capacity ~~to operate the~~ for both of the following:

(1) Operate the carbon monoxide detection system under quiescent load (system operating in a nonalarm condition) for a minimum of 24 hours~~ and, at~~

(2) At the end of ~~that period, shall be~~ the 24 hours, be capable of operating the carbon monoxide detection system and all notification appliances for 5 minutes.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized listed items in accordance with MOS section 3.3.1 Listed Items.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:39:27 EST 2022
Committee: SIG-FUN

Public Input No. 488-NFPA 72-2022 [New Section after 10.6.8.5]

10.6.8.6* Power sources for remotely located equipment that are listed to UL 864, shall be acceptable for use for by the following listed life safety systems: Mass Notification Systems (MNS), Smoke Control Systems, Two-Way In-Building Wired Emergency Services Communications Systems, Two-Way Radio Communications Enhancement Systems, and Two-Way Emergency Communications Systems for Rescue Assistance, when specifically specified for use by the manufacturer of specific listed life safety systems.

A.10.6.8.6 Power sources for remote equipment may power devices servicing more than one type of listed life safety system, or devices servicing different life safety systems connected to a common network. For example, a UL 864 listed UPS may provide dedicated secondary power for a mix of listed life safety system devices (speakers, amplifiers, strobes, and other devices) distributed across a common network. By providing a common listing (UL 864) that can support service power requirements for other life safety system, listed to different life safety standards, a more commercially viable means of establishing safety and reliability is supported.

Statement of Problem and Substantiation for Public Input

Most UL life safety standards are derived from UL 864 as a gold standard for system design. However, it is impractical, time consuming, and costly for manufactures of power supplies to submit power sourcing products intended for general life safety system use, against all life safety system standards. A power source that is deemed safe enough (fire and shock) and reliable enough for a fire alarm system, has already passed testing necessary to utilize it for similar protection of life and property purposes. By creating a common listing option, unnecessary administrative overhead can be reduced, saving time and money. In this era of increasing regulations and challenging global supply chain challenges, consolidation of common regulations and administration improvements the availability of quality life safety equipment, which improves life safety overall.

Submitter Information Verification

Submitter Full Name: Michael Pallett
Organization: Pallett Corner Consulting
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 08:16:07 EDT 2022
Committee: SIG-FUN

Public Input No. 489-NFPA 72-2022 [New Section after 10.6.8.5]

10.6.8.7* Power sources for remotely located equipment, not listed to UL 864 shall be acceptable for use by the following listed life safety systems: Fire Alarm Systems, Evacuation Voice Fire Alarm Systems (EVAC), Mass Notification Systems (MNS), Smoke Control Systems, Two-Way In-Building Wired Emergency Services Communications Systems, Two-Way Radio Communications Enhancement Systems, and Two-Way Emergency Communications Systems for Rescue Assistance, when complying with all the following conditions:

(1) The specific power source and its use is specified by the listed life safety system manufacturer for specific listed life safety systems

(2) Power sources are listed to UL60950, UL60065, UL1310, or UL62368-1, or other standards acceptable to the authority having jurisdiction

(3) Power sources are dedicated for use with only listed life safety systems

(4) The system manufacture provides a risk analysis qualitatively or quantitatively identifying the risks, likelihoods, impacts & consequences, controls, and mitigations in accordance with 10.6.8.7.1

(5) Power source use is acceptable to the authority having jurisdiction based on the system manufacturer risk analysis

(6) Residual risks are accepted in writing by the facilities governing body (owners), permitting the installation of non-UL 864 listed power sources for life safety purposes.

A.10.6.8.7 It is not always commercially viable to list reliable infrastructure equipment to specific life safety standards. For example, a commercially available Power over Ethernet switch may meet all conditions required by a life safety standard, but not be listed because the market is too limited to support the costs associated with obtaining and maintaining the listing. Alternative approaches are required because: (1) supply chain challenges exist, (2) new models and technologies are rapidly brought to market with comparatively short product lifecycles (as compared to lifecycles of many life safety systems), (3) the potential number of combinations between customer preferred manufactures and models of equipment and various life safety systems is large, (4) the time and cost to obtain specific standard listings for specific makes and models is high, and (5) maintaining availability of specific third-party equipment makes and models over the life cycle of a life safety system is challenging or impossible.

It is important that any equipment that is considered for deployment as part of a life safety system infrastructure is vetted by the manufacturer of the life safety system for compatibility and a low risk of system compromise. That includes insuring that such equipment is listed for fire and shock safety, and that power sources are dedicated for life safety system use, and not shared with other potentially unlisted systems.

It is also important that after any risks have been identified, and all controls intended to reduce the risk are considered, that any residual risk is clearly identified and accepted by the system owner, and authority having jurisdiction. An example may be equipment that is used at a high altitude, may have its load capped at a reduced factor as a control to compensate for the environmental condition imposed. However, due to operation at higher altitude, the life expectancy of the equipment may still be reduced, and the stakeholders will need to accept that risk.

10.6.8.7.1* Power source risk analysis shall at a minimum identify risks based on the following considerations, in relation to any applicable corresponding requirements of UL 864:

(1) Accidental disconnection of power source from mains and accidental disconnection(s) to powered device(s)

(2) Method and security of connection to mains and backup power

(3) Methods of monitoring power supply for integrity

(4) Power source compromise due to a fan failure

(5) Power source damage due to jarring & impact

(6) Power sources with a mean time between failure (MTBF) of less than 100,000 hours

(7) Power source failure due to field wiring faults (short circuit and short to ground)

(8) Power source operation at ambient temperatures above or below manufactures environmental requirements

(9) Power source operation at humidity levels above or below manufactures environmental requirements

(10) Power supply operation at the facilities altitude (relative to sea level)

(11) Power supply operation with mains under voltages (below 85%), or over voltages (above 115%)

(12) Power source immunity to power mains supply transients of 2400V (80us) or less

(13) Power sources with a dielectric withstand voltage of less than 1,000 VAC or 1,414 VDC.

A.10.6.8.7.1 Power source equipment, designed and tested by the manufacturer to meet the listing requirements of UL 60950, UL 60065, UL 1310, or UL 62368-1, may also meet, or exceed the requirements of life safety standards, without ever being listed to those standards. However, established equipment manufactures that produce known reliable equipment often publish specifications that shows performance in relation to life safety standards such as UL 864. In conducting a risk analysis, consideration should focus on risks associated with product performance required by UL 864, but not required by the listed standard the product is tested to.

For example, in consideration of overall reliability, MFBF of 100,000 hours is consistent with requirements in UL 864 for use of hard drives in a fire alarm system. Also, since UL 864 references jarring, impact and fan failure, these life safety system requirements need to be considered in a risk analysis for life safety system use. Potentially additional risk mitigation such as specified enclosures may be applied to reduce risk of accidental damage due to impact of jarring.

Statement of Problem and Substantiation for Public Input

It is not always commercially viable to list safe and reliable third-party equipment to all applicable life safety standards. There is a great deal of administrative overhead, fees, and time required to secure, and then maintain UL life safety listings for third-party products. Manufactures who undertake such ventures can be forced to purchase large inventories of third-party products, to protect the investment in obtaining the UL listing. Stockpiles are also used to maintain availability of the specific UL listed version of a product, for the time when the product has become obsolete and replaced with a newer more advanced model, or just otherwise unavailable due to challenges in the supply chain.

For example, look at the Ethernet switches provided by Johnson Controls for their Metasys Smoke Control systems. In the document entitled: Metasys® System UL 864 10th Edition UUKL/ORD-C100-13 UUKLC Smoke Control System, updated July 15, 2020, it references Cisco Catalyst 2960 and Asante NU-RJ45SW1-0U which are no longer available for ordering. Then it references 24-Port Ethernet Switch: Cisco IE 4010-4S24P and related power supplies. Then the 16-Port Ethernet Switch: Cisco IE 4000-16T4G-E, and related power supplies. Then it references 5-Port Ethernet Switches: Contemporary Controls® CTRLink™ EISK5-100T, which is no longer available at release 8.1. All of these were UL 864 listed. Then it references Netgear FS105 5-Port Copper Switch, which is not required to be UL listed. Then it referenced 8-Port Ethernet Switch: Contemporary Controls® CTRLink™ EIS8-100T, which are UL 864 listed. Then it references 4-Port Ethernet Switch: Contemporary Controls CTRLink EIS6-100T/FT which is UL 864 listed. Then it references Single-Port Media Converter: Contemporary Controls® EIMK-100T/FT, which is UL Listed.

Obviously, this is complex for Johnson Controls and its customers. In most cases, Johnson Control supplies the products (that are still available, or available due to Johnson Controls pre-purchased

stockpiles), with additional enhancements, such as mounting and enclosures consistent with UL 864 requirements. Frequently Johnson Controls includes disclaimers that technical specifications of the third-party are subject to change with out notice, and warnings not to purchase product from third-party vendors but only from Johnson Controls. This demonstrates the risk assessment process already in action at Johnson Controls, and similar top-tier companies.

The potential to modernize life safety system equipment to available and established technologies is, in part, hampered by the commercial necessity to develop advanced technologies for applications across the entire marketplace. Responsible manufactures of already listed life safety systems such as Johnson Controls, are already doing the risk analysis work to utilize some of these advanced technologies. But the management overhead costs associated with obtaining and maintaining third-party equipment listings for a comparatively narrow vertical market, with increasingly complex customer demands, especially in times of supply chain upheaval, negatively impact the advancement and availability of solutions.

This risk analysis option would allow manufactures of listed life safety equipment to efficiently review and apply third party technologies that are needed to support availability and bring more advanced functionality to the market. For example, a system of devices supported on a Class N network and powered by Power over Ethernet (PoE) switches can bring forward new technological innovation if the deployment infrastructures can be more quickly, efficiently, and effectively evaluated and realized. This option will lower barriers for utilizing newer advanced technology by lowering cost compared to UL submissions based on each specific model of component and minor variation of component, especially as product availability changes over time.

It is often argued that it is a significant challenge for codes and standard on multi-year version cycles to keep pace with technological advancement. This proposal attempts to address one small aspect of this challenge.

Submitter Information Verification

Submitter Full Name: Michael Pallett
Organization: Pallett Corner Consulting
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 08:26:51 EDT 2022
Committee: SIG-FUN

Public Input No. 185-NFPA 72-2022 [Section No. 10.6.9.1.6]

10.6.9.1.6

Monitoring shall not be required for the output of an engine-driven generator that is part of the secondary power supply, provided the generator is tested ~~weekly in~~ monthly in accordance with Chapter 14.

Statement of Problem and Substantiation for Public Input

Section 10.6.9.1.6 is inconsistent with Chapter 14 of NFPA 72 & NFPA 110. Section 10.6.9.1.6 requires generators to be tested weekly to avoid monitoring by the fire alarm system. Chapter 14 of NFPA 72 requires generators to be tested monthly, not weekly. NFPA 110 Section 8.4.1 requires weekly inspections and monthly testing. NFPA 110 Section A.8.4.1 discourages weekly testing due to long-term problems such as wet stacking. The proposed change aligns Section 10.6.9.1.6 with Chapter 14 of NFPA 72 and NFPA 110.

Submitter Information Verification

Submitter Full Name: Laura Jacobsen
Organization: The Boeing Company
Street Address:
City:
State:
Zip:
Submittal Date: Thu Mar 10 11:39:12 EST 2022
Committee: SIG-FUN

Public Input No. 252-NFPA 72-2022 [Section No. 10.6.10.1.3]

10.6.10.1.3*

~~Effective January 1, 2024, rechargeable~~ Rechargeable batteries for ~~the~~ secondary power ~~supply~~ supplies used in control units, ~~devices,~~ NAC extender panels, power supplies, data gathering panels, devices, and accessories shall be listed or component recognized by a nationally recognized testing laboratory.

Statement of Problem and Substantiation for Public Input

The effective date needs to be removed. Further clarification that remote power supplies, NAC panels, etc. are also included in this requirement.

Submitter Information Verification

Submitter Full Name: Rodger Reiswig
Organization: Johnson Controls
Street Address:
City:
State:
Zip:
Submittal Date: Wed Apr 27 15:21:35 EDT 2022
Committee: SIG-FUN

Public Input No. 116-NFPA 72-2022 [New Section after 10.6.11.7.1]

10.6.11.7.2

The separate storage battery and separate automatic charger shall not be used for any other purpose.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 115-NFPA 72-2022 [Section No. 10.6.11.7.1]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:49:43 EST 2022
Committee: SIG-FUN

Public Input No. 115-NFPA 72-2022 [Section No. 10.6.11.7.1]

10.6.11.7.1

A separate storage battery and separate automatic charger shall be provided for starting the engine-driven generator~~ and shall not be used for any other purpose~~ .

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 116-NFPA 72-2022 [New Section after 10.6.11.7.1]	
Public Input No. 117-NFPA 72-2022 [Section No. 10.6.11.7.2]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Associations (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:48:02 EST 2022
Committee: SIG-FUN

Public Input No. 117-NFPA 72-2022 [Section No. 10.6.11.7.2]

10.6.11.7.~~2~~ 3

The battery shall be sized in accordance with 5.6.4 of NFPA 110.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, then this paragraph required renumbering.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 115-NFPA 72-2022 [Section No. 10.6.11.7.1]	Directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:52:40 EST 2022
Committee: SIG-FUN

Public Input No. 119-NFPA 72-2022 [New Section after 10.10.4]

10.11.4.1

An audible notification appliance on a control unit, on multiple control units that are interconnected to form a system, or at a remote location, shall be permitted to have the same audible characteristics for all alerting functions.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 118-NFPA 72-2022 [Section No. 10.10.4]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:56:56 EST 2022
Committee: SIG-FUN

Public Input No. 120-NFPA 72-2022 [New Section after 10.10.4]

10.10.4.2

The audible notification appliance described in 10.10.4.1 is not limited to alarm, trouble, and supervisory, provided that the distinction between signals shall be by other means.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 118-NFPA 72-2022 [Section No. 10.10.4]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:01:27 EST 2022
Committee: SIG-FUN

Public Input No. 118-NFPA 72-2022 [Section No. 10.10.4]

10.10.4*

~~An audible notification appliance on a control unit, on multiple control units that are interconnected to form a system, or at a remote location, shall be permitted to have the same audible characteristics for all alerting functions including, but not limited to, alarm, trouble, and supervisory, provided that the distinction between signals shall be by other means~~ Audible Characteristics .

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 119-NFPA 72-2022 [New Section after 10.10.4]	
Public Input No. 120-NFPA 72-2022 [New Section after 10.10.4]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 14:55:02 EST 2022
Committee: SIG-FUN

Public Input No. 122-NFPA 72-2022 [New Section after 10.10.5]

10.10.5.1

Supervisory signals shall be distinctive in sound from other signals.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 121-NFPA 72-2022 [Section No. 10.10.5]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:06:26 EST 2022
Committee: SIG-FUN

Public Input No. 123-NFPA 72-2022 [New Section after 10.10.5]

10.10.5.2

Supervisory signals sound shall not be used for any other purpose except as permitted in 10.10.4.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 121-NFPA 72-2022 [Section No. 10.10.5]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:27:36 EST 2022
Committee: SIG-FUN

Public Input No. 121-NFPA 72-2022 [Section No. 10.10.5]

10.10.5*

Supervisory signals ~~shall be distinctive in sound from other signals, and their sound shall not be used for any other purpose except as permitted in 10~~ . ~~10.4.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 122-NFPA 72-2022 [New Section after 10.10.5]	
Public Input No. 123-NFPA 72-2022 [New Section after 10.10.5]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:04:48 EST 2022
Committee: SIG-FUN

Public Input No. 125-NFPA 72-2022 [New Section after 10.10.6]

10.10.6.1

Trouble signals required to indicate at the protected premises shall be indicated by distinctive audible signals.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 124-NFPA 72-2022 [Section No. 10.10.6]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:33:03 EST 2022
Committee: SIG-FUN

Public Input No. 126-NFPA 72-2022 [New Section after 10.10.6]

10.10.6.2

Trouble signals described in 10.10.6.1 shall be distinctive from alarm signals.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 124-NFPA 72-2022 [Section No. 10.10.6]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:36:20 EST 2022
Committee: SIG-FUN

Public Input No. 127-NFPA 72-2022 [New Section after 10.10.6]

10.10.6.3

Trouble signals described in 10.1.6.1 shall be permitted to be used for other purposes as permitted in 10.10.4.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 124-NFPA 72-2022 [Section No. 10.10.6]	Directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:38:53 EST 2022
Committee: SIG-FUN

Public Input No. 124-NFPA 72-2022 [Section No. 10.10.6]

10.10.6

Trouble signals ~~required to indicate at the protected premises shall be indicated by distinctive audible signals, which shall be distinctive from alarm signals except as permitted in 10~~ . ~~10.4.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 125-NFPA 72-2022 [New Section after 10.10.6]	
Public Input No. 126-NFPA 72-2022 [New Section after 10.10.6]	
Public Input No. 127-NFPA 72-2022 [New Section after 10.10.6]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:30:21 EST 2022
Committee: SIG-FUN

Public Input No. 129-NFPA 72-2022 [New Section after 10.10.7]

10.10.7.1

Alarm evacuation signals shall be distinctive in sound from other signals.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 128-NFPA 72-2022 [Section No. 10.10.7]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:44:58 EST 2022
Committee: SIG-FUN

Public Input No. 130-NFPA 72-2022 [New Section after 10.10.7]

10.10.7.2
Alarm evacuation signals shall comply with the requirements of 18.4.2.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 128-NFPA 72-2022 [Section No. 10.10.7]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:47:23 EST 2022
Committee: SIG-FUN

Public Input No. 131-NFPA 72-2022 [New Section after 10.10.7]

10.10.7.3

Alarm evacuation signals described in 10.10.7.1 and 10.10.7.2 shall not be used for any other purpose.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 128-NFPA 72-2022 [Section No. 10.10.7]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:49:18 EST 2022
Committee: SIG-FUN

Public Input No. 128-NFPA 72-2022 [Section No. 10.10.7]

10.10.7

Alarm evacuation signals ~~shall be distinctive in sound from other signals, shall comply with the requirements of 18~~ . ~~4.2, and their sound shall not be used for any other purpose.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 3 separate paragraphs for the 3 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 129-NFPA 72-2022 [New Section after 10.10.7]	
Public Input No. 130-NFPA 72-2022 [New Section after 10.10.7]	
Public Input No. 131-NFPA 72-2022 [New Section after 10.10.7]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:43:44 EST 2022
Committee: SIG-FUN

Public Input No. 133-NFPA 72-2022 [New Section after 10.10.8]

10.10.8.1
Pre-alarm signals shall be distinctive in sound from other signals.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 132-NFPA 72-2022 [Section No. 10.10.8]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:53:28 EST 2022
Committee: SIG-FUN

Public Input No. 134-NFPA 72-2022 [New Section after 10.10.8]

10.10.8.2

Pre-alarm signals described in 10.10.8.1 shall not be used for any other purpose except as permitted in 10.10.4.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 132-NFPA 72-2022 [Section No. 10.10.8]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:55:04 EST 2022
Committee: SIG-FUN

Public Input No. 132-NFPA 72-2022 [Section No. 10.10.8]

10.10.8

Pre-alarm signals ~~shall be distinctive in sound from other signals, and their sound shall not be used for any other purpose except as permitted in 10~~ . ~~10.4.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 133-NFPA 72-2022 [New Section after 10.10.8]	
Public Input No. 134-NFPA 72-2022 [New Section after 10.10.8]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:51:41 EST 2022
Committee: SIG-FUN

Public Input No. 255-NFPA 72-2022 [Section No. 10.12.2]

10.12.2*

When an occupant notification alarm signal deactivation means is actuated, both audible and visual notification appliances shall be simultaneously deactivated.

Delete section or require notification appliances on the exterior and that they remain active until system is reset.

Statement of Problem and Substantiation for Public Input

The justification for original inclusion of the code language is flawed. Saying that a mixed message would be provided to those with a visual impairment therefore, we need to equally send that mixed message to everyone is not a valid reason to not allow the audible to be silenced and facilitate better fire ground operations.

Submitter Information Verification

Submitter Full Name: William Sullivan
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Thu Apr 28 08:47:25 EDT 2022
Committee: SIG-FUN

Public Input No. 352-NFPA 72-2022 [Section No. 10.14.7.4]

10.14.7.4

Subsequent activation of supervisory initiating devices in other building zones shall cause supervisory notification appliances to activate as required by the ~~system input~~ sequence of operation provided in narrative form, a logic diagram or an input input /output matrix.

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 16:17:03 EDT 2022
Committee: SIG-FUN

Public Input No. 189-NFPA 72-2022 [New Section after 10.15.9.2]

TITLE OF NEW CONTENT

10.15.9.2 Reactivation of the audible and visible trouble signal shall not be required for supervising station alarm system installed in compliance with Chapter 26.

Statement of Problem and Substantiation for Public Input

Reactivation of the local audible and visible trouble signal every 24 hours as a reminder that the fire alarm system remains in a fault condition is not always necessary.

Some fire panels are provided with a trouble acknowledge notification that will continuously activate throughout a 24-hour period. For example, one manufacturer's trouble reactivation programming options all require a 60 second acknowledgement resound such that once the trouble is acknowledged at the panel for the first time, the panel automatically provides one chirp of the piezo and one blink of the trouble LED every 60 seconds for 24 hours. At 11:00 am each day the trouble signal will come back in until its acknowledged again and the cycle repeats. Panels with these limited options could potentially be installed in critical communication areas such as control rooms, hospitals, fire departments, etc.

Chapter 26 requires supervising stations to communicate immediately with designated person(s) to ascertain the reason for a trouble signal and to dispatch personnel to arrive within 4 hours to initiate maintenance, if necessary. The Chapter also requires supervising station fire alarm systems to report restoral signals to the supervising station of all alarm, supervisory, and trouble signals upon restoration of the activation. For any signal received by the supervising station that has not restored to normal condition within 24 hours of initial receipt, Chapter 26 requires that the signal is to be redisplayed to an operator as a non-restored signal and reported to the subscriber.

The requirements of Section 26.4.6.1.6.4, Trouble Signals, ensure that unrestored trouble signals for supervising station alarm systems are continuously reported to the owner, subscriber or designated person. The building occupant(s) often are not the owner or those responsible for the system, who need reminding that the system is in a fault condition. Occupants of the building may not have authorization to initiate service and must cope with a continuous interruption to business.

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Affiliation: DOE SAVANNAH RIVER SITE
Street Address:
City:
State:
Zip:
Submittal Date: Tue Mar 22 16:29:48 EDT 2022
Committee: SIG-FUN

Public Input No. 190-NFPA 72-2022 [Section No. 10.15.9.2]

10.15.9.~~2~~ 3

The audible and visible trouble signal associated with signaling the depletion or failure of the primary battery of a wireless system as required by 23.16.2.1 and 23.16.2.2 shall automatically resound every 4 hours or less until the depletion signal is restored to normal.

Statement of Problem and Substantiation for Public Input

Renumber Section 10.15.9.2 to 10.15.9.3 due to addition of adding new text within Section 10.15.9.2 per 189-NFPA 72-2025.

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Affiliation: DOE SAVANNAR RIVER SITE
Street Address:
City:
State:
Zip:
Submittal Date: Wed Mar 23 08:13:26 EDT 2022
Committee: SIG-FUN

Public Input No. 353-NFPA 72-2022 [Section No. 10.15.10.5]

10.15.10.5

Subsequent trouble signals shall cause trouble notification appliances to activate as required by the ~~system~~ sequence of operation provided in narrative form, a logic diagram, or an input/output matrix.

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 16:28:30 EDT 2022
Committee: SIG-FUN

Public Input No. 136-NFPA 72-2022 [New Section after 10.21.1]

10.21.2
Impairments to systems shall include out-of-service events.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, then renumber subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:00:56 EST 2022
Committee: SIG-FUN

Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]

10.21.1

The system owner or the owner's designated representative shall be notified when a system or part thereof is impaired. ~~Impairments to systems shall include out-of-service events.~~

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, then renumber subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 136-NFPA 72-2022 [New Section after 10.21.1]	
Public Input No. 137-NFPA 72-2022 [Section No. 10.21.2]	
Public Input No. 138-NFPA 72-2022 [Section No. 10.21.3]	
Public Input No. 139-NFPA 72-2022 [Section No. 10.21.4]	
Public Input No. 141-NFPA 72-2022 [Section No. 10.21.5]	
Public Input No. 143-NFPA 72-2022 [Section No. 10.21.6]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 15:57:57 EST 2022
Committee: SIG-FUN

Public Input No. 572-NFPA 72-2022 [Section No. 10.21.1]

10.21.1

The system owner or the owner's designated representative shall be notified in writing within 8 hours when a system or part thereof is impaired. Impairments to systems shall include out-of-service events.

Statement of Problem and Substantiation for Public Input

Added additional text to clarify the importance of reporting system Impairments. Deficiencies must be reported to the Owner within 24 hours and in writing, but Impairments are required to be reported to the Owner but no requirement exists for the notification to be in writing or within a certain amount of time. This language would better match the requirements of section 14.2.2.2 and 14.2.2.3.2. An out of service impairment must be reported to the AHJ within 8 hours per 10.21.4, so it makes sense that the Owner would be notified within this time period as well.

Submitter Information Verification

Submitter Full Name: Larry Rietz
Organization: Jensen Hughes
Street Address:
City:
State:
Zip:
Submittal Date: Wed Jun 01 15:06:38 EDT 2022
Committee: SIG-FUN

Public Input No. 137-NFPA 72-2022 [Section No. 10.21.2]

10.21.2~~.2~~ 3

A record of the impairments shall be maintained by the system owner or the owner's designated representative for a period of 1 year from the date the impairment is corrected.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, then renumber the subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:04:40 EST 2022
Committee: SIG-FUN

Public Input No. 138-NFPA 72-2022 [Section No. 10.21.3]

10.21.3 ~~–~~ 4 .

The supervising station shall report to the authority having jurisdiction any system for which required monitoring has been terminated.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, subsequent paragraphs require renumbering.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:07:08 EST 2022
Committee: SIG-FUN

Public Input No. 139-NFPA 72-2022 [Section No. 10.21.4]

10.21.4 5 *

The service provider shall report to the authority having jurisdiction any system that is out of service for more than 8 hours.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, thus renumbering the subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related
Public Input No. 140-NFPA 72-2022 [Section No. A.10.21.4]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:09:13 EST 2022
Committee: SIG-FUN

Public Input No. 141-NFPA 72-2022 [Section No. 10.21.5]

10.21.5 ~~5~~ 6 *

Where required by the authority having jurisdiction, mitigating measures shall be implemented for the period that the system is impaired.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, subsequent sections therefore renumbered.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related.
Public Input No. 142-NFPA 72-2022 [Section No. A.10.21.5]	

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:13:26 EST 2022
Committee: SIG-FUN

Public Input No. 143-NFPA 72-2022 [Section No. 10.21.6]

10.21.~~6~~ 7

The system owner or the owner's designated representative and the authority having jurisdiction shall be notified when an impairment period ends.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, thus renumbering subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 135-NFPA 72-2022 [Section No. 10.21.1]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:17:34 EST 2022
Committee: SIG-FUN

Public Input No. 533-NFPA 72-2022 [Chapter 11]

Chapter 11 Cybersecurity

Executive summary: There has been a significant amount of interest and activity regarding cybersecurity. This led to the establishment of a new Chapter 11 in NFPA 72-2022, but most information was placed in Annex J .

~~1 * – Cybersecurity.~~

~~Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided for~~

This proposal is intended to expound on the excellent work that was done by a number of great people for 72-2022 and to incorporate advances that have been made in technology since then.

Much of the literature that has been promulgated about cybersecurity asks questions, goes over what has happened at certain events, but does not provide some concrete guidance on how to implement at cybersecurity solution to Life Safety Systems. Chapter 11 is intended to provide actionable material that can be applied to systems.

Cybersecurity is constantly evolving. The changes in threats, technology and societies need to be assessed and when it make sense, applied to systems.

One size does not fit all. This has nothing to do with the system itself, meaning a small FACU that is monitoring a waterflow and tamper switch at a convenience store may not require any cybersecurity to be applied as determined by the risk assessment. That same FACU that is monitoring a waterflow and tamper switch that is installed at a secure data center with connection to an ISP may require a full barrier gateway (data firewall) and other protection as determined by the risk analysis.

Some people ask, “How do I know my system is cybersecure?” The response is all dependent on the risk. If the risks are assessed and the appropriate measures are implemented and maintained, then the system can be considered cybersecure at that time. A bad actor with enough time, talent and treasure will be eventually able to compromise virtually any system. The goal of Chapter 11 is to develop a reasonable approach to the probable, not all the possible cybersecurity risks that a system may be subjected to.

Note: This section is intended to replace and augment 72-2022 11.1, A11.1 and Annex J and in their entirety.

Chapter 11 – Cybersecurity (SEC)

11.1 Application

11.1.1 Where cybersecurity is required by a risk analysis, or by federal, state, or local regulations, systems shall be designed, installed, and maintained in accordance with the requirements of this chapter.

11.2 Purpose

11.2.1 To reduce unauthorized actuation or impairment of a fire alarm and signaling system,

cybersecurity risks shall be assessed.

11.3 Risk Analysis

11.3.1 A cybersecurity risk analysis shall be by stakeholders as to the nature and anticipated risks for which the system is it being designed.

11.3.1.1 The stakeholders shall consider both internal, external and maintenance risks to the system.

11.3.1.2 The risk analysis shall consider the number of persons, type of occupancy and perceived peril to the occupants, facilities, contents, systems, value, and operations.

11.4 Cybersecurity Levels

11.4.1 Cybersecurity levels shall be assigned to a system based on risk analysis.

11.4.2 Solution Levels (SL) are as follows:

11.4.2.1 SL 0. No specific network security features or operations are required

11.4.2.2 SL 1. This level correlates to Capability Security Levels (SL-C) of ISA/IEC 62443

11.4.2.3 SL 2. This level includes all of SL 1 and monitored physical tamper switches on all cabinets.

A11.4.2.3 This level correlates to Target Security Levels (SL-T) of ISA/IEC 62443

11.4.2.4 SL 3. This level includes all of SL2 requirements with the additional requirements that all bounded media shall be installed in continuous raceways

A11.4.2.4 This level correlates to Achieved Security Levels (SL-A) of ISA/IEC 62443

11.4.2.5 SL 4. This level includes all of SL 3 and the following:

11.4.2.5.1 All equipment enclosures that are not inside of a restricted access-controlled space shall be provided with tamper switches that are monitored by the system and automatically report to required on-site control locations that the enclosure has been accessed within 10 seconds.

11.4.2.5.1.1 Tamper signals shall be transmitted off-site if the site system is not continually monitored by properly trained on-premise staff.

11.4.2.5.2 All junction boxes or other pathway enclosures on bounded media that are not inside of a restricted access-controlled space shall be equipped with:

11.4.2.5.2.1 Tamper resistant fasteners and the enclosure covers equipped with frangible, tamper-evident seals or

11.4.2.5.2.2 Enclosure covers equipped with tamper switches that are monitored by the system and report to required on-site control and annunciation that the enclosure has been accessed within 10 seconds.

11.4.2.5.2.2.1 Tamper signals shall be transmitted off-site if the site system is not continually monitored by properly trained on-premise staff.

11.5 General

11.5.1 Bounded and unbounded data shall be protected with encryption in accordance with FPIS 140-3 or equivalent standard.

11.5.2 All unconnected or unmonitored physical data ports shall be protected by at least one or more of the following:

11.5.2.1 Physically protected from unauthorized access

11.5.2.2 Administratively shutdown

11.5.2.3 Require a password or other form of credentials to access the port

11.5.3 All service data devices shall be verified that they are equipped with and are operating on/with:

11.5.3.1 The latest verified operating systems with patches

11.5.3.2 Current antivirus/antimalware software and that antivirus scans have been done within the last 24 hours before the device is connected to the system being serviced

11.5.4 When any data connection is made from the system to an external network, the connection shall be protected by a barrier gateway or equivalent

11.6 Documentation

11.6.1 All system documentation shall be in accordance with this chapter and Chapter 7.

11.6.2 All system cybersecurity documentation shall be presented to and maintained by the facility owner.

11.6.3 All system cybersecurity documentation shall be delivered to the owner or the owner's representative upon final acceptance of the system

11.7 System Credentials

11.7.1 System passwords and system access credentials, herein referred to as credentials, shall be configured and maintained in accordance with this section.

11.7.1.1 Credentials shall be changed from factory or default to an owner-defined credential when system is placed in service.

11.7.1.2 Credentials shall be stored in a secure location and not visible or accessible to unauthorized personnel.

11.7.1.3 Only authorized persons who have approved equipment shall be permitted to connect to the system to make any changes in the system.

11.8 Testing & Maintenance

11.8.1 All system testing and maintenance shall be in accordance with this Chapter and Chapter 14.

11.8.2 System risk assessment shall be reviewed and updated at least annually. Any required changes shall be implemented, tested and documented.

11.9 Cybersecurity Software Revisions

11.9.1 Changes made only for cybersecurity purposes to barrier gateways shall not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all of the following are true:

(1) The changes do not affect the function of the executive or site-specific software.

(2) The integrity of the software update installed in the barrier gateway is verified to ensure complete and intact software delivery.

(3) The software is digitally signed by the manufacturer.

(4) The digital signature of the software is verified prior to the execution by the system or system components using secure signing keys.

11.9.2 Software changes to systems or system components made only for cybersecurity purposes shall be permitted to be made by remote access in accordance with Chapter 23.

11.10 Cybersecurity Standards

11.10.1 Systems shall be designed, installed, and maintained in accordance with one or more of the following cybersecurity standards:

(1) ANSI/ISA/IEC-62443 Global Automation Cybersecurity Standards Series

(2) NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufactures

(3) NIST Framework for Improving Critical Infrastructure Cybersecurity

(4) UL 2900-2-3. Software Cybersecurity for Network-Connectable Products

(5) NISTIR 8286 Integrating Cyber And Enterprise Management

(6) Other standards accepted by the Authority Having Jurisdiction

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 test laboratory

(2) Manufacturer certification for the specific type and brand of system provided

(3) An assessment of certification program acceptable to the authority having jurisdiction

11.11.2 Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate shall be checked annually.

Annex Material

A.11.1.1 Cybersecurity convers site end-to-end equipment, software, firmware, tools,

installation

~~methods~~

, physical security of and access to equipment

,

and data pathways, testing

,

and maintenance.

A11.3 Network risk analysis typically includes addressing:

- Physical installation and protection of devices and pathways
- Access to devices and pathways
- External and internal accessibility to data
- Firewalls and other barrier gateways
- Interconnection to other site systems
- Anti-agent software, services and scanning
- Vulnerability assessments
- Downtime/impairment impacts
- Recovery procedures
- Legal impacts
- Threat assessment
- Failure modes
- Backups
- Disaster recovery
- Equipment backups
- Penetration testing
- Updating processes
- Password and credential management
- Maintenance and support operations and devices

- Local and remote service connections
- Documentation, access to documentation and maintenance of documentation
- Staff training and certifications
- Vendor support

Additional Proposed Changes

File Name	Description	Approved
NFPA_72-2025_Proposed_Chapter_11_053122ms3.docx	New Chapter 11 72-2025	

Statement of Problem and Substantiation for Public Input

Create actual code requirements for cybersecurity for Chapter 11 and replace Annex J

Submitter Information Verification

Submitter Full Name: Morris Stoops
Organization: Carrier
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 31 14:40:32 EDT 2022
Committee: SIG-FUN

NFPA 72 – 2025 Edition, Chapter 11

Executive summary: There has been a significant amount of interest and activity regarding cybersecurity. This led to the establishment of a new Chapter 11 in NFPA 72-2022, but most information was placed in Annex J.

This proposal is intended to expound on the excellent work that was done by a number of great people for 72-2022 and to incorporate advances that have been made in technology since then.

Much of the literature that has been promulgated about cybersecurity asks questions, goes over what has happened at certain events, but does not provide some concrete guidance on how to implement at cybersecurity solution to Life Safety Systems. Chapter 11 is intended to provide actionable material that can be applied to systems.

Cybersecurity is constantly evolving. The changes in threats, technology and societies need to be assessed and when it make sense, applied to systems.

One size does not fit all. This has nothing to do with the system itself, meaning a small FACU that is monitoring a waterflow and tamper switch at a convenience store may not require any cybersecurity to be applied as determined by the risk assessment. That same FACU that is monitoring a waterflow and tamper switch that is installed at a secure data center with connection to an ISP may require a full barrier gateway (data firewall) and other protection as determined by the risk analysis.

Some people ask, “How do I know my system is cybersecure?” The response is all dependent on the risk. If the risks are assessed and the appropriate measures are implemented and maintained, then the system can be considered cybersecure at that time. A bad actor with enough time, talent and treasure will be eventually able to compromise virtually any system. The goal of Chapter 11 is to develop a reasonable approach to the probable, not all the possible cybersecurity risks that a system may be subjected to.

NFPA 72 – 2025 Edition, Chapter 11

Note: This section is intended to replace and augment 72-2022 11.1, A11.1 and Annex J and in their entirety.

Chapter 11 – Cybersecurity (SEC)

11.1 Application

11.1.1 Where cybersecurity is required by a risk analysis, or by federal, state, or local regulations, systems shall be designed, installed, and maintained in accordance with the requirements of this chapter.

11.2 Purpose

11.2.1 To reduce unauthorized actuation or impairment of a fire alarm and signaling system, cybersecurity risks shall be assessed.

11.3 Risk Analysis

11.3.1 A cybersecurity risk analysis shall be by stakeholders as to the nature and anticipated risks for which the system is it being designed.

11.3.1.1 The stakeholders shall consider both internal, external and maintenance risks to the system.

11.3.1.2 The risk analysis shall consider the number of persons, type of occupancy and perceived peril to the occupants, facilities, contents, systems, value, and operations.

11.4 Cybersecurity Levels

11.4.1 Cybersecurity levels shall be assigned to a system based on risk analysis.

11.4.2 Solution Levels (SL) are as follows:

11.4.2.1 SL 0. No specific network security features or operations are required

11.4.2.2 SL 1. This level correlates to Capability Security Levels (SL-C) of ISA/IEC 62443

11.4.2.3 SL 2. This level includes all of SL 1 and monitored physical tamper switches on all cabinets.

A11.4.2.3 This level correlates to Target Security Levels (SL-T) of ISA/IEC 62443

11.4.2.4 SL 3. This level includes all of SL2 requirements with the additional requirements that all bounded media shall be installed in continuous raceways

A11.4.2.4 This level correlates to Achieved Security Levels (SL-A) of ISA/IEC 62443

11.4.2.5 SL 4. This level includes all of SL 3 and the following:

11.4.2.5.1 All equipment enclosures that are not inside of a restricted access-controlled space shall be provided with tamper switches that are monitored by the system and automatically report to required on-site control locations that the enclosure has been accessed within 10 seconds.

11.4.2.5.1.1 Tamper signals shall be transmitted off-site if the site system is not continually monitored by properly trained on-premise staff.

11.4.2.5.2 All junction boxes or other pathway enclosures on bounded media that are not inside of a restricted access-controlled space shall be equipped with:

11.4.2.5.2.1 Tamper resistant fasteners and the enclosure covers equipped with frangible, tamper-evident seals or

11.4.2.5.2.2 Enclosure covers equipped with tamper switches that are monitored by the system and report to required on-site control and annunciation that the enclosure has been accessed within 10 seconds.

11.4.2.5.2.2.1 Tamper signals shall be transmitted off-site if the site system is not continually monitored by properly trained on-premise staff.

11.5 General

11.5.1 Bounded and unbounded data shall be protected with encryption in accordance with FPIS 140-3 or equivalent standard.

11.5.2 All unconnected or unmonitored physical data ports shall be protected by at least one or more of the following:

11.5.2.1 Physically protected from unauthorized access

11.5.2.2 Administratively shutdown

11.5.2.3 Require a password or other form of credentials to access the port

11.5.3 All service data devices shall be verified that they are equipped with and are operating on/with:

11.5.3.1 The latest verified operating systems with patches

11.5.3.2 Current antivirus/antimalware software and that antivirus scans have been done within the last 24 hours before the device is connected to the system being serviced

11.5.4 When any data connection is made from the system to an external network, the connection shall be protected by a barrier gateway or equivalent

11.6 Documentation

11.6.1 All system documentation shall be in accordance with this chapter and Chapter 7.

11.6.2 All system cybersecurity documentation shall be presented to and maintained by the facility owner.

11.6.3 All system cybersecurity documentation shall be delivered to the owner or the owner's representative upon final acceptance of the system

11.7 System Credentials

11.7.1 System passwords and system access credentials, herein referred to as credentials, shall be configured and maintained in accordance with this section.

11.7.1.1 Credentials shall be changed from factory or default to an owner-defined credential when system is placed in service.

11.7.1.2 Credentials shall be stored in a secure location and not visible or accessible to unauthorized personnel.

11.7.1.3 Only authorized persons who have approved equipment shall be permitted to connect to the system to make any changes in the system.

11.8 Testing & Maintenance

11.8.1 All system testing and maintenance shall be in accordance with this Chapter and Chapter 14.

11.8.2 System risk assessment shall be reviewed and updated at least annually. Any required changes shall be implemented, tested and documented.

11.9 Cybersecurity Software Revisions

11.9.1 Changes made only for cybersecurity purposes to barrier gateways shall not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all of the following are true:

(1) The changes do not affect the function of the executive or site-specific software.

(2) The integrity of the software update installed in the barrier gateway is verified to ensure complete and intact software delivery.

(3) The software is digitally signed by the manufacturer.

(4) The digital signature of the software is verified prior to the execution by the system or system components using secure signing keys.

11.9.2 Software changes to systems or system components made only for cybersecurity purposes shall be permitted to be made by remote access in accordance with Chapter 23.

11.10 Cybersecurity Standards

11.10.1 Systems shall be designed, installed, and maintained in accordance with one or more of the following cybersecurity standards:

(1) ANSI/ISA/IEC-62443 Global Automation Cybersecurity Standards Series

(2) NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufactures

(3) NIST Framework for Improving Critical Infrastructure Cybersecurity

(4) UL 2900-2-3. Software Cybersecurity for Network-Connectable Products

(5) NISTIR 8286 Integrating Cyber And Enterprise Management

(6) Other standards accepted by the Authority Having Jurisdiction

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 test laboratory

(2) Manufacturer certification for the specific type and brand of system provided

(3) An assessment of certification program acceptable to the authority having jurisdiction

11.11.2 Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate shall be checked annually.

Annex Material

A.11.1.1 Cybersecurity convers site end-to-end equipment, software, firmware, tools, installation, physical security of and access to equipment and data pathways, testing and maintenance.

A11.3 Network risk analysis typically includes addressing:

- Physical installation and protection of devices and pathways
- Access to devices and pathways
- External and internal accessibility to data
- Firewalls and other barrier gateways
- Interconnection to other site systems
- Anti-agent software, services and scanning
- Vulnerability assessments
- Downtime/impairment impacts
- Recovery procedures
- Legal impacts
- Threat assessment
- Failure modes
- Backups
- Disaster recovery
- Equipment backups
- Penetration testing

- Updating processes
- Password and credential management
- Maintenance and support operations and devices
- Local and remote service connections
- Documentation, access to documentation and maintenance of documentation
- Staff training and certifications
- Vendor support

Public Input No. 490-NFPA 72-2022 [New Section after 11.1]

11.2* Life Safety Systems Cybersecurity Risk Analysis

Manufactures of life safety systems, including Emergency Communications Systems (ECS), shall provide system specific cybersecurity risk analyses for review by the authority having jurisdiction, building owners, systems installation personnel, and building owner's designated cybersecurity teams responsible for providing cybersecurity as required by 11.2.1 through 11.2.5.

11.2.1 Life safety systems include, but are not limited to, Fire Alarm Systems, Evacuation Voice Fire Alarm Systems (EVAC), Mass Notification Systems (MNS), Smoke Control Systems, Two-Way In-Building Wired Emergency Services Communications Systems, Two-Way Radio Communications Enhancement Systems, and Two-Way Emergency Communications Systems for Rescue Assistance.

11.2.2* Cybersecurity Risk Analysis shall comply with NIST SP 800-30 Rev 1.1 Guide for Conducting Risk Assessments, or another risk analysis framework acceptable to the authority having jurisdiction.

11.2.3* System risk analysis shall at a minimum qualitatively identify risks, likelihoods, impacts & consequences, controls, countermeasures, and mitigations for the following:

(1) Account Management, including default passwords, user account management, privileged account management, system, service, and operating system accounts, authentication and authorization, multi-factor authentication, session limitations, and access failed attempt retry rates & limits including account timeouts and lockout settings

(2) Personally Identifiable Information (PII) maintained by the system

(3) Data that may be considered confidential in nature such as floor plans, system wiring, IP addresses and ports, or diagnostic information

(4) Logging and audit trail management and access

(5) Software bill of materials (SBOM) as it relates to third party code modules, libraries, open-source software (OSS), and commercial off-the-shelf (COTS) software

(6) Software and firmware development methodologies and known system code vulnerabilities including deployed encryption methodologies

(7) Update and patch management

(8) Known cybersecurity vulnerabilities inherent to or affecting the system

(9) Configuration management

(10) Known or expected external system threats, including risks associated with malware, open communications ports, and configuration

(11) Potential insider threats due to intentional or unintentional access privilege abuse or leakage

(12) Common controls such as firewalls

(13) Components hosted on any non-life safety dedicated equipment such as shared use computers or the cloud

(14) System monitoring capabilities including monitoring for integrity, monitoring of system components and assets, and system status monitoring

(15) System communication pathway vulnerabilities including physical and wireless pathway susceptibility to disconnection, interception and insertion of data, and jamming.

11.2.4* Risk Analysis shall provide an executive summery and risk registers for review, and details for individual risks explaining the analysis and recommended practices, controls, countermeasures, and mitigations.

11.2.5* Risk Analysis shall be republished with applicable updates annually for the duration of the system's support lifecycle.

A.11.2 Life Safety Systems Cybersecurity Risk Analysis

Annex J, Guidelines for Cybersecurity, outline several cybersecurity standards, anyone of which could be applied to emergency communications systems, and maintained by manufactures. However, cybersecurity for emergency communications has many contexts and objectives for applying cybersecurity standards including:

(1) The security practices for the overall design, development, production, and service of life safety systems, in addition to the overall cybersecurity posture of the manufacturing company itself. For example, it does not matter how well a system is designed from a cybersecurity perspective, if the manufacturer does not adequately secure its own systems, threat actors can compromise products by installing covert back doors during initial development or development and distribution of code updates.

(2) The cybersecurity practices of the installation and maintenance company both during and after the installation, and the overall cybersecurity posture of the installation company itself. Again, as an example, it does not matter how secure the system is if the installation company does not do background checks, and an insider configures the systems insecurely on purpose, or uses passwords and credentials inappropriately, or sells them to other threat actors.

(3) The cybersecurity practices of the owner's organization, both during installation, and during maintenance over the systems lifecycle. This can be viewed from both the perspectives of the security of the infrastructure that the life safety system depends on, and the security posture of the organization that is using the system. Again, the system and infrastructure security is only as strong as the weakest link of the organization utilizing it. For example, it does not matter if the system cannot be accessed directly from the internet, if the inside network users are not well trained on cybersecurity practices and are susceptible to phishing campaigns. An attacker having taken advantage of a user to breach the network, may be able to directly access the life safety system to cause damage.

Which cybersecurity standard might apply is largely based on the objectives that are being sought. However, one commonality for all cybersecurity programs is the risk analysis. The risk analysis informs decision makers on the risks, likelihoods, impacts and consequences, potential controls and mitigations, business continuity and disaster recovery plans, and the residual risk that must be communicated to and ultimately accepted by the owner.

Since the risk analysis is a common requirement of all major cybersecurity programs, it lends itself as a common resource for all systems that are subject to cybersecurity threats.

Cybersecurity for life safety systems starts with the manufacturer. No other organization has as much insight into the system as the company that designed and built it. So, it is necessary that the manufactures make available an initial risk analysis to other stakeholders as a starting point for installation and maintenance companies to evaluate their own practices, as well as to the system owners, and those who are responsible for maintaining the security posture of the connected infrastructure.

The responsibility of making system risk analysis' available does not imply that the risk analysis must be

publicly published. Manufacturers must evaluate the sensitivity of the information contained and manage sharing of this information responsibly. If necessary, risk analysis can be provided through secure access, NDAs, watermarks, or other controls. However, as with all security related information, the risk analysis confidentiality cannot be the security measure itself. Good security utilizes a defense in depth approach. Security through obscurity is not a recommended practice.

A.11.2.2 There are many frameworks available for conducting a risk analysis. Some are created from an Enterprise Risk Management (ERM) perspective, such as the ISO 31000 Framework, while other focus on cybersecurity specifically such as the Common Weakness Risk Analysis Framework (CWRAF). NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments is focused on information technology threats and the relationship with cybersecurity risks. The activities outlined include system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and results documentation.

While this framework is specifically reference in the code because it is targeted, well understood, and publicly available, there are other recognized risk assessment frameworks that can be considered. For example, the manufacture may already have a robust enterprise risk management program enacted and is utilizing another framework to conduct their risk analysis. Or there may already be a third-party analysis' being conducted by organizations such as UL, that produce risk analysis' according to other standards. These can all be considered viable documents.

A.11.2.3 A cybersecurity risk analysis considers multiple avenues for exploitation:

(1) Many types of cybersecurity attacks attempt to compromise user and system accounts, especially privileged accounts. It is not uncommon to find networkable devices that have limited account management. Some devices are configured with built-in accounts that have no individual users (requiring multiple users to share passwords), no levels of access (effectively making any access privileged access), with no ability to apply permissions based on the users job functions, with no ability to disable specific accounts (necessary when users change jobs), and no centralized management of these accounts (accounts may be isolated to specific devices and must be managed one device at a time). It is not uncommon for devices to ship with common default account names and passwords (like admin, admin), that rely upon specific actions to change these accounts, that may never occur, and not be know to the system owners. In some cases, manufactures may implement backdoor access, for service convenience or recovery, that are fixed and if become known compromise any security until a system update can be installed that resolves the issue. There may be no password complexity requirements, and if access attempt limitations and automatic lockouts are not present, passwords can be defeated by brute force using password dictionaries.

(2) Personally Identifiable Information (PII) can include names, addresses, IP addresses, email addresses, telephone numbers, date of birth, credit card information, photographs and video that includes faces, biometric information including fingerprints, employment information, and medical data. PII is specifically protected by many laws internationally including the US Privacy Act, the EU General Data Protection Regulation (GDPR), and Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). Cybersecurity breaches that compromise PII are subject to governmental, law enforcement, and often public reporting requirements. As such, if life safety systems maintain any PII data, special consideration must be given to risks associated with protecting it.

(3) There may be other data that a life safety system maintains that would be considered confidential. While security though obscurity is never a recommended practice, neither is a failure to protect information that may be used to aid in compromising a system. For example, information such as online documentation that reveals system maintenance status, locations and IP addresses of devices, wiring information such as network switch port numbers, riser information, cabling pathways, encryption keys or user credentials, if compromised could all be used to attack the life safety system or other related systems.

(4) Logs and audit trails are critically important to helping establish if a system is being attacked, and who the attacker may be, or the avenue of attack. For example, changes to a system configuration or software version may be legitimate or illegitimate. But unless it is known when and who made these changes, it can be very difficult to assess the intent. Also, if particular credentials are being utilized inappropriately, information contained in logs and audit trails are often necessary to properly respond. In this context, logs and audit trails themselves require appropriate protection. Individuals and account that have privileges that are being tracked, should not also have privileges to access and change the logs or audit trails.

(5) There is more emphasis on supply-chain attacks as multiple high-profile cybersecurity failures have highlighted the far-reaching impacts of exploiting these vulnerabilities. Software bills of material (SBOM) have gain increasing attention as a mechanism for products to identify components (especially third-party components) that are utilized in products used in critical infrastructure. This subject deserves attention in the risk analysis as SBOM requirements become more integrated into the commercial and regulatory landscapes.

(6) Software development systems are continuously evolving. For example, DevSecOps is the merging of security with DevOps. DevOps is integrated development and quality assurance, often automating the process of software development to a great extent. By implementing a DevSecOps development program, manufactures are committing to embedding security awareness, secure coding practices, and security focused testing into their product development lifecycle. These approaches can reveal previously unknown vulnerabilities due to past coding practices. Examples include SQL injection, buffer overflow, or deprecated encryption methodologies. MD5, a widely used hashing mechanism is an example of a compromised encryption technology.

(7) As security vulnerabilities are discovered, existing systems may be affected. Not only is it important for manufactures to provide solutions when vulnerabilities are discovered, but just as importantly to carefully manage the update and patch management infrastructure to ensure that corrections are available, have integrity, have not been modified or spoofed, and are applied successfully. This can be a challenging area for consideration for life safety systems as remote access and updates are impacted by other areas of the NFPA 72 code.

(8) When cybersecurity vulnerabilities are discovered, how is this information conveyed in a timely manner to the owners of life safety systems? It may be critically important that some corrective actions, controls, or countermeasures be deployed to minimize the risk to the system. This is especially the case when zero-day vulnerabilities are discovered. How will the manufacture maintain communications with other stakeholders to keep them informed of such developments?

(9) How life safety systems are configured are critical to their deployment and operation. Changes to configuration may be instigated after careful consideration, testing, approval, and documentation, such as would be required by a change control policy. But configuration changes may also be undertaken using an undocumented ad-hoc approach. Risks include how baseline configurations are maintained, such that a known tested and approved configuration may be restored should the system configuration be damaged, intentionally, or unintentionally.

(10) There are many avenues of cybersecurity attack that are widely used and very successful. Phishing is a good example, where authorized users are compromised revealing user accounts, passwords, and other critical information. One of the best defenses against phishing is education and training. To the extent that a life safety system is secure can be seen as a function of the training and proficiency that its users have - to resist phishing attacks.

(11) While training of any designer, developer, installer, maintenance person, or user on related aspects of life safety system design, deployment, and use is critical, so too is the due diligence that is performed to ensure the trustworthiness of these people. Background checks are an obvious example, but so too is the management of credentials, separation of duties, least privilege, need-to-know, and account maintenance. An authorized employee, who is terminated and disgruntled, may cause significant damage to systems if their access privileges are not promptly revoked.

(12) Many networks have protection such as Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). Others such as Security Information Event Management (SEIM) systems collect log information from various systems to identify, warn, and take action when a cybersecurity event is detected. Risks to consider incorporate to what extent might these systems include or exclude monitoring of the life safety system, and to what extent is it possible for these systems to affect the operation of the life safety system.

(13) If is not unreasonable to expect more and more hosting of life safety systems, or partial hosting of life safety systems in the cloud. This is currently the case amongst many unlisted systems utilized for life safety purposes. The extent to which such systems may be compromised, and how vulnerable are their function to interruptions in communications must be considered.

(14) Many aspects of life safety systems are monitored for integrity. Reporting of integrity issues is a very desirable capability that can be provided by connected systems. Risks and protections for this reporting should be reviewed as part of a cybersecurity risk assessment. If there is an expectation that remote monitoring is working, local annunciations of trouble may be ignored if it is assumed that maintenance personnel are aware. How would these services be affected by a denial-of-service attack?

(15) Often, when confronting cybersecurity issues, the assumption made is that attacks are launched remotely from the internet. However, there are ample examples of attackers gaining physical access to a facility to enable an attack. Even a system that has no networking capability, with only a RS232 serial port can be connected to an RS232-to-Ethernet adapter. This may be intended benignly, as a way of enabling remote monitoring or remote service. But it is a risk that should be considered none-the-less. Take for example a building that is connected to a system via a wireless link. What risk are present if an attacker utilizes an inexpensive RF jammer to disrupt communications?

A.11.2.4 The structure of the risk analysis report requires both high level summaries (executive summery and risk registers) and detailed explanations. The high-level reviews are intended for stakeholder decision makers (such as managers, executives, code officials, and system and building owners) to understand the risks and some of the controls that may be employed to reduce the risk or mitigate the impact of an event. The high-level summaries may also include heat maps to help illustrate the levels of risk. The detailed analysis is intended to inform technical personnel involved with installing, maintaining, and securing the system's infrastructure regarding the vulnerabilities and deploying technical, physical, and administrative controls and other safeguards and countermeasures to reduce risk.

A.11.2.5 Fundamental to risk management, is the ongoing monitoring of the risk landscape as it applies to the deployment of life safety systems over time. As new vulnerabilities are discovered and new threats emerge, how risks are changing must be considered. Also, systems evolve over time such that some risks may be reduced or eliminated. It is important to update the risk analysis, so valuable resources are not consumed by controls that protect systems from risk that no longer exist. Just as the continued availability of spare parts is important for maintenance of a system, so to is the continued availability of up-to-date information to protect those systems.

Statement of Problem and Substantiation for Public Input

As systems become more and more connected, the implications for life safety are significant. For example, emerging technologies in augmented reality using heads-up displays can provide fire fighters with critical information to help enhance rescue efforts, while also improving prospects for their own safety in precarious circumstances. But a clear lesson we can take from the cybersecurity world, and society at large, is the need to protect the availability, confidentiality, and integrity of the information that is being utilized for any life safety purpose.

Cybersecurity includes a large and complex body of knowledge with many organizations, governmental, commercial, and associations involved in creating many standards, best practices, and resources aimed at many different types of organizations and systems, for many purposes. Additionally, the cybersecurity threat landscape is continuously and rapidly evolving. It is unlikely that

meaningful cybersecurity goals can be achieved by creating prescriptive cybersecurity requirements for life safety systems, that rely on codes and standards, with multi-year version cycles, while facing threats such as zero-day vulnerabilities. Likewise, attempting to specify one or a limited number of external cybersecurity standards, not developed specifically for life safety systems is problematic. Also, the limited cybersecurity experience that currently exists in the life safety equipment design, manufacturing, installation, maintenance, inspection and regulatory communities, means that compliance details of many cybersecurity standards is not well understood by the related stakeholders, nor by the ultimate owners. Some are product-based standards. Others are organizational based. Others are developmentally focused. Some are regulatory in nature. Some require third-party audits, while others are self-administered.

But one thing that they all have in common, is that they all require a risk analysis. This is a common fixture that can be utilized by all responsible manufactures to evaluate their products for cybersecurity risks. But most importantly, in the deployment of the systems, a manufacture provided risk analysis, serves to support the installation company, inspection, maintenance, all the way up the line to the owners. Each of these stakeholders, who likely will have different cybersecurity approaches or standards-based certification programs, can utilize the manufacture's risk analysis.

This proposal leverages the common ground, to feed the installation, inspection, and maintenance teams with relevant actionable information about the products that they are engaged with. It also serves the system owners and the providers of infrastructure for which ongoing security will ultimately depend. While some may argue that this is an additional burden for manufactures, others can argue that it is also in manufactures best interest. Providing a document that manufactures will need to create and maintain is a reasonable requirement, since no other stakeholder is in the position to have the detailed product insights necessary. Yet, in the spirit of minimal standards, it is less arduous than requiring compliance with an external standard that may not be in the best interest of the manufacture or the product. But since it is such a common component of any cybersecurity standard, it allows the different stakeholders to comply with this code, and satisfy a responsible level of cybersecurity control, that is supportive of each organization's individual cybersecurity program.

Submitter Information Verification

Submitter Full Name: Michael Pallett
Organization: Pallett Corner Consulting
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 08:52:41 EDT 2022
Committee: SIG-FUN

Public Input No. 272-NFPA 72-2022 [Section No. 11.1]

11.1* Cybersecurity.

~~Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided for equipment,~~ Equipment, software, firmware, tools, installation methods, physical security of and access to equipment, data pathways, inspecting, testing, and maintenance shall comply with UL 2900-2-3 Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems .

Statement of Problem and Substantiation for Public Input

Chapter 11 currently lacks any specific enforceable provisions. Mandating compliance with UL 2900-2-3 will provide a baseline from an existing accepted industry standard that addresses the cybersecurity issues covered within the scope of NFPA 72.

Submitter Information Verification

Submitter Full Name: Anthony Apfelbeck
Organization: Altamonte Springs Building/Fire Safety Department
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 02 10:30:14 EDT 2022
Committee: SIG-FUN

Public Input No. 384-NFPA 72-2022 [Section No. 11.1]

11.1* Cybersecurity.

11.1.1 Cybersecurity Provisions

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be

~~provided for~~
provided in accordance with Chapter 11, for equipment, software,

~~firmware,~~

~~tools~~

system support tools , installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1.2 Connected Equipment Software Development

Equipment shall be developed by the manufacturer in accordance with one or more of the following secure software development lifecycle standards:

A) ANSI/ISA/IEC 62443 Security for Industrial and Automation Control Systems Series of standards

B) ANSI/CAN/UL 2900 Standard for Software Cybersecurity for Network-Connectable Products

C) NIST Cybersecurity Framework

E) NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.3 Network Connectable Equipment Software Development and Production Environments

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

A) NIST Cybersecurity Framework

B) ISO/IEC 27001 Information Security Management

C) IASME Consortium Cyber Essentials

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.4 Security Levels for Network Connectable Equipment

All interfaces used to communicate with network connectable equipment shall be protected using the following minimum security levels:

A) For all non-internet facing wireless Interfaces and those non-internet facing wired interfaces that employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

B) For non-internet facing wired interfaces that do not employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 1 or UL 2900 Security Level 1 or the equivalent level associated with 11.1.3 D.

C) For all wired or wireless internet facing (WiFi) interfaces, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 3 or UL 2900 Security Level 3 or the equivalent level associated with 11.1.3 D.

D) For all cellular, Bluetooth, and other wireless interfaces that do not employ internet protocol, IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

11.1.5 Network Connectable Equipment Cybersecurity-related Software Updates

11.1.5.1 The equipment manufacturer shall evaluate all discovered cybersecurity threats at least quarterly and shall determine if a software update is required to maintain the cybersecurity level achieved in complying with 11.1.2 and 11.1.3 until the equipment is no longer be supported by the manufacturer.

11.1.5.2

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

11.1.5.4 The equipment manufacturer shall notify the system owner or their representative, of all required software security updates required to maintain he cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.5 Software for network connectable devices shall be maintained by installing software security updates as required by the manufacturer to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.6 Software security updates that are deemed necessary by the manufacturer for compliance with 11.1.3.2 shall be installed at least annually.

11.1.5.7 Cybersecurity-related only software updates applied to system elements that do not affect the system site-specific or system executive software shall not be required to comply with 14.4.2.

11.1.5.8 Cybersecurity-related only software changes to systems or system components shall be permitted to be made by remote access in accordance with Chapter 23.

11.1.6 Notification of Termination of Cybersecurity Update Support

The manufacturer shall notify the system owner or their representative, of the termination of software cybersecurity-related software update support required by 11.1.5 for any element of the system.

11.1.7 Cybersecurity for System Support Tools

A system support tool and the support tool interfaces shall comply with the requirements of 11.1.2 through 11.1.6.

11.1.8 Evidence of Compliance.

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

(1) Certification of compliance by a nationally recognized test 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

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

11.1.9 Documentation

The standards used and security levels employed in complying with Chapter 11 shall be

identified and included in the system documentation required by Chapter 7

Statement of Problem and Substantiation for Public Input

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.
Their report lists gaps that include:
• Configuration – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
• Implementation – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
• Security – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.
• Access – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment
The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here:
https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
https://www.wired.com/2013/05/googles-control-system-hacked/
https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 388-NFPA 72-2022 [Sections J.1, J.2, J.3, J.4, J.5, J.6]	
Public Input No. 390-NFPA 72-2022 [Section No. A.11.1]	

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:59:57 EDT 2022
Committee: SIG-FUN

Public Input No. 469-NFPA 72-2022 [Section No. 11.1]

11.1* Cybersecurity.

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided for equipment, software, firmware, tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1* **Cybersecurity.**

11.1.1 Cybersecurity Provisions

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided in accordance with Chapter 11, for equipment, software,

~~firmware,~~

system support tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1.2 Connected Equipment Software Development

Equipment shall be developed by the manufacturer in accordance with one or more of the following secure software development lifecycle standards:

A) ANSI/ISA/IEC 62443 Security for Industrial and Automation Control Systems Series of standards

B) ANSI/CAN/UL 2900 Standard for Software Cybersecurity for Network-Connectable Products

C) NIST Cybersecurity Framework

E) NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.3 Network Connectable Equipment Software Development and Production Environments

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

A) NIST Cybersecurity Framework

B) ISO/IEC 27001 Information Security Management

C) IASME Consortium Cyber Essentials

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.4 Security Levels for Network Connectable Equipment

All interfaces used to communicate with network connectable equipment shall be protected using the following minimum security levels:

A) For all non-internet facing wireless Interfaces and those non-internet facing wired interfaces that employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

B) For non-internet facing wired interfaces that do not employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 1 or UL 2900 Security Level 1 or the equivalent level associated with 11.1.3 D.

C) For all wired or wireless internet facing (WiFi) interfaces, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 3 or UL 2900 Security Level 3 or the equivalent level associated with 11.1.3

D.

D) For all cellular, Bluetooth, and other wireless interfaces that do not employ internet protocol, IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

11.1.5 Network Connectable Equipment Cybersecurity-related Software Updates

11.1.5.1 The equipment manufacturer shall evaluate all discovered cybersecurity threats at least quarterly and shall determine if a software update is required to maintain the cybersecurity level achieved in complying with 11.1.2 and 11.1.3 until the equipment is no longer be supported by the manufacturer.

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

11.1.5.3 The equipment manufacturer shall notify the system owner or their representative, of all required software security updates required to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.4 Software for network connectable devices shall be maintained by installing software security updates as required by the manufacturer to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.5 Software security updates that are deemed necessary by the manufacturer for compliance with 11.1.3 shall be installed at least annually.

11.1.5.6 Cybersecurity-related only software updates applied to system elements that do not affect the system site-specific or system executive software shall not be required to comply with 14.4.2.

11.1.5.7 Cybersecurity-related only software changes to systems or system components shall be permitted to be made by remote access in accordance with Chapter 23.

11.1.6 Notification of Termination of Cybersecurity Update Support

The manufacturer shall notify the system owner or their representative, of the termination of software cybersecurity-related software update support required by 11.1.5 for any element of the system.

11.1.7 Cybersecurity for System Support Tools

A system support tool and the support tool interfaces shall comply with the requirements of 11.1.2 through 11.1.6.

11.1.8 Evidence of Compliance.

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

(1) Certification of compliance by a nationally recognized test 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

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

11.1.9 Documentation

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

J A . 11. 1 ~~Introduction.~~ Cybersecurity

NFPA 72 **contains requirements for fire alarm and emergency communications systems that can be impacted by cybersecurity threats. Coordination of cybersecurity frameworks to protect the functions of systems is essential ~~in order~~ to prevent unwanted impacts on the system. Where the ~~system would need to interface~~ system interfaces with the internet or other systems ~~, it would make sense to provide~~ a secure firewall or gateway ~~. In any case, protection from cybersecurity threats is essential.~~**

~~The Technical Committee has determined that, in lieu of establishing requirements in Chapter 11 on cybersecurity at this time, it is appropriate to provide such guidance and framework in this annex. This allows the industry and the public the ability to gain experience with cybersecurity measures and provide constructive feedback for future editions of this Code.~~

should be provided to effect vital protection against cybersecurity threats.

~~J.2 Cybersecurity Provisions.~~

~~Where cybersecurity provisions are required, manufacturers, system designers, system installers, inspection personnel, testing personnel, and service technicians involved in the design, installation, testing, and maintenance of cybersecurity provisions should provide cybersecurity measures as outlined in this annex.~~

J 11 . 4 1.8 Evidence of Compliance.

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

(1) **Certification of compliance by a nationally recognized test 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**

~~J.5 Documentation.~~

~~All system-related documentation associated with the use of the selected standard(s) is included as part of the system documentation required by Chapter 7.~~

~~J.6 Cybersecurity Certificate Maintenance.~~

~~J.6.1 Certificate Validation.~~

~~Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate should be checked~~

~~annually.~~

~~J.6.2 Cybersecurity Software Revisions.~~

~~Software changes made only for cybersecurity purposes to firewalls or barrier gateways should not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all the following are true:~~

(1) ~~The changes do not affect the function of the executive or site-specific software.~~

(2) ~~The integrity of the software update installed in the firewall or barrier gateway is verified to ensure complete and intact software delivery.~~

(3) ~~The software is digitally signed by the manufacturer.~~

(4) ~~The digital signature of the software is verified prior to execution by the system or system components using secure signing keys.~~

~~Figure J.6.2~~

11.1.8.2 The validity of cybersecurity certificates shall be verified annually.

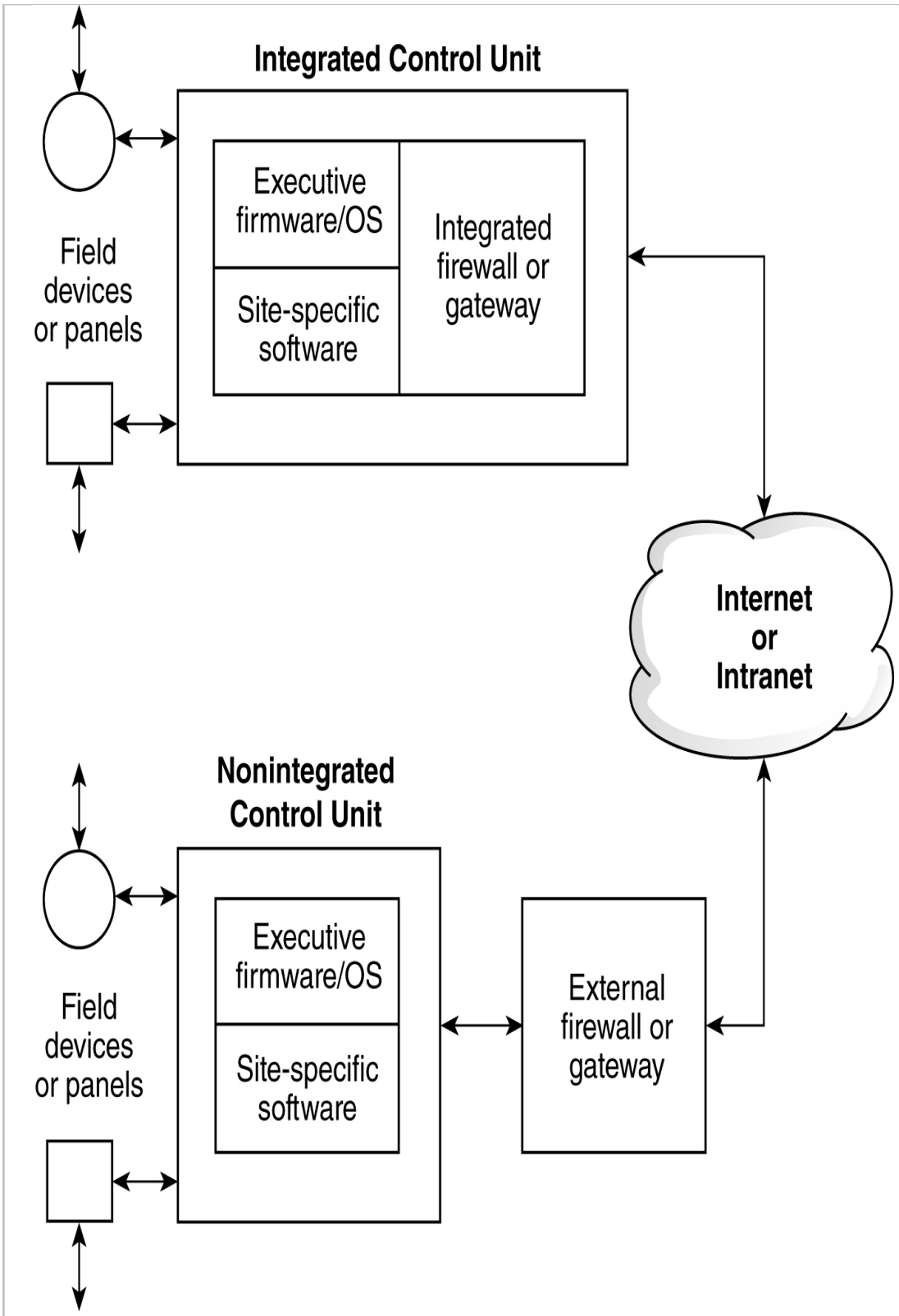
A.1.11.5.7 Figure A.1.11.5.7 depicts system typical firewall/gateway operation. Such functionality is not mandated but when deployed might take the form of physical hardware, firmware, or a combination of both. The firewall/gateway might be physically integrated into the control unit as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit as shown in the nonintegrated control unit. If the firewall/gateway is segmented from the executive firmware and site-specific software and if security software changes to the cybersecurity-related only software within the firewall/gateway are made, these changes should not require system retesting. If changes are made in a firewall/gateway that is not segmented from the executive firmware and site-specific software, the system should be retested.

~~Figure J~~

Figure A.

~~6.2 System~~

1.11.5.7 System Typical Firewall/Gateway Operation.



J

11.

~~6.3 Remote Software Changes.~~

~~Software~~

1.5.8 Cybersecurity-related only changes to systems or system components made only for cybersecurity purposes should components shall be permitted to be made by remote access in accordance with Chapter 23.

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_11.1_comments.docx		

Statement of Problem and Substantiation for Public Input

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.
Their report lists gaps that include:

- Configuration – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
- Implementation – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
- Security – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.
- Access – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment

The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here.

- https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
- Researchers Hack Building Control System at Google Australia Office | WIRED
- Target Hackers Broke in Via HVAC Company – Krebs on Security

Submitter Information Verification

Submitter Full Name: Tim Knisely
Organization: Automatic Fire Alarm Association (AFAA)
Affiliation: Automatic Fire Alarm Association (AFAA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 10:15:27 EDT 2022
Committee: SIG-FUN

Public Input No. 508-NFPA 72-2022 [Section No. 11.1]

11.1* Cybersecurity.

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided for equipment, software, firmware, tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1.1 Cybersecurity Provisions

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided in accordance with Chapter 11, for equipment software, system support tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1.2 Connected Equipment Software Development

Equipment shall be developed by the manufacture in accordance with one or more of the following secure software development life cycle standards:

A) ANSI/ISA/IEC 62443 Security for Industrial and Automation Control Systems Series of standards

B) ANSI/CAN/UL 2900 Standard for Software Cybersecurity for Network-Connectable Products

C) NIST Cybersecurity Frameword

D) Other equivalent standards acceptable to the authority having jurisdiction

E) NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers

11.1.3 Network Connectable Equipment Software Development and Production Environments

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

A) NIST Cybersecurity Framework

B)ISO/IEC 27001 Information Security Management

C) IASME Consortium Cyber Essentials

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.4 Security Levels for Network Connectable Equipment

All interfaces used to communicate with network connectable equipment shall be protected using the following minimum security levels:

A) For all non-internet facing wireless interfaces and those non-internet facing wired interfaces that employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3, Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3D.

B) For non-internet facing wired interfaces that do not employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 1 or UL 2900 Security Level 1 or the equivalent level associated with 11.1.3D.

C) For all wired or wireless internet facing (WIFI) interfaces, ANSI/ISA/IEC 62443-4-2/2-3 Security Level 3 or UL 2900 Security Level 3 or the equivalent level associated with 11.1.3.D.

D) For all cellular, Bluetooth, and othe wireless interfaces that do not employ internet protocol, IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3.D.

11.1.5 Network Connectable Equipment Cybersecurity-related Updates

11.1.5.1 The equipment manufacture shall evaluate all discovered cybersecurity threats at least quarterly and shall determine if a software is required to maintain the cybersecurity level achieved in complying with 11.1.2 and 11.1.3 until the equipment is no longer be supported by the manufacturer.

11.1.5.2 The system installer shall provide the name and contact information of the system ownere or their representative to the manufacturer at the time of system acceptance testing.

11.1.5.3 The equipment manufacturer shall notify the system owner or their representative of

all required software security updates required to maintain the cybersecurity level achieved in compying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.4 Software for network connectable devices shall be maintained by installing sofware security updates as required by the manufacturer to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.5 Software security updates that are deemd necessary by the manufacturer for compliance with 11.1.3 shall be installed at least annually.

11.1.5.6 Cybersecurity-related only software updates applied to system elements that do not affect the system site-specific or system executive software shall not be required to comply with 14.4.2.

11.1.5.7 Cybersecuity-related only software change to systems or system components shall be permitted to be made by remote access in accordance with Chapter 23.

11.1.6 Notification of Termination of Cybersecurity Update Support

The manufacturer shall notify the system owner or their representative of the termination of software cybersecurity-related software update support required by 11.1.5 for any element of the system.

11.1.7 Cybersecurity for System Support Tools

A system support tool and the support tool interfaces shall comply with the requirements of 11.1.2 through 11.1.6.

11.1.8 Evidence of Compliance

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

1. Certification of compliance by a nationally recognized test 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

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

11.1.9 Documentation

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

Statement of Problem and Substantiation for Public Input

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.
Their report lists gaps that include:

- Configuration – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
- Implementation – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
- Security – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.

- Access – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment

The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here.

- https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
- Researchers Hack Building Control System at Google Australia Office | WIRED
- Target Hackers Broke in Via HVAC Company – Krebs on Security

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:
Zip:
Submittal Date: Mon May 30 16:21:44 EDT 2022
Committee: SIG-FUN

Public Input No. 74-NFPA 72-2022 [Section No. A.1.6.5]

A.1.6.5

Where dimensions are expressed in inches, it is intended that the precision of the measurement be 1 in., thus plus or minus ½ in. The conversion and presentation of dimensions in millimeters would then have a precision of 25 mm, thus plus or minus 13 mm. It is not intended that the application or enforcement of these values be more precise than the precision expressed.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 2.3.3.3 requires Chapter 1 written in mandatory language. The task group proposed text in PI-73 includes mandatory language for section 1.6.5 and proposes this PI for moving the second sentence to the Annex, since it is more informative vs. mandatory.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 13:08:48 EST 2022
Committee: SIG-FUN

Public Input No. 375-NFPA 72-2022 [Section No. A.7.3.2]

A.7.3.2

Design (layout) documents should contain information related to the system that could include specifications, shop drawings, ~~input/output matrix~~ sequence of operation , battery calculations, notification appliance voltage drop calculations for visual notification appliances and loudspeakers, and product technical data sheets.

Design (layout) documents could include such items as preliminary plans issued as guidance and direction, risk analysis, emergency response plan, or a combination of these.

Deviations from requirements of governing laws, codes, standards, or preliminary plan requirements specified by an engineer should be clearly identified and documented as such.

Documentation of equivalency, where applicable, should be provided in accordance with Section 1.5 and be included with the record drawings.

It is the intent that existing systems that are altered should have design (layout) documents prepared that are applicable only to the portion(s) of the system being altered.

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e.,

NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 15:16:13 EDT 2022
Committee: SIG-FUN

Public Input No. 451-NFPA 72-2022 [Section No. A.7.4.9]

A.7.4.9

For an example of a logic diagram see A.14.6.1.1(a) and for an example of an input/output matrix ~~of operation~~ , see A.14.6.1.1(b) .

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_Figure_A.14.6.1.1_a_Final_002_.pdf	Sample Logic Diagram	

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Thu May 26 16:44:39 EDT 2022
Committee: SIG-FUN

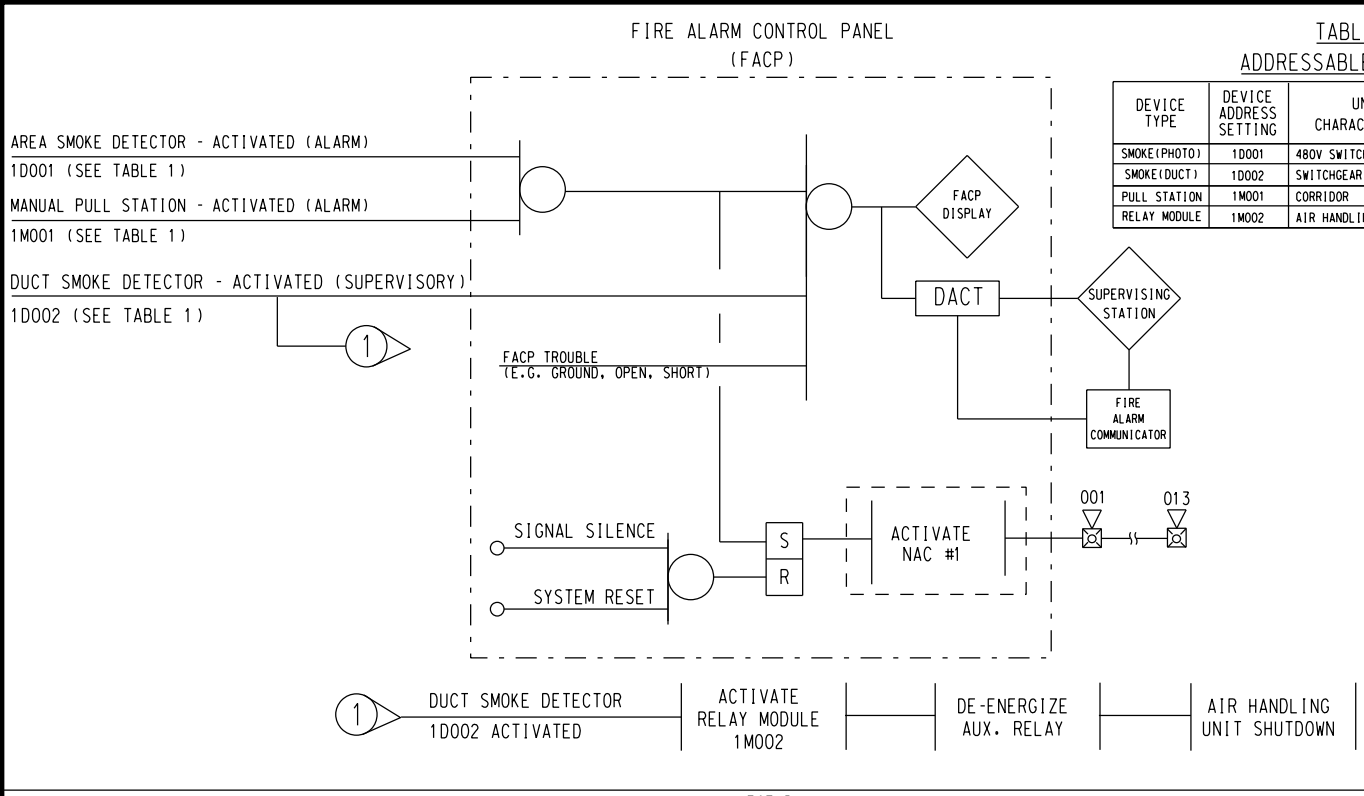


TABLE 1
ADDRESSABLE DEVICES

DEVICE TYPE	DEVICE ADDRESS SETTING	UNIQUE CHARACTER LABEL	CHARACTER LABEL EXTENSION
SMOKE(PHOTO)	1D001	480V SWITCHGEAR ROOM	DETECTOR
SMOKE(DUCT)	1D002	SWITCHGEAR ROOM	DUCT DETECTOR
PULL STATION	1M001	CORRIDOR	PULL STATION
RELAY MODULE	1M002	AIR HANDLING UNIT	SHUTDOWN

LEGEND

MANUAL INPUT ● — MAINTAINED HAND SWITCH INPUT

MANUAL INPUT ○ — MOMENTARY HAND SWITCH INPUT

OUTPUT EXIST WHEN ONE OR MORE INPUTS ARE PRESENT

OUTPUT ACTION — INITIATE NAC #1 — ACTION DESCRIPTION

MEMORY

A — S — C
B — R

LOGIC OUTPUT "C" EXIST AS SOON AS INPUT "A" EXISTS. "C" CONTINUES TO EXIST REGARDLESS OF SUBSEQUENT STATE OF "A" UNTIL RESET INPUT "B" IS PRESENT. "C" REMAINS REGARDLESS OF SUBSEQUENT STATE OF "B" UNTIL "A" CAUSES THE MEMORY TO BE SET.

SUPERVISING STATION — ANNUNCIATOR/LED READ OUT DISPLAY ON SUPERVISING STATION PANEL

FIRE ALARM HORN/STROBE ASSEMBLY

Public Input No. 456-NFPA 72-2022 [Section No. A.7.5.5.2]

A.7.5.5.2

For an example of a logic diagram, see A.14.6.1.1(a) and for an example of an input/output matrix of operation, see A.14.6.1.1(b) .

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_Figure_A.14.6.1.1_a_Final_002_.1653601205227.pdf	Logic Diagram	

Statement of Problem and Substantiation for Public Input

Provide consistent language among paragraphs related to the sequence of operation and add logic diagram as a means to depict the sequence of operation.

In addition to a narrative or an input/output matrix, a logic diagram is also a valid method to document the sequence of operation of a system. Sections of the Code that currently refer to documenting the sequence of operation only refer to a narrative description and/or an input/output matrix. Approvers of system design documentation are sometimes hesitant to approve or will not approve a design without a narrative or an input /output matrix even when a logic diagram is part of the design and provides more concise information, because NFPA 72 doesn't include a logic diagram as means to show the sequence of operation.

A logic diagram depicts the sequence of operation in easy-to-understand graphics, by interconnection of symbols representing the design of the entire system, not only showing the output for various inputs, but also the inter-working relationship between hardware and software within the system. A typical logic diagram will include internal components such as monitor modules, control modules, control relays, program addresses and custom messages for system inputs required for actuation of evacuation signals and ancillary functions for the intended sequence of operation. A logic diagram is particularly useful for addressable systems where an enormous amount of information representing the sequence of operation is required in large buildings or complex systems, whereas an input/output matrix is often confusing to produce and read (so many dots) when the system is large or complex. (NFPA 72 Figure A.14.6.1.1, for example, shows duplicate entries for 1st floor detectors, no 2nd floor detectors, and duct detectors that actuate alarm signals).

Older model addressable systems that require panel upgrades (CPU) for maintenance issues will come with firmware versions that won't likely support the older model software revision. In fact the older software revision software may require out of date laptop computer software (i.e., windows 98) to read it. The software media required to be controlled by NFPA 72 in cases such as this could be useless. A good logic diagram in a design is capable of providing the programming information necessary to restore the original sequence of operation because all programmable hardware is shown on the drawing with custom messages and program addresses.

A logic diagram is also a useful tool to convey detailed programming information to the programmer to ensure that site-specific software is configured to meet the owner's intended sequence of operation. Some facilities for example may be directed to implement software design control processes (i.e., NQA-1, Quality Assurance Requirements for Nuclear Facility Applications) that identify and document software design requirements including the operating system, function, interfaces, performance criteria, and design inputs of a computer program, such as site-specific fire alarm programs that can be created or modified. These software design requirements can be met with a logic diagram whereas an input/output matrix lacks interconnection detail between hardware and software.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 315-NFPA 72-2022 [Section No. 7.2.1]	

Submitter Information Verification

Submitter Full Name: Herbert Hurst
Organization: Savannah River Nuclear Solutio
Street Address:
City:
State:
Zip:
Submittal Date: Fri May 27 09:07:37 EDT 2022
Committee: SIG-FUN

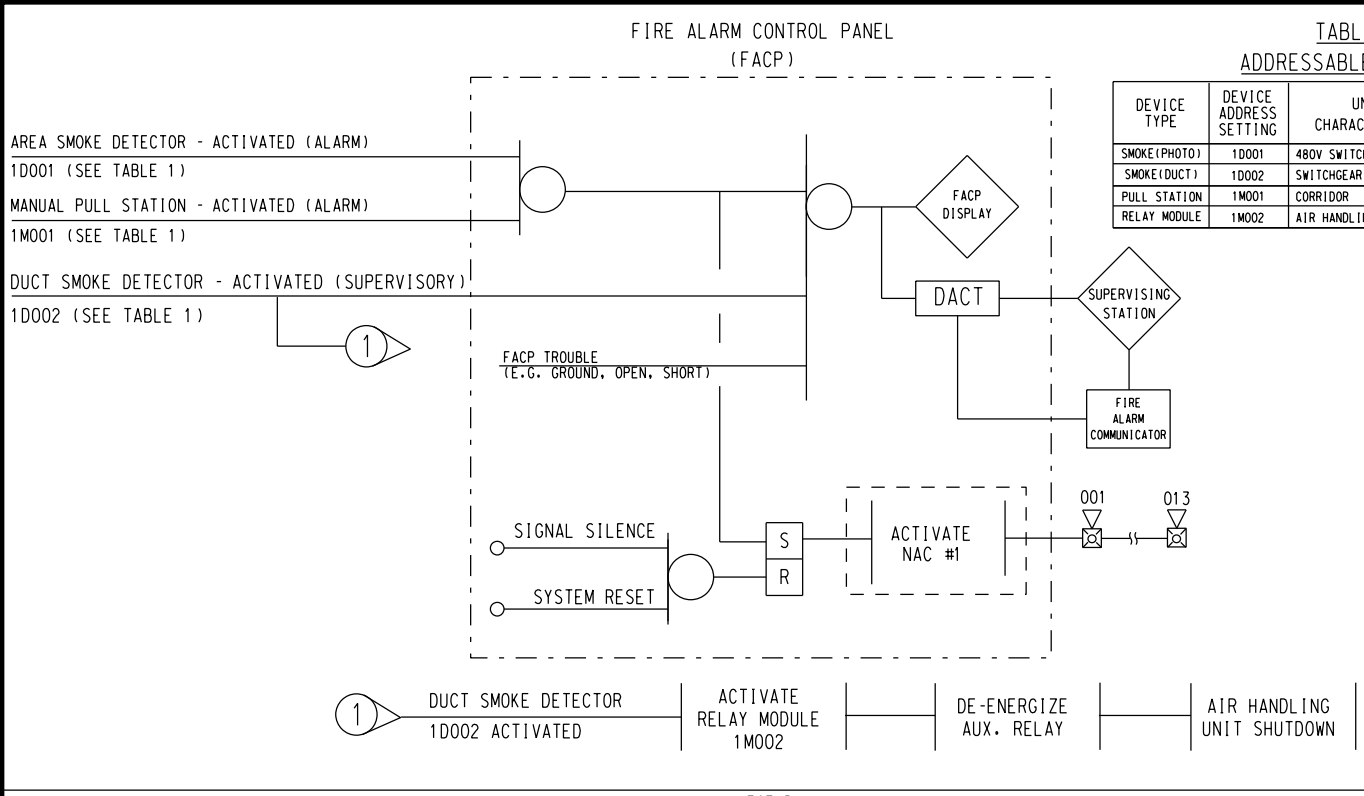


TABLE 1
ADDRESSABLE DEVICES

DEVICE TYPE	DEVICE ADDRESS SETTING	UNIQUE CHARACTER LABEL	CHARACTER LABEL EXTENSION
SMOKE(PHOTO)	1D001	480V SWITCHGEAR ROOM	DETECTOR
SMOKE(DUCT)	1D002	SWITCHGEAR ROOM	DUCT DETECTOR
PULL STATION	1M001	CORRIDOR	PULL STATION
RELAY MODULE	1M002	AIR HANDLING UNIT	SHUTDOWN

LEGEND

MANUAL INPUT ● — MAINTAINED HAND SWITCH INPUT

MANUAL INPUT ○ — MOMENTARY HAND SWITCH INPUT

OUTPUT EXIST WHEN ONE OR MORE INPUTS ARE PRESENT

OUTPUT ACTION — INITIATE NAC #1 — ACTION DESCRIPTION

MEMORY

A — S — C
B — R

LOGIC OUTPUT "C" EXIST AS SOON AS INPUT "A" EXISTS. "C" CONTINUES TO EXIST REGARDLESS OF SUBSEQUENT STATE OF "A" UNTIL RESET INPUT "B" IS PRESENT. "C" REMAINS REGARDLESS OF SUBSEQUENT STATE OF "B" UNTIL "A" CAUSES THE MEMORY TO BE SET.

SUPERVISING STATION — ANNUNCIATOR/LED READ OUT DISPLAY ON SUPERVISING STATION PANEL

FIRE ALARM HORN/STROBE ASSEMBLY

Public Input No. 576-NFPA 72-2022 [Section No. A.7.5.5.2]

A.7.5.5.2

For an example of an input/output matrix of operation, see A.14.6.1.1. The actually programmed sequence of operation should include all applicable items found in the list for 7.4.9.

Statement of Problem and Substantiation for Public Input

It is critical that the Owner receives a copy of the sequence of operation that is actually programmed into the fire alarm system. As such, a detailed list is included in PI No. 575 and should be referenced in this Annex material so reference is made back to this inclusive list.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 575-NFPA 72-2022 [Section No. 7.4.9]	Reference to detailed list

Submitter Information Verification

Submitter Full Name: Larry Rietz
Organization: Jensen Hughes
Street Address:
City:
State:
Zip:
Submittal Date: Wed Jun 01 17:44:20 EDT 2022
Committee: SIG-FUN

Public Input No. 85-NFPA 72-2022 [Section No. A.7.5.6.6.3]

A.7.5.6.6.3 ~~3~~ 4

It is the intent that if an original or current record of completion is not available for the overall system, the installer would provide a new record of completion that addresses items discovered about the system. The installer will complete the respective sections related to the overall system that have been discovered under the current scope of work. It is not the intent of this section to require an in-depth evaluation of an existing system solely for the purpose of completing a system-wide record of completion.

Statement of Problem and Substantiation for Public Input

This PI links with PI-82 and PI-84. If accepted/revised, this annex paragraph will require renumbering.
Substantiation from PI-82: NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue.
Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text creates a new section and provides new paragraphs for each requirement.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 82-NFPA 72-2022 [Section No. 7.5.6.6.1]	renumber

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Sat Jan 15 20:11:11 EST 2022
Committee: SIG-FUN

Public Input No. 81-NFPA 72-2022 [New Section after A.7.7.1.2]

A.7.6.6

Figure 7.6.6(a) through Figure 7.6.6(f) are sample forms intended to reflect the general information that should be provided by the system and testing contractor at the time of a system test. However, they are not intended to mandate a specific format for the report. A report format customized to the specific system configuration, devices, appliances, and system functions being tested meets the intent of the requirement. If these forms are used, they can be modified as needed to provide a more complete and/or clear record, along with additional sheets, data, or calculations as necessary.

In Figure 7.6.6(e) , Section 2.1 , an example of a single-voice-channel emergency communications system is a system that provides a single message or evacuation signal to multiple floors or areas at the same time. An example of a multiple-voice-channel emergency communications system is a system that can provide multiple messages or evacuation signals to multiple floors or areas at the same time.

Figure 7.6.6(a) System Record of Inspection and Testing.

SYSTEM RECORD OF INSPECTION AND TESTING

This form is to be completed by the system inspection and testing contractor at the time of a system test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.
Attach additional sheets, data, or calculations as necessary to provide a complete record.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Supplemental Form(s) Attached: _____ (yes/no)

1. PROPERTY INFORMATION

Name of property: _____
Address: _____
Description of property: _____
Name of property representative: _____
Address: _____
Phone: _____ Fax: _____ E-mail: _____

2. TESTING AND MONITORING INFORMATION

Testing organization: _____
Address: _____
Phone: _____ Fax: _____ E-mail: _____
Monitoring organization: _____
Address: _____
Phone: _____ Fax: _____ E-mail: _____
Account number: _____ Phone line 1: _____ Phone line 2: _____
Means of transmission: _____
Entity to which alarms are retransmitted: _____ Phone: _____

3. DOCUMENTATION

Onsite location of the required record documents and site-specific software: _____

4. DESCRIPTION OF SYSTEM OR SERVICE

4.1 Control Unit

Manufacturer: _____ Model number: _____

4.2 Software Firmware

Firmware revision number: _____

4.3 System Power

4.3.1 Primary (Main) Power

Nominal voltage: _____ Amps: _____ Location: _____
Overcurrent protection type: _____ Amps: _____ Disconnecting means location: _____

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

4. DESCRIPTION OF SYSTEM OR SERVICE *(continued)*

4.3.2 Secondary Power

Type: _____ Location: _____

Battery type (if applicable): _____

Calculated capacity of batteries to drive the system:

In standby mode (hours): _____ In alarm mode (minutes): _____

5. NOTIFICATIONS MADE PRIOR TO TESTING

Monitoring organization	Contact: _____	Time: _____
Building management	Contact: _____	Time: _____
Building occupants	Contact: _____	Time: _____
Authority having jurisdiction	Contact: _____	Time: _____
Other, if required	Contact: _____	Time: _____

6. TESTING RESULTS

6.1 Control Unit and Related Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground-fault monitoring	❑	❑	
Supervision	❑	❑	
Local annunciator	❑	❑	
Remote annunciators	❑	❑	
Remote power panels	❑	❑	

6.2 Secondary Power

Description	Visual Inspection	Functional Test	Comments
Battery condition	❑	❑	
Load voltage	❑	❑	
Discharge test	❑	❑	
Charger test	❑	❑	
Remote panel batteries	❑	❑	
Batteries marked with date of manufacture	❑	❑	

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

6. TESTING RESULTS *(continued)*

6.3 Alarm and Supervisory Alarm Initiating Device

Attach supplementary device test sheets for all initiating devices.

6.4 Notification Appliances

Attach supplementary appliance test sheets for all notification appliances.

6.5 Interface Equipment

Attach supplementary interface component test sheets for all interface components.

Circuit Interface / Signaling Line Circuit Interface / Fire Alarm Control Interface

6.6 Supervising Station Monitoring

Description	Yes	No	Time	Comments
Alarm signal	❑	❑		
Alarm restoration	❑	❑		
Trouble signal	❑	❑		
Trouble restoration	❑	❑		
Supervisory signal	❑	❑		
Supervisory restoration	❑	❑		

6.7 Public Emergency Alarm Reporting System

Description	Yes	No	Time	Comments
Alarm signal	❑	❑		
Alarm restoration	❑	❑		
Trouble signal	❑	❑		
Trouble restoration	❑	❑		
Supervisory signal	❑	❑		
Supervisory restoration	❑	❑		

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

7. NOTIFICATIONS THAT TESTING IS COMPLETE

Monitoring organization	Contact: _____	Time: _____
Building management	Contact: _____	Time: _____
Building occupants	Contact: _____	Time: _____
Authority having jurisdiction	Contact: _____	Time: _____
Other, if required	Contact: _____	Time: _____

8. SYSTEM RESTORED TO NORMAL OPERATION

Date: _____ Time: _____

9. CERTIFICATION

This system as specified herein has been inspected and tested according to NFPA 72, _____ edition, Chapter 14.

Signed: _____ Printed name: _____ Date: _____

Organization: _____ Title: _____ Phone: _____

Qualifications (refer to 10.6.3): _____

10. DEFECTS OR MALFUNCTIONS NOT CORRECTED AT CONCLUSION OF SYSTEM INSPECTION, TESTING, OR MAINTENANCE

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

10.1 Acceptance by Owner or Owner's Representative:

The undersigned accepted the test report for the system as specified herein:

Signed: _____ Printed name: _____ Date: _____

Organization: _____ Title: _____ Phone: _____

© 2021 National Fire Protection Association

Figure 7.6.6(b) Notification Appliance Supplementary Record of Inspection and Testing.

NOTIFICATION APPLIANCE SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes a notification appliance test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. NOTIFICATION APPLIANCE TEST RESULTS

Appliance Type	Location/Identifier	Test Results

© 2021 National Fire Protection Association NFPA 72 (p. 1 of 2)

NOTIFICATION APPLIANCE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. NOTIFICATION APPLIANCE TEST RESULTS *(continued)*

Appliance Type	Location/Identifier	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association NFPA 72 (p. 2 of 2)

Figure 7.6.6(c) Initiating Device Supplementary Record of Inspection and Testing.

INITIATING DEVICE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes an initiating device test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. INITIATING DEVICE TEST RESULTS

Device Type	Address	Location	Test Results

© 2021 National Fire Protection Association

INITIATING DEVICE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. INITIATING DEVICE TEST RESULTS *(continued)*

Device Type	Address	Location	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association NFPA 72 (p. 2 of 2)

Figure 7.6.6(d) Mass Notification System Supplementary Record of Inspection and Testing.

MASS NOTIFICATION SYSTEM
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes a mass notification system test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. MASS NOTIFICATION SYSTEM

2.1 System Type

❑ In-building MNS—combination

❑ In-building MNS—stand alone ❑ Wide-area MNS ❑ Distributed recipient MNS

❑ Other (specify): _____

2.2 System Features

❑ Combination fire alarm/MNS ❑ MNS ACU only ❑ Wide-area MNS to regional national alerting interface

❑ Local operating console (LOC) ❑ Direct recipient MNS (DRMNS) ❑ Wide-area MNS to DRMNS interface

❑ Wide-area MNS to high-power loudspeaker array (HPLA) interface ❑ In-building MNS to wide-area MNS interface

❑ Other (specify): _____

3. IN-BUILDING MASS NOTIFICATION SYSTEM

3.1 Primary Power

Input voltage of MNS panel: _____ MNS panel amps: _____

3.2 Engine-Driven Generator ❑ This system does not have a generator.

Location of generator: _____

Location of fuel storage: _____ Type of fuel: _____

3.3 Stored-Energy Emergency Power Supply Systems ❑ This system does not have an SEPSS.

Equipment powered by an SEPSS: _____

Location of SEPSS: _____

Calculated capacity of SEPSS batteries to drive the system components connected to it:

In standby mode (hours): _____ In alarm mode (minutes): _____

3.4 Batteries

Location: _____ Type: _____ Nominal voltage: _____ Amp/hour rating: _____

Calculated capacity of batteries to drive the system:

In standby mode (hours): _____ In alarm mode (minutes): _____

❑ Batteries are marked with date of manufacture.

© 2021 National Fire Protection Association

MASS NOTIFICATION SYSTEM
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. MASS NOTIFICATION EQUIPMENT TEST RESULTS

Description	Visual Inspection	Functional Test	Comments
Functional test			
Reset/power down test			
Fuses			
Primary power supply			
SEPSS power test			
Trouble signals			
Disconnect switches			
Ground-fault monitoring			
CCU security mechanism			
Prerecorded message content			
Prerecorded message activation			
Software backup performed			
Test backup software			
Fire alarm to MNS interface			
MNS to fire alarm interface			
In-building MNS to wide-area MNS			
MNS to direct recipient MNS			
Sound pressure levels Occupied ❑ Yes ❑ No Ambient dBA:_____ Alarm dBA:_____ (attach supplementary notification appliance form(s) with locations, values, and weather conditions)			
System intelligibility Test method:_____ Score:_____ CIS value: _____ (attach supplementary notification appliance form(s) with locations, values, and weather conditions)			
Other (specify):			

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association NFPA 72 (p. 2 of 2)

Figure 7.6.6(e) Emergency Communications Systems Supplementary Record of Inspection and Testing.

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes systems and components specific to emergency communication systems.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. DESCRIPTION OF SYSTEM OR SERVICE

❑ Fire alarm with in-building fire emergency voice alarm communications system (EVAC)

❑ Mass notification system

❑ Combination system, with the following components:

❑ Fire alarm ❑ EVACS ❑ MNS ❑ Two-way, in-building, emergency communications system

❑ Other (specify): _____

Additional description of system(s): _____

_____

2.1 In-Building Fire Emergency Voice Alarm Communications System

Manufacturer: _____ Model number: _____

Number of single voice alarm channels: _____ Number of multiple voice alarm channels: _____

Number of loudspeakers: _____ Number of loudspeaker circuits: _____

Location of amplification and sound processing equipment: _____

_____

_____

Location of paging microphone stations:

Location 1: _____

Location 2: _____

Location 3: _____

2.2 Mass Notification System

2.2.1 System Type:

❑ In-building MNS—combination

❑ In-building MNS ❑ Wide-area MNS ❑ Distributed recipient MNS

❑ Other (specify): _____

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. DESCRIPTION OF SYSTEM OR SERVICE *(continued)*

2.2.2 System Features:

❑ Combination fire alarm/MNS ❑ MNS autonomous control unit ❑ Wide-area MNS to regional national alerting interface
❑ Local operating console (LOC) ❑ Distributed-recipient MNS (DRMNS) ❑ Wide-area MNS to DRMNS interface
❑ Wide-area MNS to high-power loudspeaker array (HPLA) interface ❑ In-building MNS to wide-area MNS interface
❑ Other (specify): _____

2.2.3 MNS Local Operating Consoles

Location 1: _____
Location 2: _____
Location 3: _____

2.2.4 High-Power Loudspeaker Arrays

Number of HPLA loudspeaker initiation zones: _____
Location 1: _____
Location 2: _____
Location 3: _____

2.2.5 Mass Notification Devices

Combination fire alarm/MNS visual devices: _____ MNS-only visual devices: _____
Textual signs: _____ Other (describe): _____
Supervision class: _____

2.2.6 Special Hazard Notification

❑ This system does not have special suppression pre-discharge notification
❑ MNS systems DO NOT override notification appliances required to provide special suppression pre-discharge notification

3. TWO-WAY EMERGENCY COMMUNICATION SYSTEMS

3.1 Telephone System

Number of telephone jacks installed: _____ Number of warden stations installed: _____
Number of telephone handsets stored on site: _____
Type of telephone system installed: ❑ Electrically powered ❑ Sound powered

3.2 Area of Refuge Emergency Communications Systems

Number of stations: _____ Location of central control point: _____
Days and hours when central control point is attended: _____
Location of alternate control point: _____
Days and hours when alternate control point is attended: _____

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

3. TWO-WAY EMERGENCY COMMUNICATIONS SYSTEMS *(continued)*

3.3 Elevator Emergency Communications Systems

Number of elevators with stations: _____ Location of central control point: _____

Days and hours when central control point is attended: _____

Location of alternate control point: _____

Days and hours when alternate control point is attended: _____

3.4 Other Two-Way Communications System

Describe: _____

4. TESTING RESULTS

4.1 Control Unit and Related Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
Supervision	❑	❑	
Local annunciator	❑	❑	
Remote annunciators	❑	❑	
Remote power panels	❑	❑	
Other:	❑	❑	

4.2 Secondary Power

Description	Visual Inspection	Functional Test	Comments
Battery condition	❑	❑	
Load voltage	❑	❑	
Discharge test	❑	❑	
Charger test	❑	❑	
Remote panel batteries	❑	❑	

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. TESTING RESULTS *(continued)*

4.3 Emergency Communications Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Secondary power supply	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
Panel supervision	❑	❑	
System performance	❑	❑	
System audibility	❑	❑	
System intelligibility	❑	❑	
Other:	❑	❑	

4.4 Mass Notification Equipment

Description	Visual Inspection	Functional Test	Comments
Functional test	❑	❑	
Reset/Power down test	❑	❑	
Fuses	❑	❑	
Primary power supply	❑	❑	
SEPSS power test	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
CCU security mechanism	❑	❑	
Prerecorded message content	❑	❑	
Prerecorded message activation	❑	❑	
Software backup performed	❑	❑	
Test backup software	❑	❑	
Fire alarm to MNS Interface	❑	❑	
MNS to fire alarm interface	❑	❑	
In-building MNS to wide-area MNS	❑	❑	
MNS to direct recipient MNS	❑	❑	

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. TESTING RESULTS *(continued)*

4.4 Mass Notification Equipment *(continued)*

Description	Visual Inspection	Functional Test	Comments
Sound pressure levels (attach report with locations, values, and weather conditions)	❑	❑	
System intelligibility ❑ CSI ❑ STI (attach report with locations, values, and weather conditions)	❑	❑	
Other:	❑	❑	

4.5 Two-Way Communication Equipment

Description	Visual Inspection	Functional Test	Comments
Phone handsets	❑	❑	
Phone jacks	❑	❑	
Off-hook indicator	❑	❑	
Call-in signal	❑	❑	
System performance	❑	❑	
System audibility	❑	❑	
System intelligibility	❑	❑	
Other:	❑	❑	

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association *NFPA 72 (p. 5 of 5)*

Figure 7.6.6(f) Interface Component Supplementary Record of Inspection and Testing.

INTERFACE COMPONENT
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes an interface component test record for circuit interfaces, signaling line circuit interfaces, and fire alarm control interfaces.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. INTERFACE COMPONENT TEST RESULTS

Interface Component Type	Address	Location	Test Results

© 2021 National Fire Protection Association

INTERFACE COMPONENT
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. INTERFACE COMPONENT TEST RESULTS *(continued)*

Interface Component Type	Address	Location	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Figure 7.8.2(m) Installation and Inspection Form Single- and Multiple-Station Alarms and Household Fire Alarm Systems.

INSTALLATION AND INSPECTION FORM
SINGLE- AND MULTIPLE-STATION ALARMS AND
HOUSEHOLD FIRE ALARM SYSTEMS

This form is to be completed at the time of installation/final inspection of any household fire alarm system and single- or multiple-station alarms. It shall be permitted to modify this form as required to provide a more complete and/or clear record.
Insert N/A in all unused lines.
Attach additional sheets, data, or calculations as necessary to complete form.

Form Completion Date: _____ Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Property Owner: _____
Address: _____
Phone: _____ E-Mail: _____ Other: _____

2. INSTALLATION, CONTRACTOR, AND MONITORING INFORMATION

Installation Contractor: _____
Address: _____
Phone: _____ E-Mail: _____ Other: _____

2.1 Type of Off-Premises Notification

Monitoring Organization: _____
Address: _____
Phone: _____ E-Mail: _____ Other: _____
Account Number: _____ Means of Transmission: _____

3. DESCRIPTION OF SYSTEM OR SERVICE

NFPA 72 Edition: _____

3.1 Type of System

❑ Single-Station ❑ Multiple-Station ❑ Household Fire Alarm System ❑ Carbon Monoxide Alarm System

3.2 Number of Devices

Single-Station Smoke Alarms: _____ Multiple-Station Smoke Alarms: _____
Single-Station Heat Alarms: _____ Multiple-Station Heat Alarms: _____
Single-Station Carbon Monoxide Alarms: _____ Multiple-Station Carbon Monoxide Alarms: _____
System Smoke Detectors: _____ System Heat Detectors: _____
Waterflow Switches: _____
Notification Appliances: _____ Type: _____
Interfaced/Other Equipment: _____

3.3 Location (L) and Date (D) of Devices

Device type, location and manufacture date of devices (date shown on back of devices)

_____ _____ _____ _____
_____ _____ _____ _____
_____ _____ _____ _____

Electrical Panel (L): _____ Breaker Number: _____
Alarm Control Unit (L): _____ Battery Back-up (D): _____
Plug in Transformer (L): _____
Relay for Interconnection (L): _____

4. PREPARED BY

Signed: _____ Printed Name: _____ Date: _____
Title: _____ Organization: _____

© 2021 National Fire Protection Association NFPA 72

Additional Proposed Changes

File Name	Description	Approved
Edits_to_I_T_Form.docx		

Statement of Problem and Substantiation for Public Input

This PI calls for Section 7.6.6 to be the placeholder for the annex note currently located at A.7.8.2.(2), pointing the reader to a new Section A.7.6.6 rather
than to Section 7.8.2 for sample forms for Inspection and Testing. Furthermore, the requirement in this section for a
record of inspection and testing more correctly points to the true basis of the forms, namely Chapter 14's requirements.

This is linked to a related PI calling for the deletion of the Inspection and Testing forms from Chapter 7

and a relocation of those same forms to A.7.6.6

Relocation (not removal) of the inspection and testing sample forms to the annex concurs with what the Code's intent has been all along (and which is stated clearly in the Annex)
which is that the forms are to serve as a guide, not a mandate. The AHJ can still mandate that these sample forms be used but in line with the Annex material currently in A.7.8.2(2), these sample forms should not be in the body of the Code. (Note: In line with the proposed move of these forms to the Annex, much of the italicized explanatory language at the beginning of each form has been incorporated into the annex note itself. See attached document. for a visual of this).

The annex note in this PI is currently found in Section A.7.8.2(2) but has been edited with regard to the form figures that appear immediately afterward.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 80-NFPA 72-2022 [Section No. 7.6.6]	
Public Input No. 67-NFPA 72-2022 [Section No. 7.8.2]	
Public Input No. 68-NFPA 72-2022 [Section No. A.7.8.2(2)]	
Public Input No. 67-NFPA 72-2022 [Section No. 7.8.2]	
Public Input No. 68-NFPA 72-2022 [Section No. A.7.8.2(2)]	
Public Input No. 80-NFPA 72-2022 [Section No. 7.6.6]	

Submitter Information Verification

Submitter Full Name: Joe Scibetta
Organization: BuildingReports
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 14 17:01:02 EST 2022
Committee: SIG-FUN

Figure 7.8.2(~~a~~a) System Record of Inspection and Testing.

SYSTEM RECORD OF INSPECTION AND TESTING

This form is to be completed by the system inspection and testing contractor at the time of a system test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.
Attach additional sheets, data, or calculations as necessary to provide a complete record.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Supplemental Form(s) Attached: _____ (yes/no)

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

Description of property: _____

Name of property representative: _____

Address: _____

Phone: _____ Fax: _____ E-mail: _____

2. TESTING AND MONITORING INFORMATION

Testing organization: _____

Address: _____

Phone: _____ Fax: _____ E-mail: _____

Monitoring organization: _____

Address: _____

Phone: _____ Fax: _____ E-mail: _____

Account number: _____ Phone line 1: _____ Phone line 2: _____

Means of transmission: _____

Entity to which alarms are retransmitted: _____ Phone: _____

3. DOCUMENTATION

Onsite location of the required record documents and site-specific software: _____

4. DESCRIPTION OF SYSTEM OR SERVICE

4.1 Control Unit

Manufacturer: _____ Model number: _____

4.2 Software Firmware

Firmware revision number: _____

4.3 System Power

4.3.1 Primary (Main) Power

Nominal voltage: _____ Amps: _____ Location: _____

Overcurrent protection type: _____ Amps: _____ Disconnecting means location: _____

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

4. DESCRIPTION OF SYSTEM OR SERVICE *(continued)*

4.3.2 Secondary Power

Type: _____ Location: _____

Battery type (if applicable): _____

Calculated capacity of batteries to drive the system:

In standby mode (hours): _____ In alarm mode (minutes): _____

5. NOTIFICATIONS MADE PRIOR TO TESTING

Monitoring organization	Contact: _____	Time: _____
Building management	Contact: _____	Time: _____
Building occupants	Contact: _____	Time: _____
Authority having jurisdiction	Contact: _____	Time: _____
Other, if required	Contact: _____	Time: _____

6. TESTING RESULTS

6.1 Control Unit and Related Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground-fault monitoring	❑	❑	
Supervision	❑	❑	
Local annunciator	❑	❑	
Remote annunciators	❑	❑	
Remote power panels	❑	❑	

6.2 Secondary Power

Description	Visual Inspection	Functional Test	Comments
Battery condition	❑	❑	
Load voltage	❑	❑	
Discharge test	❑	❑	
Charger test	❑	❑	
Remote panel batteries	❑	❑	
Batteries marked with date of manufacture	❑	❑	

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

6. TESTING RESULTS *(continued)*

6.3 Alarm and Supervisory Alarm Initiating Device

Attach supplementary device test sheets for all initiating devices.

6.4 Notification Appliances

Attach supplementary appliance test sheets for all notification appliances.

6.5 Interface Equipment

Attach supplementary interface component test sheets for all interface components.

Circuit Interface / Signaling Line Circuit Interface / Fire Alarm Control Interface

6.6 Supervising Station Monitoring

Description	Yes	No	Time	Comments
Alarm signal	❑	❑		
Alarm restoration	❑	❑		
Trouble signal	❑	❑		
Trouble restoration	❑	❑		
Supervisory signal	❑	❑		
Supervisory restoration	❑	❑		

6.7 Public Emergency Alarm Reporting System

Description	Yes	No	Time	Comments
Alarm signal	❑	❑		
Alarm restoration	❑	❑		
Trouble signal	❑	❑		
Trouble restoration	❑	❑		
Supervisory signal	❑	❑		
Supervisory restoration	❑	❑		

© 2021 National Fire Protection Association

SYSTEM RECORD OF INSPECTION AND TESTING *(continued)*

7. NOTIFICATIONS THAT TESTING IS COMPLETE

Monitoring organization	Contact: _____	Time: _____
Building management	Contact: _____	Time: _____
Building occupants	Contact: _____	Time: _____
Authority having jurisdiction	Contact: _____	Time: _____
Other, if required	Contact: _____	Time: _____

8. SYSTEM RESTORED TO NORMAL OPERATION

Date: _____ Time: _____

9. CERTIFICATION

This system as specified herein has been inspected and tested according to NFPA 72, _____edition, Chapter 14.

Signed: _____ Printed name: _____ Date: _____

Organization: _____ Title: _____ Phone: _____

Qualifications (refer to 10.6.3): _____

10. DEFECTS OR MALFUNCTIONS NOT CORRECTED AT CONCLUSION OF SYSTEM INSPECTION, TESTING, OR MAINTENANCE

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

10.1 Acceptance by Owner or Owner's Representative:

The undersigned accepted the test report for the system as specified herein:

Signed: _____ Printed name: _____ Date: _____

Organization: _____ Title: _____ Phone: _____

© 2021 National Fire Protection Association

Figure 7.8.2(~~h~~b) Notification Appliance Supplementary Record of Inspection and Testing.

NOTIFICATION APPLIANCE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes a notification appliance test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. NOTIFICATION APPLIANCE TEST RESULTS

Appliance Type	Location/Identifier	Test Results

© 2021 National Fire Protection Association

NOTIFICATION APPLIANCE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. NOTIFICATION APPLIANCE TEST RESULTS *(continued)*

Appliance Type	Location/Identifier	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Figure 7.8.2(~~i~~c) Initiating Device Supplementary Record of Inspection and Testing.

INITIATING DEVICE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes an initiating device test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. INITIATING DEVICE TEST RESULTS

Device Type	Address	Location	Test Results

© 2021 National Fire Protection Association

INITIATING DEVICE
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. INITIATING DEVICE TEST RESULTS *(continued)*

Device Type	Address	Location	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Figure 7.8.2(jd) Mass Notification System Supplementary Record of Inspection and Testing.

MASS NOTIFICATION SYSTEM
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes a mass notification system test record.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. MASS NOTIFICATION SYSTEM

2.1 System Type

❑ In-building MNS—combination

❑ In-building MNS—stand alone ❑ Wide-area MNS ❑ Distributed recipient MNS

❑ Other (specify): _____

2.2 System Features

❑ Combination fire alarm/MNS ❑ MNS ACU only ❑ Wide-area MNS to regional national alerting interface

❑ Local operating console (LOC) ❑ Direct recipient MNS (DRMNS) ❑ Wide-area MNS to DRMNS interface

❑ Wide-area MNS to high-power loudspeaker array (HPLA) interface ❑ In-building MNS to wide-area MNS interface

❑ Other (specify): _____

3. IN-BUILDING MASS NOTIFICATION SYSTEM

3.1 Primary Power

Input voltage of MNS panel: _____ MNS panel amps: _____

3.2 Engine-Driven Generator ❑ This system does not have a generator.

Location of generator: _____

Location of fuel storage: _____ Type of fuel: _____

3.3 Stored-Energy Emergency Power Supply Systems ❑ This system does not have an SEPSS.

Equipment powered by an SEPSS: _____

Location of SEPSS: _____

Calculated capacity of SEPSS batteries to drive the system components connected to it:

In standby mode (hours): _____ In alarm mode (minutes): _____

3.4 Batteries

Location: _____ Type: _____ Nominal voltage: _____ Amp/hour rating: _____

Calculated capacity of batteries to drive the system:

In standby mode (hours): _____ In alarm mode (minutes): _____

❑ Batteries are marked with date of manufacture.

© 2021 National Fire Protection Association

MASS NOTIFICATION SYSTEM
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. MASS NOTIFICATION EQUIPMENT TEST RESULTS

Description	Visual Inspection	Functional Test	Comments
Functional test			
Reset/power down test			
Fuses			
Primary power supply			
SEPSS power test			
Trouble signals			
Disconnect switches			
Ground-fault monitoring			
CCU security mechanism			
Prerecorded message content			
Prerecorded message activation			
Software backup performed			
Test backup software			
Fire alarm to MNS interface			
MNS to fire alarm interface			
In-building MNS to wide-area MNS			
MNS to direct recipient MNS			
Sound pressure levels Occupied ❑ Yes ❑ No Ambient dBA:_____ Alarm dBA:_____ (attach supplementary notification appliance form(s) with locations, values, and weather conditions)			
System intelligibility Test method:_____ Score:_____ CIS value:_____ (attach supplementary notification appliance form(s) with locations, values, and weather conditions)			
Other (specify):			

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Figure 7.8.2(~~k~~e) Emergency Communications Systems Supplementary Record of Inspection and Testing.

EMERGENCY COMMUNICATIONS SYSTEMS SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes systems and components specific to emergency communication systems.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. DESCRIPTION OF SYSTEM OR SERVICE

❑ Fire alarm with in-building fire emergency voice alarm communications system (EVAC)

❑ Mass notification system

❑ Combination system, with the following components:

❑ Fire alarm ❑ EVACS ❑ MNS ❑ Two-way, in-building, emergency communications system

❑ Other (specify): _____

Additional description of system(s): _____

_____

2.1 In-Building Fire Emergency Voice Alarm Communications System

Manufacturer: _____ Model number: _____

Number of single voice alarm channels: _____ Number of multiple voice alarm channels: _____

Number of loudspeakers: _____ Number of loudspeaker circuits: _____

Location of amplification and sound processing equipment: _____

_____

_____

Location of paging microphone stations:

Location 1: _____

Location 2: _____

Location 3: _____

2.2 Mass Notification System

2.2.1 System Type:

❑ In-building MNS—combination

❑ In-building MNS ❑ Wide-area MNS ❑ Distributed recipient MNS

❑ Other (specify): _____

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. DESCRIPTION OF SYSTEM OR SERVICE *(continued)*

2.2.2 System Features:

❑ Combination fire alarm/MNS ❑ MNS autonomous control unit ❑ Wide-area MNS to regional national alerting interface

❑ Local operating console (LOC) ❑ Distributed-recipient MNS (DRMNS) ❑ Wide-area MNS to DRMNS interface

❑ Wide-area MNS to high-power loudspeaker array (HPLA) interface ❑ In-building MNS to wide-area MNS interface

❑ Other (specify): _____

2.2.3 MNS Local Operating Consoles

Location 1: _____

Location 2: _____

Location 3: _____

2.2.4 High-Power Loudspeaker Arrays

Number of HPLA loudspeaker initiation zones: _____

Location 1: _____

Location 2: _____

Location 3: _____

2.2.5 Mass Notification Devices

Combination fire alarm/MNS visual devices: _____ MNS-only visual devices: _____

Textual signs: _____ Other (describe): _____

Supervision class: _____

2.2.6 Special Hazard Notification

❑ This system does not have special suppression pre-discharge notification

❑ MNS systems DO NOT override notification appliances required to provide special suppression pre-discharge notification

3. TWO-WAY EMERGENCY COMMUNICATION SYSTEMS

3.1 Telephone System

Number of telephone jacks installed: _____ Number of warden stations installed: _____

Number of telephone handsets stored on site: _____

Type of telephone system installed: ❑ Electrically powered ❑ Sound powered

3.2 Area of Refuge Emergency Communications Systems

Number of stations: _____ Location of central control point: _____

Days and hours when central control point is attended: _____

Location of alternate control point: _____

Days and hours when alternate control point is attended: _____

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

3. TWO-WAY EMERGENCY COMMUNICATIONS SYSTEMS *(continued)*

3.3 Elevator Emergency Communications Systems

Number of elevators with stations: _____ Location of central control point: _____

Days and hours when central control point is attended: _____

Location of alternate control point: _____

Days and hours when alternate control point is attended: _____

3.4 Other Two-Way Communications System

Describe: _____

4. TESTING RESULTS

4.1 Control Unit and Related Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
Supervision	❑	❑	
Local annunciator	❑	❑	
Remote annunciators	❑	❑	
Remote power panels	❑	❑	
Other:	❑	❑	

4.2 Secondary Power

Description	Visual Inspection	Functional Test	Comments
Battery condition	❑	❑	
Load voltage	❑	❑	
Discharge test	❑	❑	
Charger test	❑	❑	
Remote panel batteries	❑	❑	

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. TESTING RESULTS *(continued)*

4.3 Emergency Communications Equipment

Description	Visual Inspection	Functional Test	Comments
Control unit	❑	❑	
Lamps/LEDs/LCDs	❑	❑	
Fuses	❑	❑	
Secondary power supply	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
Panel supervision	❑	❑	
System performance	❑	❑	
System audibility	❑	❑	
System intelligibility	❑	❑	
Other:	❑	❑	

4.4 Mass Notification Equipment

Description	Visual Inspection	Functional Test	Comments
Functional test	❑	❑	
Reset/Power down test	❑	❑	
Fuses	❑	❑	
Primary power supply	❑	❑	
SEPSS power test	❑	❑	
Trouble signals	❑	❑	
Disconnect switches	❑	❑	
Ground fault monitoring	❑	❑	
CCU security mechanism	❑	❑	
Prerecorded message content	❑	❑	
Prerecorded message activation	❑	❑	
Software backup performed	❑	❑	
Test backup software	❑	❑	
Fire alarm to MNS Interface	❑	❑	
MNS to fire alarm interface	❑	❑	
In-building MNS to wide-area MNS	❑	❑	
MNS to direct recipient MNS	❑	❑	

© 2021 National Fire Protection Association

EMERGENCY COMMUNICATIONS SYSTEMS
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

4. TESTING RESULTS *(continued)*

4.4 Mass Notification Equipment *(continued)*

Description	Visual Inspection	Functional Test	Comments
Sound pressure levels (attach report with locations, values, and weather conditions)	❑	❑	
System intelligibility ❑ CSI ❑ STI (attach report with locations, values, and weather conditions)	❑	❑	
Other:	❑	❑	

4.5 Two-Way Communication Equipment

Description	Visual Inspection	Functional Test	Comments
Phone handsets	❑	❑	
Phone jacks	❑	❑	
Off-hook indicator	❑	❑	
Call-in signal	❑	❑	
System performance	❑	❑	
System audibility	❑	❑	
System intelligibility	❑	❑	
Other:	❑	❑	

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Figure 7.8.2(If) Interface Component Supplementary Record of Inspection and Testing.

INTERFACE COMPONENT
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING

This form is a supplement to the System Record of Inspection and Testing.
It includes an interface component test record for circuit interfaces, signaling line circuit interfaces, and fire alarm control interfaces.
This form is to be completed by the system inspection and testing contractor at the time of the inspection and/or test.
It shall be permitted to modify this form as needed to provide a more complete and/or clear record.
Insert N/A in all unused lines.

Inspection/Test Start Date/Time: _____ Inspection/Test Completion Date/Time: _____

Number of Supplemental Pages Attached: _____

1. PROPERTY INFORMATION

Name of property: _____

Address: _____

2. INTERFACE COMPONENT TEST RESULTS

Interface Component Type	Address	Location	Test Results

© 2021 National Fire Protection Association

INTERFACE COMPONENT
SUPPLEMENTARY RECORD OF INSPECTION AND TESTING *(continued)*

2. INTERFACE COMPONENT TEST RESULTS *(continued)*

Interface Component Type	Address	Location	Test Results

See main System Record of Inspection and Testing for additional information, certifications, and approvals.

© 2021 National Fire Protection Association

Public Input No. 378-NFPA 72-2022 [Section No. A.10.3.1]

A.10.3.1

~~Terms used by testing laboratories for equipment that is listed or labeled could include certified, approved, or listed.~~

Just noting that a piece of equipment is listed is not sufficient. Listing involves evaluation of the equipment to determine its suitability for a specific purpose for use. The evaluation is usually accomplished using product testing standards developed to demonstrate that specific performance requirements have been met. Many of these performance requirements are based on specific requirements in the Code and go far beyond requirements used only to demonstrate electrical safety.

While most equipment would be listed for fire alarm system use, some equipment may have a different listing. For example, routers and modems that may be used with some transmission methods in the signal transmission path between a protected premises and a supervising station might be listed as general communications equipment (see 26.6.3.12).

Equipment listings generally contain information pertaining to the permitted use, required ambient conditions, mounting orientation, voltage tolerances, compatibility, and so on. Equipment must be installed, tested, and maintained in conformance with the listing and the manufacturer's published instructions to meet the requirements of the Code. Conformance with the listing and the manufacturer's instructions has been a long-standing requirement, originating in the requirements of NFPA 70.

Another aspect to equipment listing is the compatibility with the other parts of the system. This is key as it is designed to ensure system functionality and reliability.

In seismic hazard zones, the fire alarm designer should verify seismic certification requirements for control equipment with the AHJ.

Statement of Problem and Substantiation for Public Input

The text as modified further clarifies the intended listing requirements. Products must be listed to compatible standards as identified in Chapter 2.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 377-NFPA 72-2022 [Section No. 10.3.1]	related to section 10.3.1

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 16:43:17 EDT 2022

Committee: SIG-FUN

Public Input No. 343-NFPA 72-2022 [Section No. A.10.5.3.5]

A.10.5.3.5

~~This is not intended to require certification where it is not offered or required by the manufacturer.~~ -----Delete this section - language moved to chapter 10 - PI 282

Statement of Problem and Substantiation for Public Input

PI 282 recommends to move the annex material into the body of the code. There are many existing systems where the manufacturer no longer provides certification for programmers. These systems still need to be maintained and it should be clear that if certification is not available that it cannot be required to program.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 282-NFPA 72-2022 [New Section after 10.5.3.5.1]	

Submitter Information Verification

Submitter Full Name: Jason Dupuis
Organization: Cintas Fire Protection F19
Street Address:
City:
State:
Zip:
Submittal Date: Tue May 24 11:01:29 EDT 2022
Committee: SIG-FUN

Public Input No. 140-NFPA 72-2022 [Section No. A.10.21.4]

A.10.21.4 5

It is important for the authority having jurisdiction, typically the local fire official, to be informed when systems have been out of service for more than 8 hours so that appropriate measures can be taken. The term *out of service* is meant to refer to the entire system or a substantial portion thereof.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, thus renumbering the subsequent sections.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 139-NFPA 72-2022 [Section No. 10.21.4]	directly related

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:11:05 EST 2022
Committee: SIG-FUN

Public Input No. 142-NFPA 72-2022 [Section No. A.10.21.5]

A.10.21.5 ~~5~~ 6

The need for mitigating measures is typically determined on a case-by-case basis. This considers the building, occupancy type, nature and duration of impairment, building occupancy level during impairment period, active work being conducted on the fire alarm system during the impairment, condition of other fire protection systems and features (i.e., sprinklers, structural compartmentation, etc.), and hazards and assets at risk.

Appropriate mitigating measures range from simple occupant notification to full-time fire watch. Determining factors vary from testing-related impairments and maintenance activities during normal business through extensive impairments to high-value, high-hazard situations.

Statement of Problem and Substantiation for Public Input

NFPA staff, Richard Roux, and NFPA SIG-FUN chair, Manuelita David, requested a task group to address Manual of Style (MOS) issues. NFPA 72 SIG-FUN MOS Task Group chair Kim Gruner, and members Fred Leber, Chris Moseley, and Paul Hail met to provide recommendations for each issue. Manual of Style for NFPA Technical Committee Documents, July 2004 Edition section 1.8.3 requires Sections containing multiple requirements subdivided into subsections, which shall be further subdivided into paragraphs of test. The task group proposed text utilized 2 separate paragraphs for the 2 requirements, thus renumbering subsequent paragraphs.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 141-NFPA 72-2022 [Section No. 10.21.5]	directly related.

Submitter Information Verification

Submitter Full Name: Kimberly Gruner
Organization: Fike Corporation
Affiliation: Fire Suppression Systems Association (FSSA)
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 24 16:15:36 EST 2022
Committee: SIG-FUN

Public Input No. 390-NFPA 72-2022 [Section No. A.11.1]

A.11.1

Cybersecurity is not required for every system or application; it is only required when other sections of this Code, authorities, or regulations mandate that cybersecurity be incorporated into the system(s). Generally, there are greater cybersecurity concerns when systems are connected to external networks.~~Cybersecurity recommendations are contained in Annex J .~~

A.11.1.5.7 Figure A.11.1.5.7 depicts system typical firewall/gateway operation. Such functionality is not mandated but when deployed might take the form of physical hardware, firmware, or a combination of both. The firewall/gateway might be physically integrated into the control unit as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit as shown in the nonintegrated control unit. If the firewall/gateway is segmented from the executive firmware and site-specific software and if security software changes to the cybersecurity-related only software within the firewall/gateway are made, these changes should not require system retesting. If changes are made in a firewall/gateway that is not segmented from the executive firmware and site-specific software, the system should be retested..

Additional Proposed Changes

File Name	Description	Approved
Cybersecurity-Integrated_Control_Unit_chart.jpg	System Typical Firewall/Gateway Operation	

Statement of Problem and Substantiation for Public Input

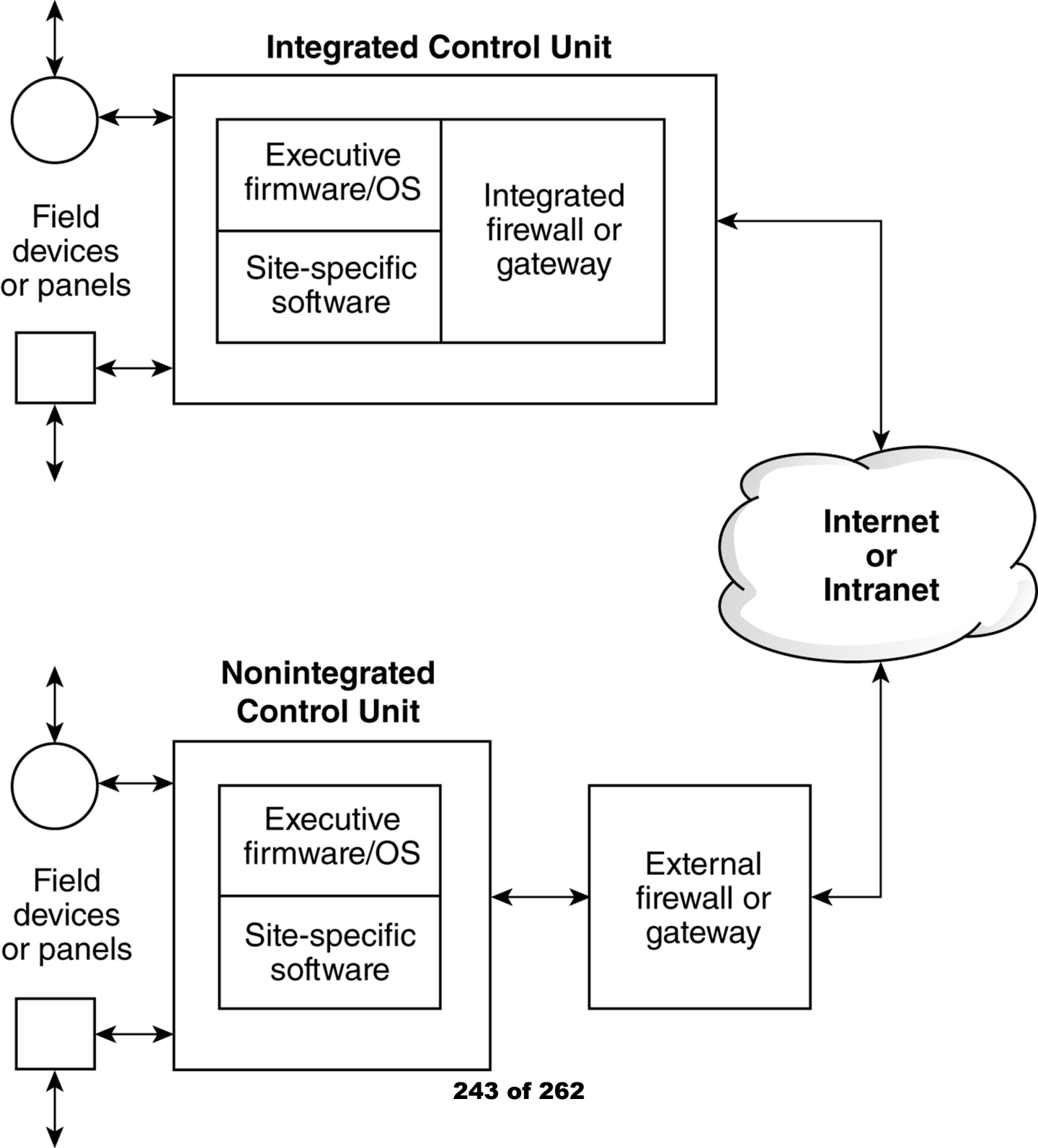
Updated and moved figure that depicts system typical firewall/gateway operation from Annex J to Annex A.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 384-NFPA 72-2022 [Section No. 11.1]	Figure and supporting information related to cybersecurity

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 17:56:27 EDT 2022
Committee: SIG-FUN


Integrated Control Unit
Executive firmware/OS
Site-specific software
Integrated firewall or gateway
Field devices or panels
Internet or Intranet
Nonintegrated Control Unit
Executive firmware/OS
Site-specific software
External firewall or gateway
Field devices or panels

Public Input No. 203-NFPA 72-2022 [Chapter E]

Annex E Sample U.S. Ordinance Adopting ***NFPA 72***

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

E.1

The following sample ordinance is provided to assist a jurisdiction in the adoption of this Code and is not part of this Code.

ORDINANCE NO. _____

An ordinance of the *[jurisdiction]* adopting the 2022 edition of *NFPA 72*, *National Fire Alarm and Signaling Code*, and documents listed in Chapter 2 of that Code; prescribing regulations governing conditions hazardous to life and property from fire or explosion; providing for the issuance of permits and collection of fees; repealing Ordinance No. _____ of the *[jurisdiction]* and all other ordinances and parts of ordinances in conflict therewith; providing a penalty; providing a severability clause; and providing for publication; and providing an effective date.

BE IT ORDAINED BY THE *[governing body]* OF THE *[jurisdiction]*:

SECTION 1 That the *NFPA 72*, *National Fire Alarm and Signaling Code*, and documents adopted by Chapter 2, three (3) copies of which are on file and are open to inspection by the public in the office of the *[jurisdiction's keeper of records]* of the *[jurisdiction]*, are hereby adopted and incorporated into this ordinance as fully as if set out at length herein, and from the date on which this ordinance shall take effect, the provisions thereof shall be controlling within the limits of the *[jurisdiction]*. The same are hereby adopted as the Code of the *[jurisdiction]* for the purpose of prescribing regulations governing conditions hazardous to life and property from fire or explosion and providing for issuance of permits and collection of fees.

SECTION 2 Any person who shall violate any provision of this code or standard hereby adopted or fail to comply therewith; or who shall violate or fail to comply with any order made thereunder; or who shall build in violation of any detailed statement of specifications or plans submitted and approved thereunder; or fail to operate in accordance with any certificate or permit issued thereunder; and from which no appeal has been taken; or who shall fail to comply with such an order as affirmed or modified by a court of competent jurisdiction, within the time fixed herein, shall severally for each and every such violation and noncompliance, respectively, be guilty of a misdemeanor, punishable by a fine of not less than $ _____ nor more than $_____ or by imprisonment for not less than _____ days nor more than _____ days or by both such fine and imprisonment. The imposition of one penalty for any violation shall not excuse the violation or permit it to continue; and all such persons shall be required to correct or remedy such violations or defects within a reasonable time; and when not otherwise specified the application of the above penalty shall not be held to prevent the enforced removal of prohibited conditions. Each day that prohibited conditions are maintained shall constitute a separate offense.

SECTION 3 Additions, insertions, and changes — that the 2022 edition of *NFPA 72*, *National Fire Alarm and Signaling Code*, is amended and changed in the following respects:

List Amendments

SECTION 4 That ordinance No. _____ of *[jurisdiction]* entitled *[fill in the title of the ordinance or ordinances in effect at the present time]* and all other ordinances or parts of ordinances in conflict herewith are hereby repealed.

SECTION 5 That if any section, subsection, sentence, clause, or phrase of this ordinance is, for any reason, held to be invalid or unconstitutional, such decision shall not affect the validity or constitutionality of the remaining portions of this ordinance. The *[governing body]* hereby declares that it would have passed this ordinance, and each section, subsection, clause, or phrase hereof, irrespective of the fact that any one or more sections, subsections, sentences, clauses, and phrases be declared unconstitutional.

SECTION 6 That the *[jurisdiction's keeper of records]* is hereby ordered and directed to cause this ordinance to be published.

[NOTE: An additional provision might be required to direct the number of times the ordinance is to be published and to specify that it is to be in a newspaper in general circulation. Posting may also be required.]

SECTION 7 That this ordinance and the rules, regulations, provisions, requirements, orders, and matters established and adopted hereby shall take effect and be in full force and effect *[time period]* from and after the date of its final passage and adoption.

Statement of Problem and Substantiation for Public Input

NFPA 72 strives to be used outside of the U.S. This Annex seems U.S.-centric. I'm not sure this is how laws are written elsewhere around the world. More broader, I wonder whether this Annex is even necessary - do cities not know how to write their ordinances?

Submitter Information Verification

Submitter Full Name: Scott Lang
Organization: Honeywell International
Street Address:
City:
State:
Zip:
Submittal Date: Wed Apr 06 09:18:28 EDT 2022
Committee: SIG-FUN

Public Input No. 388-NFPA 72-2022 [Sections J.1, J.2, J.3, J.4, J.5, J.6]

Sections J.1, J.2, J.3, J.4, J.5, J.6

J.1 Introduction.

~~J.~~

NFPA 72 contains requirements for fire alarm and emergency communications systems that can be impacted by cybersecurity threats. Coordination of cybersecurity frameworks to protect the functions of systems is ~~essential in order~~ essential to prevent unwanted impacts on the system. Where the system ~~would need to interface~~ interfaces with the internet or other systems, ~~it would make sense to provide~~ a secure firewall or gateway ~~. In any case, protection from cybersecurity threats is essential.~~

~~The Technical Committee has determined that, in lieu of establishing requirements in Chapter 11 on cybersecurity at this time, it is appropriate to provide such guidance and framework in this annex. This allows the industry and the public the ability to gain experience with cybersecurity measures and provide constructive feedback for future editions of this Code.~~

~~**J.2** – Cybersecurity Provisions.~~

~~Where cybersecurity provisions are required, manufacturers, system designers, system installers, inspection personnel, testing personnel, and service technicians involved in the design, installation, testing, and maintenance of cybersecurity provisions should provide cybersecurity measures as outlined in this annex.~~

should be provided to effect vital protection against cybersecurity threats.

J. 3 Cybersecurity Standards.

Systems should be designed, installed, and maintained in accordance with one or more of the following cybersecurity standards:

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

(2) NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

(3) NIST *Framework for Improving Critical Infrastructure Cybersecurity*

(4) UL 2900-2-3, *Software Cybersecurity for Network-Connectable Products Part 2-3: Particular Requirements for Security and Life Signaling Systems*

(5) Other standard(s) or published documents acceptable to the authority having jurisdiction

J.4 Evidence of Compliance.

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

(1) Certification of compliance by a nationally recognized test 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

~~**J.5** – Documentation.~~

~~All system-related documentation associated with the use of the selected standard(s) is included as part of the system documentation required by Chapter 7 .~~

~~**J.6** – Cybersecurity Certificate Maintenance.~~

J.6.1 – Certificate Validation.

Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate should be checked annually.

J.6.2 – Cybersecurity Software Revisions.

Software changes made only for cybersecurity purposes to firewalls or barrier gateways should not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all the following are true:

(1) The changes do not affect the function of the executive or site-specific software.

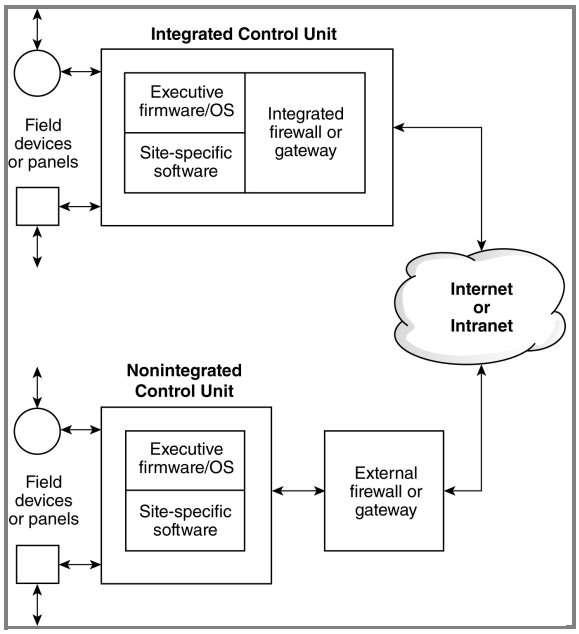
(2) The integrity of the software update installed in the firewall or barrier gateway is verified to ensure complete and intact software delivery.

(3) The software is digitally signed by the manufacturer.

(4) The digital signature of the software is verified prior to execution by the system or system components using secure signing keys.

Figure J.6.2 depicts system typical firewall/gateway operation. Such functionality is not mandated but when deployed might take the form of physical hardware, firmware, or a combination of both. The firewall/gateway might be physically integrated into the control unit as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit as shown in the nonintegrated control unit. If the firewall/gateway is segmented from the executive firmware and site-specific software and if security software changes to the firewall/gateway are made, these changes should not require system retesting. If changes are made in a firewall/gateway that is not segmented from the executive firmware and site-specific software, the system should be retested.

Figure J.6.2 System Typical Firewall/Gateway Operation.



J.6.3 – Remote Software Changes.

Software changes to systems or system components made only for cybersecurity purposes should be permitted to be made by remote access in accordance with Chapter 23 .

Statement of Problem and Substantiation for Public Input

Revisions reflect proposed text provided for Chapter 11.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 384-NFPA 72-2022 [Section No. 11.1]	anex for revised Chapter 11.

Submitter Information Verification

Submitter Full Name: Chris Heaton
Organization: Electronic Security Association
Affiliation: Electronic Security Association
Street Address:
City:
State:
Zip:
Submittal Date: Wed May 25 17:35:19 EDT 2022
Committee: SIG-FUN

Public Input No. 509-NFPA 72-2022 [Sections J.1, J.2, J.3, J.4, J.5, J.6]

Sections J.1, J.2, J.3, J.4, J.5, J.6

J.1 ~~– Introduction.~~ A.11.1 Cybersecurity

~~J.~~

NFPA 72 contains requirements for fire alarm and emergency communications systems that can be impacted by cybersecurity threats. Coordination of cybersecurity frameworks to protect the functions of systems is essential in order to prevent unwanted impacts on the system. Where the system would need to interface with the internet or other systems, ~~it would make sense to provide~~ a secure firewall or gateway ~~. In any case, protection from cybersecurity threats is essential.~~

~~The Technical Committee has determined that, in lieu of establishing requirements in Chapter 11 on cybersecurity at this time, it is appropriate to provide such guidance and framework in this annex. This allows the industry and the public the ability to gain experience with cybersecurity measures and provide constructive feedback for future editions of this Code.~~

~~**J.2** – Cybersecurity Provisions.~~

~~Where cybersecurity provisions are required, manufacturers, system designers, system installers, inspection personnel, testing personnel, and service technicians involved in the design, installation, testing, and maintenance of cybersecurity provisions should provide cybersecurity measures as outlined in this annex.~~

should be provided to effect vital protection against cybersecurity threats.

J. 3 _ Cybersecurity Standards.

Systems should be designed, installed, and maintained in accordance with one or more of the following cybersecurity standards:

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

(2) NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

(3) NIST *Framework for Improving Critical Infrastructure Cybersecurity*

(4) UL 2900-2-3, *Software Cybersecurity for Network-Connectable Products Part 2-3: Particular Requirements for Security and Life Signaling Systems*

(5) Other standard(s) or published documents acceptable to the authority having jurisdiction

J.

4

11.41.8 _ Evidence of Compliance.

Evidence of cybersecurity compliance

~~should~~

shall include one or more of the following:

(1) Certification of compliance by a nationally recognized test 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

J.

~~5 Documentation.~~

~~All system-related documentation associated with the use of the selected standard(s) is included as part of the system documentation required by Chapter 7.~~

~~**J.6** – Cybersecurity Certificate Maintenance.~~

~~**J.6.1** – Certificate Validation.~~

~~Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate should be checked annually.~~

~~**J.6.2** – Cybersecurity Software Revisions.~~

~~Software changes made only for cybersecurity purposes to firewalls or barrier gateways should not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all the following are true:~~

(1) ~~The changes do not affect the function of the executive or site-specific software.~~

(2) ~~The integrity of the software update installed in the firewall or barrier gateway is verified to ensure complete and intact software delivery.~~

(3) ~~The software is digitally signed by the manufacturer.~~

(4) ~~The digital signature of the software is verified prior to execution by the system or system components using secure signing keys.~~

~~Figure J.6.2~~

11.1.8.2 The validity of cybersecurity certificates shall be verified annually

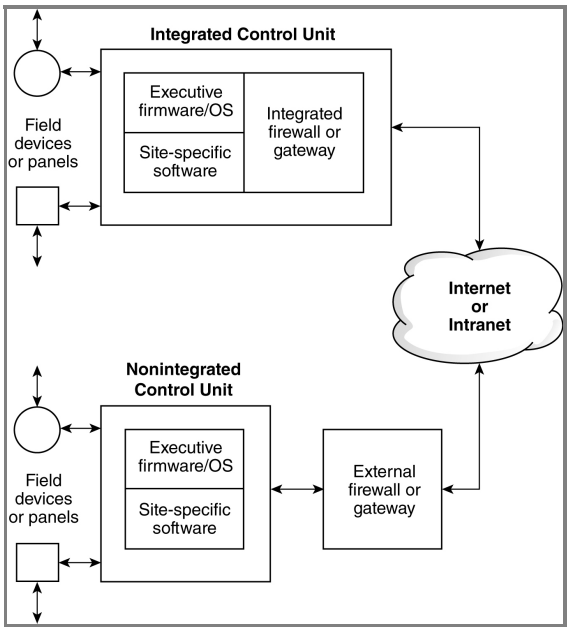
A1.11.5.7 Figure A.1.11.5.7 depicts system typical firewall/gateway operation. Such functionality is not mandated but when deployed might take the form of physical hardware, firmware, or a combination of both. The firewall/gateway might be physically integrated into the control unit as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit as shown in the nonintegrated control unit. If the firewall/gateway is segmented from the executive firmware and site-specific software and if security software changes to the cybersurity-related only software within the firewall/gateway are made, these changes should not require system retesting. If changes are made in a firewall/gateway that is not segmented from the executive firmware and site-specific software, the system should be retested.

~~Figure J~~

Figure A .

~~6.2 System~~

1.11.5.7 System Typical Firewall/Gateway Operation.



~~J~~

11 .

~~6.3 Remote Software Changes.~~

~~Software~~

~~**1.5.8 Cybersecurity-related only changes to systems or system components**~~

~~made only for cybersecurity purposes should~~

~~**shall be permitted to be made**~~

~~by~~

~~**by** remote access in accordance with Chapter 23.~~

Additional Proposed Changes

File Name	Description	Approved
NFPA_72_BS_SB_11.1_comments.docx	Cybersecurity changes to ANNEX J	

Statement of Problem and Substantiation for Public Input

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.
Their report lists gaps that include:

- Configuration – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
- Implementation – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
- Security – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.
- Access – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment

The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here.

- https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
- Researchers Hack Building Control System at Google Australia Office | WIRED

Target Hackers Broke in Via HVAC Company – Krebs on Security

Submitter Information Verification

Submitter Full Name: Megan Hayes
Organization: Nema
Street Address:
City:
State:

Zip:	
Submittal Date:	Mon May 30 17:17:21 EDT 2022
Committee:	SIG-FUN

NFPA Public Input Form

NOTE: All Public Input must be received by 5:00 pm EST/EDST on the published Public Input Closing Date.

For further information on the standards-making process, please contact the Codes and Standards Administration at 617-984-7249 or visit www.nfpa.org/codes.

For technical assistance, please call NFPA at 1-800-344-3555

FOR OFFICE USE ONLY

Log #:

Date Rec'd:

Date 3/18/22 **Name** Megan Hayes **Tel. No.** 703-841-3236

Company National Electrical Manufacturers Association (NEMA) **Email** megan.hayes@nema.org

Street Address 1300 North 17th Street, Suite 900 **City** Rosslyn **State** VA **Zip** 22209

Please indicate organization represented (if any) NEMA

1. (a) Title of NFPA Standard NFPA 72 National Fire Alarm Code **NFPA No. & Year** 72 / 2022

(b) Section/Paragraph 11.1

2. Public Input Recommends (check one): ☐ new text ☒ revised text ☐ deleted text

3. Proposed Text of Public Input (include proposed new or revised wording, or identification of wording to be deleted):
[Note: Proposed text should be in legislative format; i.e., use underscore to denote wording to be inserted (inserted wording) and strike-through to denote wording to be deleted (~~deleted wording~~).]

11.1*~~-~~Cybersecurity.

11.1.1 Cybersecurity Provisions

Where required by governing laws, codes, or standards, or other parts of this Code, cybersecurity shall be provided in accordance with Chapter 11, for equipment, software,

~~firmware,~~
system support tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

11.1.2 Connected Equipment Software Development

Equipment shall be developed by the manufacturer in accordance with one or more of the following secure software development lifecycle standards:

A) ANSI/ISA/IEC 62443 Security for Industrial and Automation Control Systems Series of standards

B) ANSI/CAN/UL 2900 Standard for Software Cybersecurity for Network-Connectable Products

C) NIST Cybersecurity Framework

E) NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.3 Network Connectable Equipment Software Development and Production Environments

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

A) NIST Cybersecurity Framework

B) ISO/IEC 27001 Information Security Management

C) IASME Consortium Cyber Essentials

D) Other equivalent standards acceptable to the authority having jurisdiction

11.1.4 Security Levels for Network Connectable Equipment

All interfaces used to communicate with network connectable equipment shall be protected using the following minimum security levels:

A) For all non-internet facing wireless Interfaces and those non-internet facing wired interfaces that employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

B) For non-internet facing wired interfaces that do not employ internet protocol, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 1 or UL 2900 Security Level 1 or the equivalent level associated with 11.1.3 D.

C) For all wired or wireless internet facing (WiFi) interfaces, ANSI/ISA/IEC 62443-4-2/3-3 Security Level 3 or UL 2900 Security Level 3 or the equivalent level associated with 11.1.3 D.

D) For all cellular, Bluetooth, and other wireless interfaces that do not employ internet protocol, IEC 62443-4-2/3-3 Security Level 2 or UL 2900 Security Level 2 or the equivalent level associated with 11.1.3 D.

11.1.5 Network Connectable Equipment Cybersecurity-related Software Updates

11.1.5.1 The equipment manufacturer shall evaluate all discovered cybersecurity threats at least quarterly and shall determine if a software update is required to maintain the cybersecurity level achieved in complying with 11.1.2 and 11.1.3 until the equipment is no longer be supported by the manufacturer.

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

11.1.5.3 The equipment manufacturer shall notify the system owner or their representative, of all required software security updates required to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.4 Software for network connectable devices shall be maintained by installing software security updates as required by the manufacturer to maintain the cybersecurity level achieved in complying with 11.1.2, 11.1.3 and 11.1.4.

11.1.5.5 Software security updates that are deemed necessary by the manufacturer for compliance with 11.1.3 shall be installed at least annually.

11.1.5.6 Cybersecurity-related only software updates applied to system elements that do not affect the system site-specific or system executive software shall not be required to comply with 14.4.2.

11.1.5.7 Cybersecurity-related only software changes to systems or system components shall be permitted to be made by remote access in accordance with Chapter 23.

11.1.6 Notification of Termination of Cybersecurity Update Support

The manufacturer shall notify the system owner or their representative, of the termination of software cybersecurity-related software update support required by 11.1.5 for any element of the system.

11.1.7 Cybersecurity for System Support Tools

A system support tool and the support tool interfaces shall comply with the requirements of 11.1.2 through 11.1.6.

11.1.8 Evidence of Compliance.

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

1. Certification of compliance by a nationally recognized test 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

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

11.1.9 Documentation

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

~~JA~~.11.1 ~~Introduction.~~Cybersecurity

NFPA 72 contains requirements for fire alarm and emergency communications systems that can be impacted by cybersecurity threats. Coordination of cybersecurity frameworks to protect the functions of systems is essential ~~in order~~ to prevent unwanted impacts on the system. Where the ~~system would need to interface~~ system interfaces with the internet or other systems ~~, it would make sense to provide~~ a secure firewall or gateway ~~. In any case, protection from cybersecurity threats is essential.~~

~~The Technical Committee has determined that, in lieu of establishing requirements in Chapter 11 on cybersecurity at this time, it is appropriate to provide such guidance and framework in this annex. This allows the industry and the public~~

~~the ability to gain experience with cybersecurity measures and provide constructive feedback for future editions of this Code.~~

should be provided to effect vital protection against cybersecurity threats.

~~**J.2** Cybersecurity Provisions.~~

~~Where cybersecurity provisions are required, manufacturers, system designers, system installers, inspection personnel, testing personnel, and service technicians involved in the design, installation, testing, and maintenance of cybersecurity provisions should provide cybersecurity measures as outlined in this annex.~~

~~**J**~~**11.4****1.8** Evidence of Compliance.

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

1. Certification of compliance by a nationally recognized test 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

~~**J.5** Documentation.~~

~~All system-related documentation associated with the use of the selected standard(s) is included as part of the system documentation required by Chapter 7.~~

~~**J.6** Cybersecurity Certificate Maintenance.~~

~~**J.6.1** Certificate Validation.~~

~~Where a system is provided with a cybersecurity certificate document as evidence of compliance, the validity of the certificate should be checked annually.~~

~~**J.6.2** Cybersecurity Software Revisions.~~

~~Software changes made only for cybersecurity purposes to firewalls or barrier gateways should not require the functional test of the system that is otherwise required by 14.4.2.4 and 14.4.2.5 where all the following are true:~~

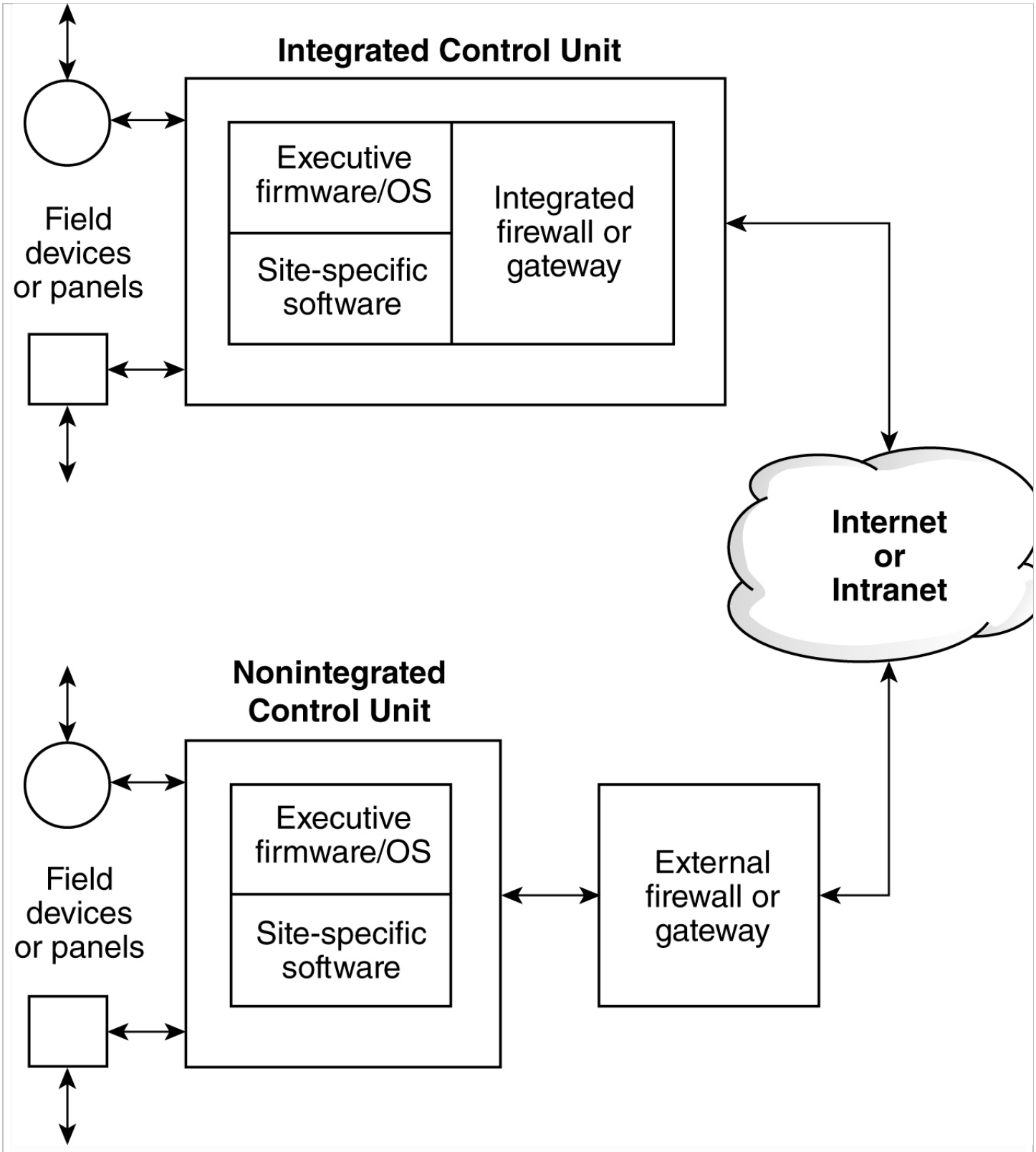
~~1. The changes do not affect the function of the executive or site-specific software.~~
~~2. The integrity of the software update installed in the firewall or barrier gateway is verified to ensure complete and intact software delivery.~~
~~3. The software is digitally signed by the manufacturer.~~
~~4. The digital signature of the software is verified prior to execution by the system or system components using secure signing keys.~~

~~Figure J.6.2~~
11.1.8.2 The validity of cybersecurity certificates shall be verified annually.

A.1.11.5.7 Figure A.1.11.5.7 depicts system typical firewall/gateway operation. Such functionality is not mandated but when deployed might take the form of physical hardware, firmware, or a combination of both. The firewall/gateway might be physically integrated into the control unit as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit as shown in the nonintegrated control unit. If the firewall/gateway is segmented from the executive firmware and site-specific software and if security software changes to the cybersecurity-related only software within the firewall/gateway are made, these changes should not require system retesting. If changes are made in a firewall/gateway that is not segmented from the executive firmware and site-specific software, the system should be retested.

~~Figure J~~
Figure A.

~~6.2 System~~
1.11.5.7 System Typical Firewall/Gateway Operation.



~~J~~

11.

~~6.3 Remote Software Changes.~~

~~Software~~

1.5.8 Cybersecurity-related only changes to systems or system

~~components made only for cybersecurity purposes should~~ components shall be permitted to be made by remote access in accordance with Chapter 23.

4. Statement of Problem and Substantiation for Public Input: (Note: State the problem that would be resolved by your recommendation; give the specific reason for your Public Input, including copies of tests, research papers, fire experience, etc. If more than 200 words, it may be abstracted for publication.)

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.
Their report lists gaps that include:

- **Configuration** – • Interconnection of external systems (call centers, service providers) could allow for unauthorized activity if those external systems are not secure. • Interconnection with other building systems with no access/restriction to prevent unintended communications. • If one interconnected system is compromised and life safety is connected, it would be safe to assume that all are compromised.
- **Implementation** – • Systems that have remote access for maintenance or monitoring could introduce vulnerabilities if not properly implemented. • Using secure gateways and configuring devices with only the necessary communication mechanisms can reduce exposure. • The use of insecure wireless devices, or lack of wireless device authentication can be a weakness.
- **Security** – • Complexity of cybersecurity threats and solutions are increasing, making systems more vulnerable to highly sophisticated arson (terrorist) attacks, industrial espionage, and insider threats. Because of this, it is becoming more difficult to defend against these attacks and new solutions need to be implemented.
- **Access** – • Weak logical and physical access to 3rd party networks and systems. • Easy to implant hardware or software devices into environment

The attached public Input addresses the above gaps by requiring industry accepted cyber security practices.
There are several incidents that have already occurred and are referenced here.

- https://www.smartcitiesdive.com/news/hackers-emergency-sirens-texas-cities/550639/
- Researchers Hack Building Control System at Google Australia Office | WIRED
- Target Hackers Broke in Via HVAC Company – Krebs on Security

5. Copyright Assignment

(a) ☒ I am the author of the text or other material (such as illustrations, graphs) proposed in the Public Input.

(b) ☐ Some or all of the text or other material proposed in this Public Input was not authored by me. Its source is as follows: (please identify which material and provide complete information on its source)

I hereby grant and assign to the NFPA all and full rights in copyright in this Public Input (including both the Proposed Text and the Statement of Problem and Substantiation). I understand that I acquire no rights in any publication of NFPA in which this Public Input in this or another similar or analogous form is used. Except to the extent that I do not have authority to make an assignment in materials that I have identified in (b) above, I hereby warrant that I am the author of this Public Input and that I have full power and authority to enter into this assignment.

Signature (Required)

PLEASE USE SEPARATE FORM FOR EACH PUBLIC INPUT

To: Secretary, Standards Council National Fire Protection Association
1 Batterymarch Park · Quincy, MA 02169-7471 OR
Fax to: (617) 770-3500 OR Email to: proposals_comments@nfpa.org

6/7/2022

Public Input No. 560-NFPA 72-2022 [Section No. K.1.2.15]

K.1.2.15 UL Publications.

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

UL 217, *Smoke Alarms*, ~~8th edition~~ 2020 , ~~2015,~~ revised ~~2016~~ 2021 .

UL 268, *Smoke Detectors for Fire Alarm Systems,* ~~7th edition~~ 2020 , ~~2016~~ revised 2021 .

UL 268A, *Smoke Detectors for Duct Application*, 2008, revised ~~2016~~ 2020 .

UL 827, *Central-Station Alarm Services*, 2014, revised ~~2019~~ 2020 .

UL 864, *Control Units and Accessories for Fire Alarm Systems*, 2014, revised ~~2018~~ 2020 .

UL 1638, *Visible Signaling Devices for Fire Alarm and Signaling Systems, Including Accessories*, 2016.

UL 1778, *Uninterruptible Power Source*, 2014, revised 2017.

UL 1971, *Signaling Devices for the Hearing Impaired,* 2002, revised 2018.

UL 1989, *Standby Batteries*, 2013, revised 2018.

UL 2034, *Single and Multiple Station Carbon Monoxide Alarms,*2017, revised 2018.

UL 2054, *Household and Commercial Batteries*, ~~2004~~ 2021 .

UL 2075, *Safety Gas and Vapor Detectors and Sensors*, 2013, revised ~~2017~~ 2021 .

UL 2572, *Mass Notification Systems*, 2018.

CAN/ UL 2900~~, Software Cybersecurity for Network - Connectable Products, 2017.UL 2900-~~ 1, *Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*, ~~2017~~ 2020 .

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

Statement of Problem and Substantiation for Public Input

UL 2900 is withdrawn and has been replaced with UL 2900-1 and UL 2900-2-3 which are now both Bi National Standards. The other changes are updates to edition or revision dates and are submitted reference updates.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 559-NFPA 72-2022 [Section No. 2.3.9]	

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL LLC
Street Address:
City:
State:
Zip:

Submittal Date:	Wed Jun 01 10:47:03 EDT 2022
Committee:	SIG-FUN

Public Input No. 270-NFPA 72-2022 [Section No. K.3]

K.3 References for Extracts in Informational Sections.

NFPA 70®, *National Electrical Code®*, 2020 edition.

NFPA 92B, *Smoke Management Systems in Malls, Atria, and Large Spaces*, 1995 edition (withdrawn).

NFPA *101®*, *Life Safety Code®*, 2021 edition.

~~NFPA 1221~~ NFPA 1225 ,~~Standard~~ Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems ~~, 2019 edition.~~

Statement of Problem and Substantiation for Public Input

As part of the Emergency Response and Responder Safety Document Consolidation Plan (consolidation plan) as approved by the NFPA Standards Council, the NFPA 1221 Standard has been combined into a new consolidated Standard, NFPA 1225.

Submitter Information Verification

Submitter Full Name: Rodger Reiswig
Organization: Johnson Controls
Street Address:
City:
State:
Zip:
Submittal Date: Fri Apr 29 09:26:09 EDT 2022
Committee: SIG-FUN