NEW starting with NFPA 72, 2016 Edition

Class A, B, and now N

Presented by:

Dan Horon

President

Cadgraphics Incorporated

dan@RescueLogic.com

www.RescueLogic.com

NFPA References:

I want to point out that the comments and opinions expressed during this presentation are mine only.

They do not reflect an official position of the National Fire Protection Association (NFPA), its employees, or any of the Technical Committees.

Also, this presentation will not cover everything about Class N in our time allotted.

Therefore, I highly recommend you purchase a copy of the Code from NFPA – and a copy of the NFPA 72 Handbook for even more material.

History

Before the 2010 Edition, Style Tables defined the properties of circuits. They were prescriptive, and prevented new technologies. Understanding them required a fire alarm engineer.

NFPA 72, 2007 Edition

Table 6.6.1 Performance of Signaling Line Circuits (SLCs)

Class	B			A			A		
Style	4			6			7		
	Alm	Trbl	ARC	Alm	Trbl	ARC	Alm	Trbl	ARC
Abnormal Condition	1	2	3	4	5	7	8	9	10
Single open	—	X	—	—	X	R	—	X	R
Single ground	—	X	R	—	X	R	—	X	R
Wire-to-wire short	—	X	—	—	X	—	—	X	R
Wire-to-wire short & open	—	X	—	—	X	—	—	X	—
Wire-to-wire short & ground	—	X	—	—	X	—	—	X	—
Open and ground	—	X	—	—	X	R	—	X	R
Loss of carrier (if used)/channel interface	—	X	—	—	X	—	—	X	—

Alm: Alarm. Trbl: Trouble. ARC: Alarm receipt capability during abnormal condition. R: Required capability.
X: Indication required at protected premises and as required by Chapter 8.

History

Throughout the years that Style Tables were in Code, the older terms *Class A* and *Class B* were still used by the industry. Everyone working in fire alarm knew Class B as being a single supervised circuit, and that Class A has an additional redundant path.

NFPA 72, 2007 Edition

Table 6.7 Notification Appliance Circuits (NACs)

Class	B		A	
	Trouble Indication at Protected Premises	Alarm Capability During Abnormal Conditions	Trouble Indication at Protected Premises	Alarm Capability During Abnormal Conditions
Abnormal Condition	1	2	3	4
Single open	X	—	X	R
Single ground	X	R	X	R
Wire-to-wire short	X	—	X	—

X: Indication required at protected premises. R: Required capability.

History

In the 2010 Edition, Class B is described in basic, performance-based terms.

NFPA 72, 2010 Edition

12.3.2* Class B. A pathway shall be designated as Class B when it performs as follows:

(1) It does not include a redundant path.
(2) Operational capability stops at a single open.
(3) Conditions that affect the intended operation of the path are annunciated.

History

In 2013, NFPA 72 required Class A, B, and X to report a single connection to ground.

NFPA 72, 2013 Edition

12.3.1* Class A. A pathway shall be designated as Class A when it performs as follows:

(1) It includes a redundant path.
(2) Operational capability continues past a single open, and the single open fault shall result in the annunciation of a trouble signal.
(3) Conditions that affect the intended operation of the path are annunciated as a trouble signal.
(4) Operational capability is maintained during the application of a single ground fault.
(5) A single ground condition shall result in the annunciation of a trouble signal.

Exception: Requirements in 12.3.1(4) and (5) shall not apply to nonconductive pathways (e.g., wireless or fiber).

History

If wireless or fiber paths are installed without redundant pathways, they already comply with Class B. That includes Ethernet.

NFPA 72, 2013 Edition

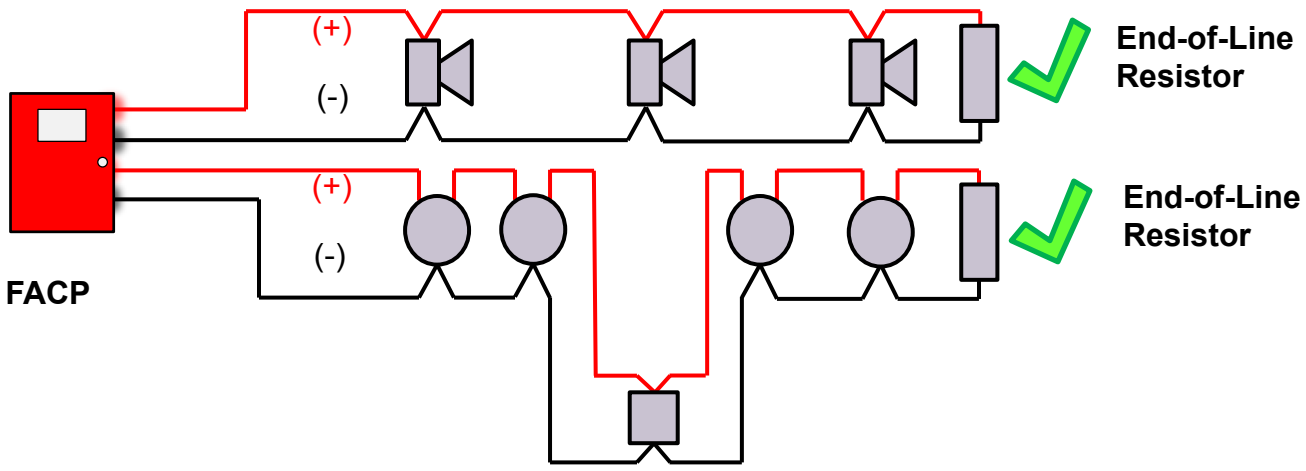
12.3.2* Class B. A pathway shall be designated as Class B when it performs as follows:

(1) It does not include a redundant path.
(2) Operational capability stops at a single open.
(3) Conditions that affect the intended operation of the path are annunciated as a trouble signal.
(4) Operational capability is maintained during the application of a single ground fault.
(5) A single ground condition shall result in the annunciation of a trouble signal.

Exception: Requirements in 12.3.2(4) and (5) shall not apply to nonconductive pathways (e.g., wireless or fiber).

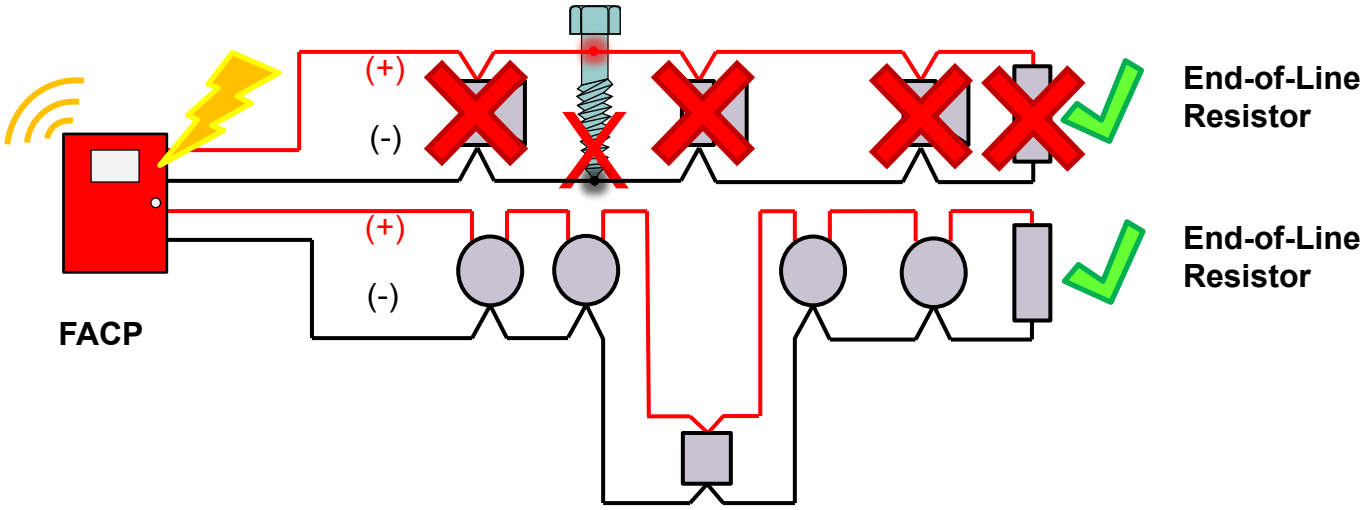
Approved Fire Alarm Pathway

One familiar type of Class B pathway has wires with direct current, and a resistor at the last device. The end-of-line resistor offers a level of assurance that the all wires are connected to the intended device.



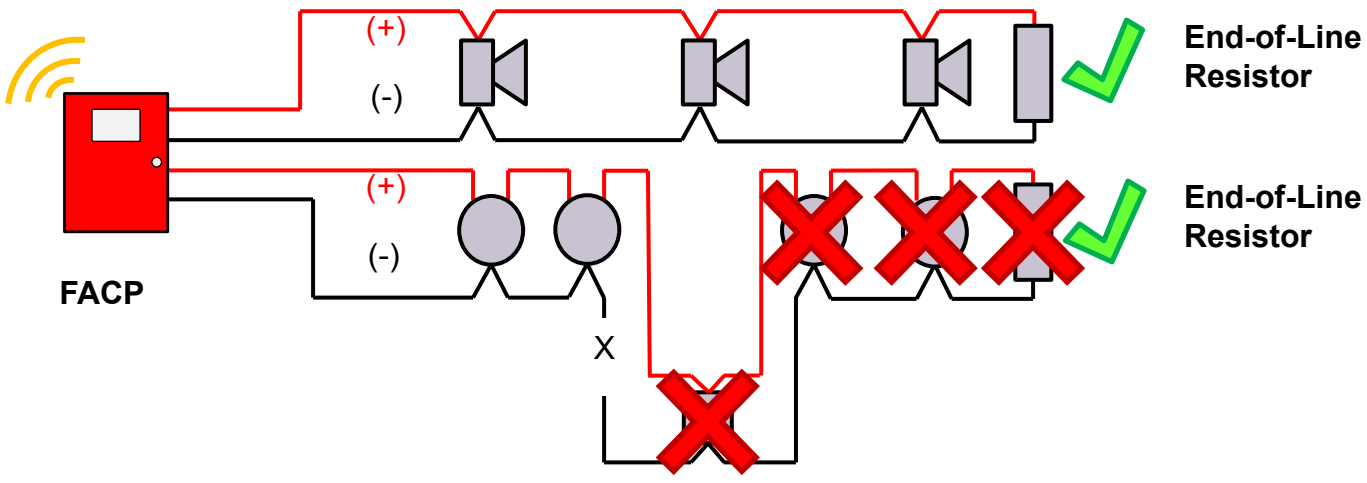
Approved Fire Alarm Pathway

If a short occurs at any point on a Class B notification appliance pathway, the entire circuit becomes inoperable.



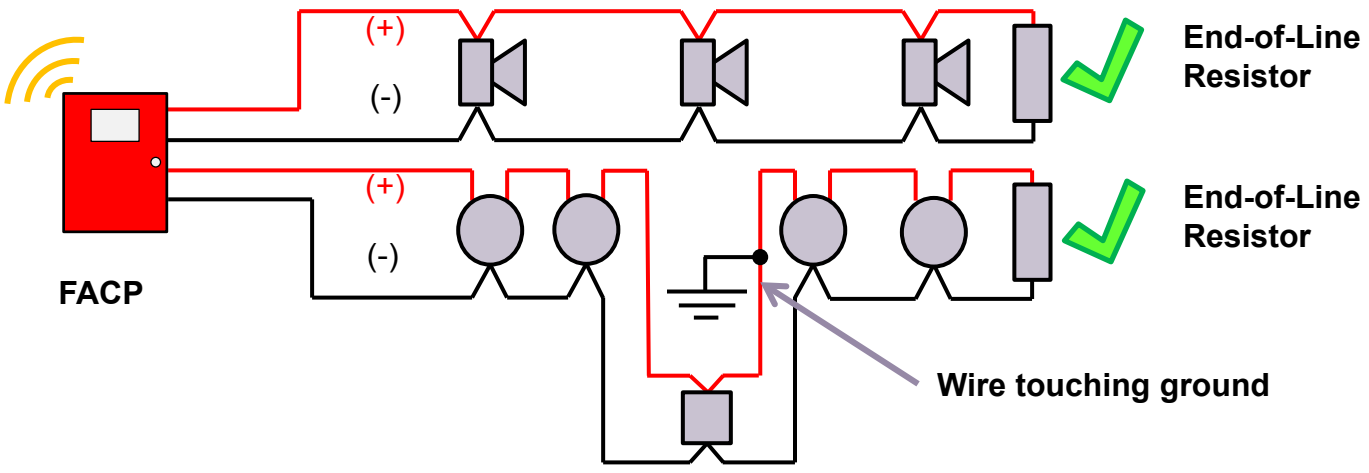
Approved Fire Alarm Pathway

If an open occurs at any point on a Class B initiating device circuit, every device thereafter is inoperable. This is true even when a smoke detector is removed for maintenance.



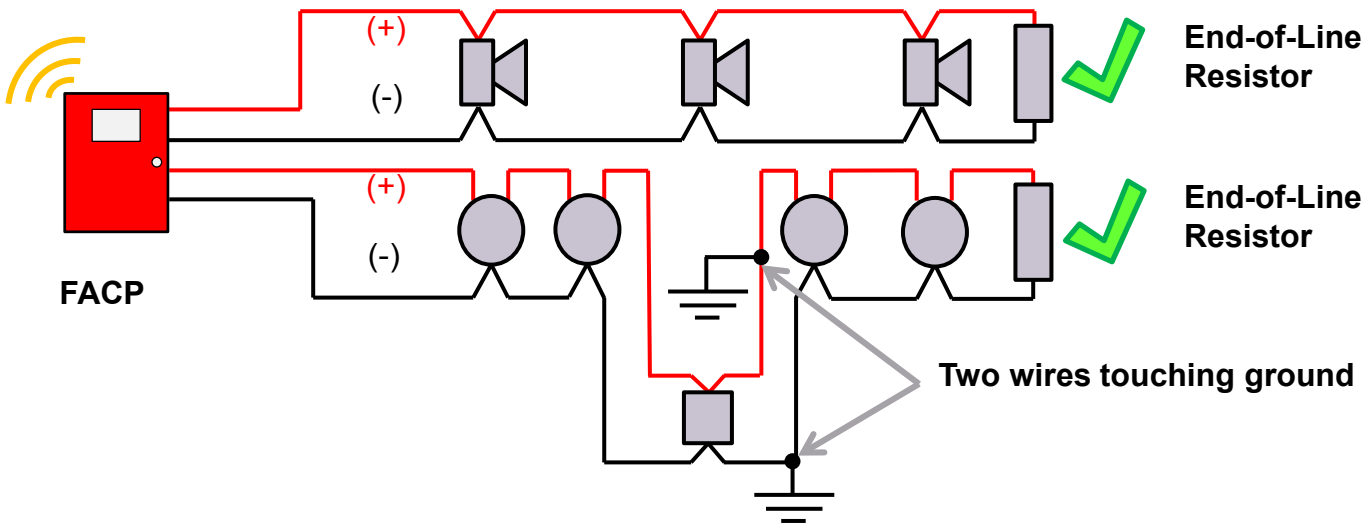
Approved Fire Alarm Pathway

Class B pathways report a single ground connection.



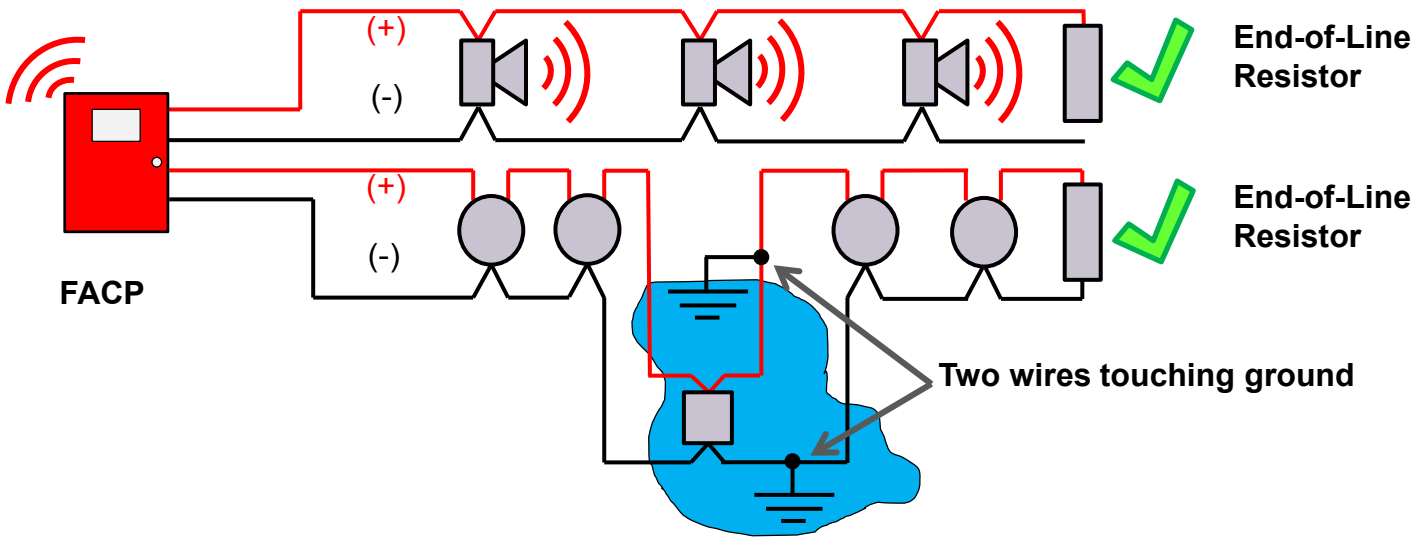
Approved Fire Alarm Pathway

Class B pathways report a single ground connection because, a second ground connection may occur at some point later, and act like a short-circuit.



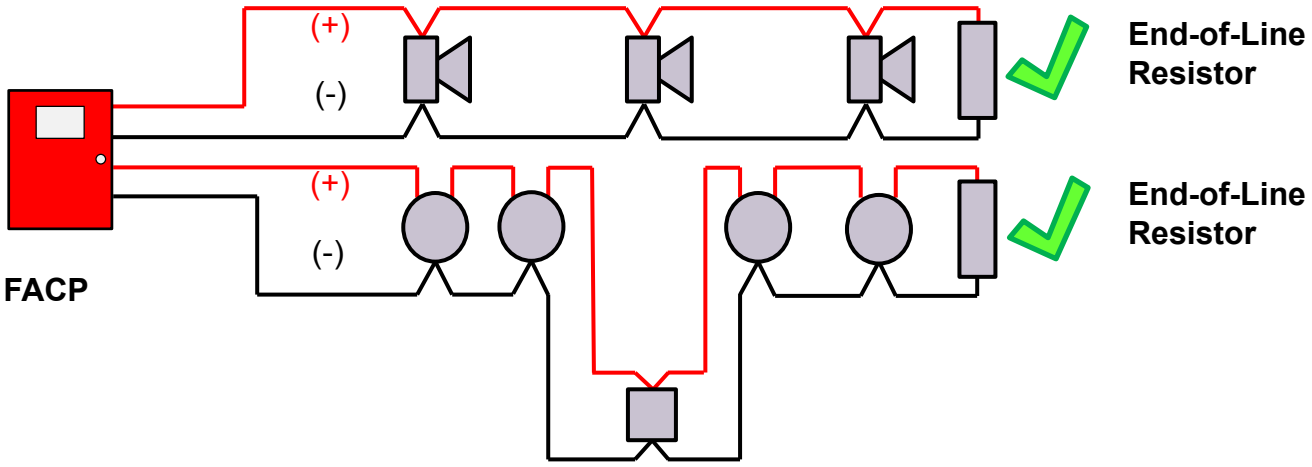
Approved Fire Alarm Pathway

Class B pathways report a single ground connection because, a second ground connection may occur at some point later, and act like a short-circuit. And, on a Class B IDC, a short-circuit means alarm!



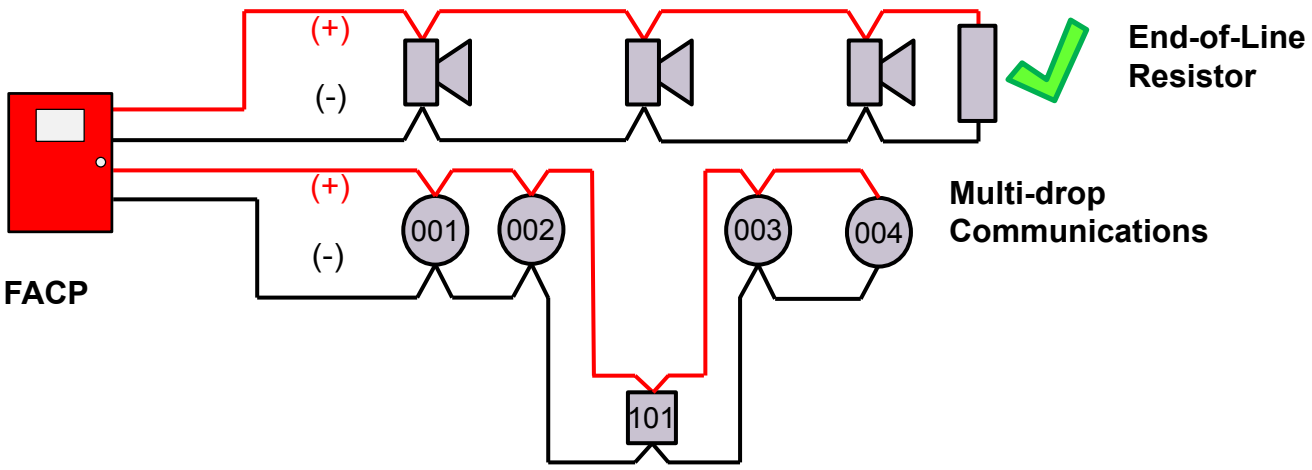
Approved Fire Alarm Pathway

It's worth noting, these methods of monitoring for integrity are only checking the wires. We don't know if any device is actually functional, but we can be reasonably certain the intended wires are connected.



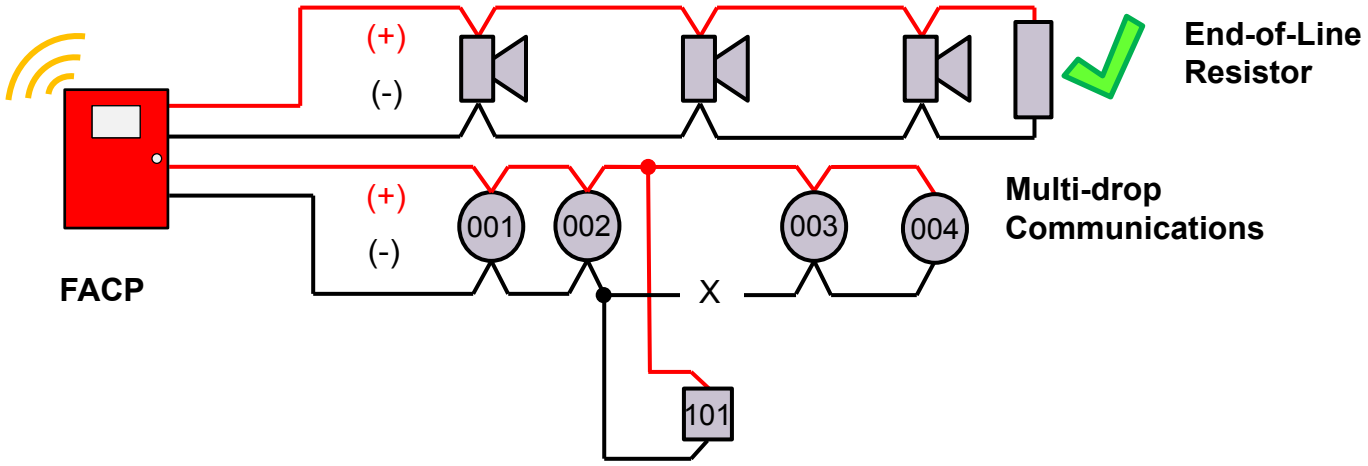
Approved Fire Alarm Pathway

The Class B, multi-drop signaling line circuit (SLC) gives each device a numerical address, and the control unit can communicate with all attached devices on just two wires in parallel.



Approved Fire Alarm Pathway

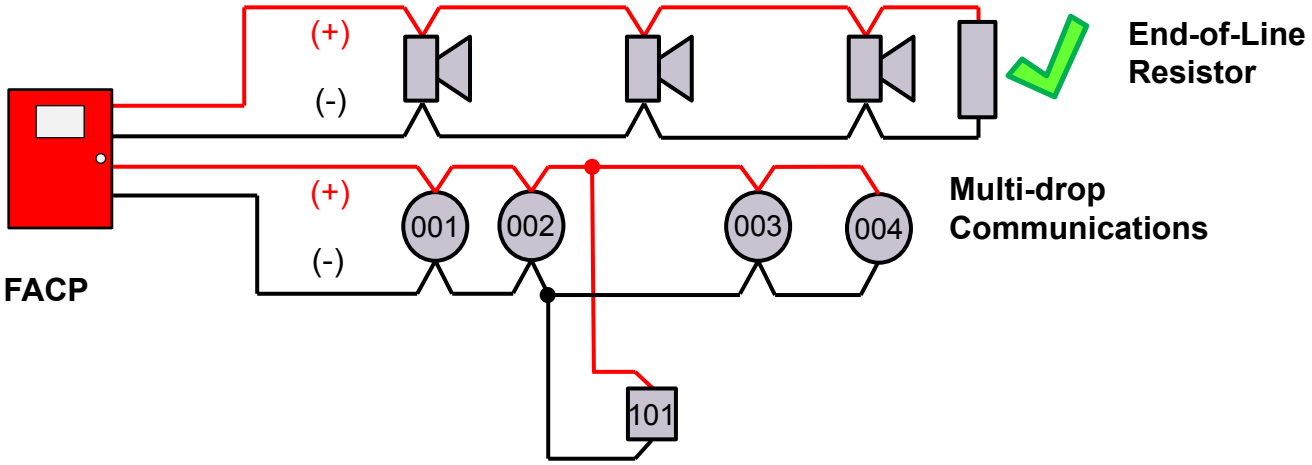
An open on a Class B SLC reports a trouble if the control unit cannot communicate with every device.



Approved Fire Alarm Pathway

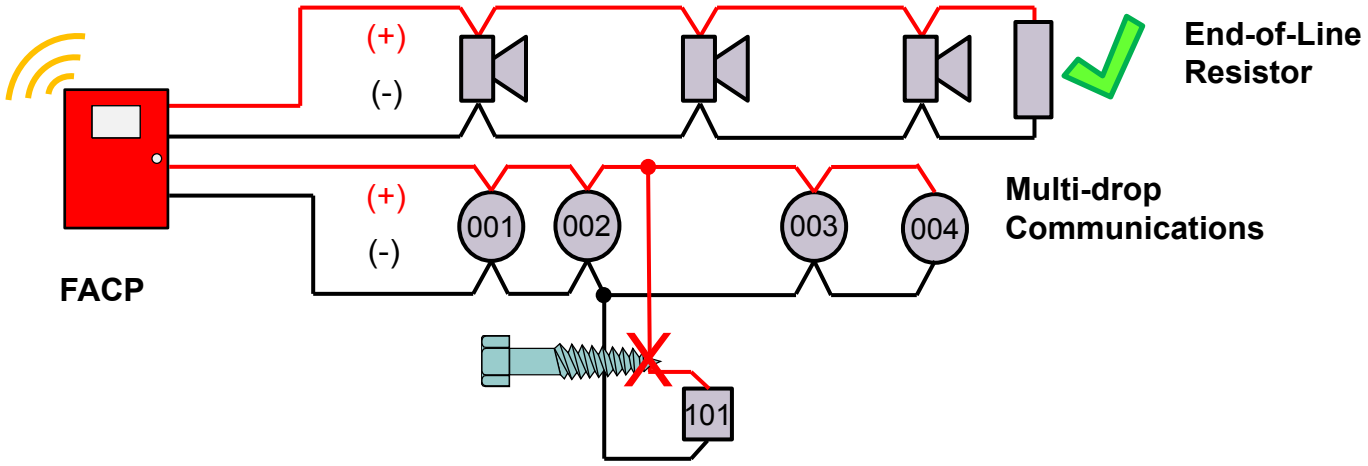
For decades, smart systems have been known as an improvement over conventional fire alarm systems. AHJs can see the obvious improvement that communication with each device provides.

Still, minimum Code requirements do not require operational capability of each device to be known. We only *require* the wires to be monitored.



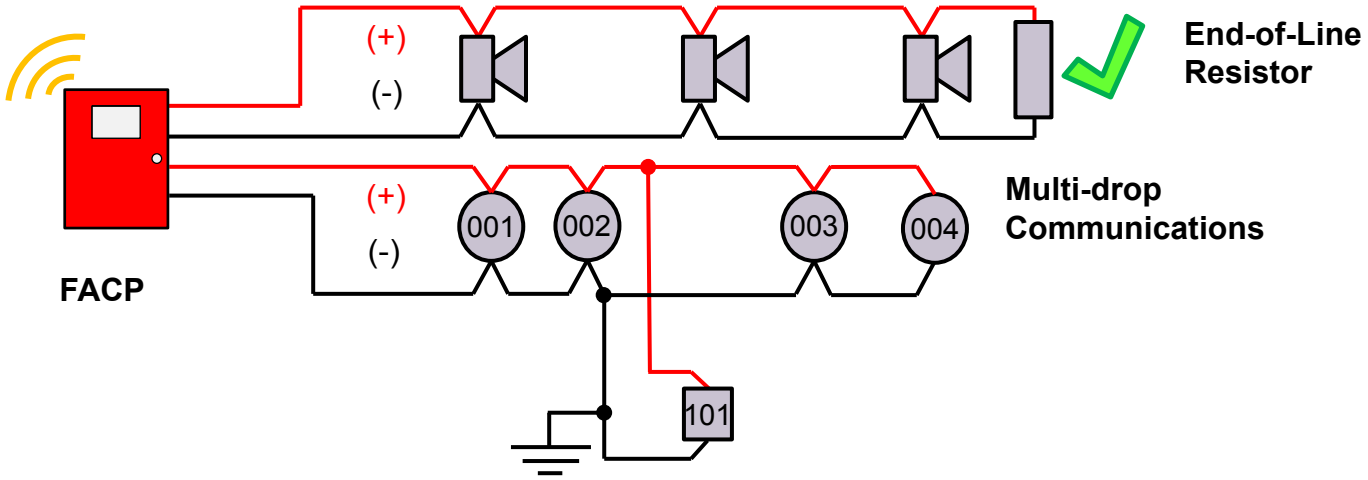
Approved Fire Alarm Pathway

Shorting the two wires at any point stops communication with every device. Not an indication of alarm as with an IDC, a short on the Class B SLC reports a trouble.



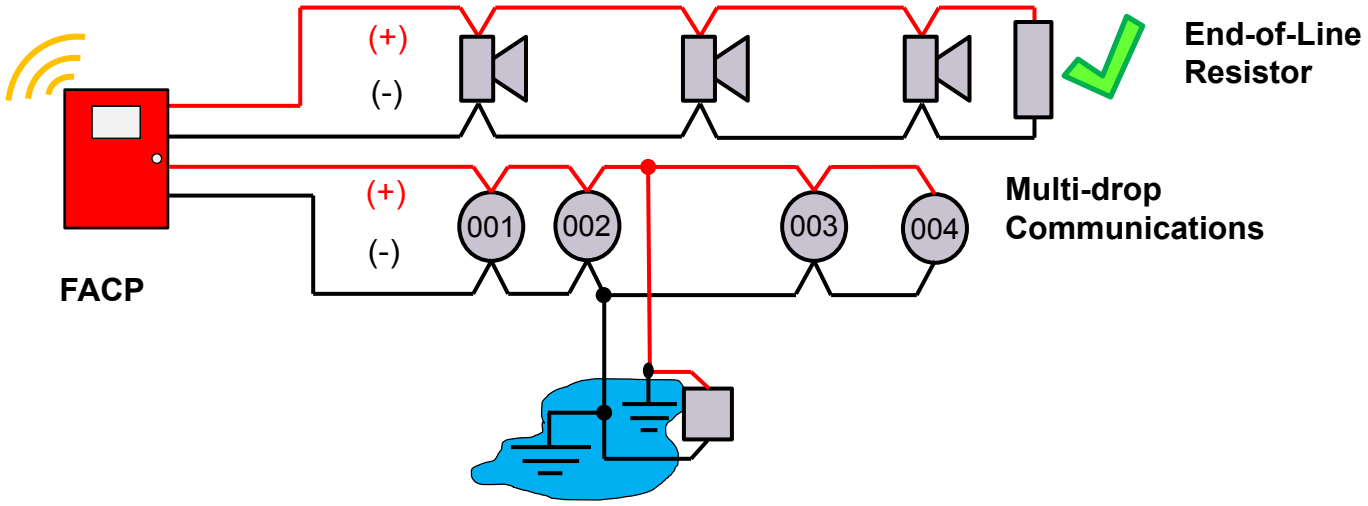
Approved Fire Alarm Pathway

While every device is attached to the same two wires, a single ground reports a trouble. But, the single ground is not allowed to impact communications.



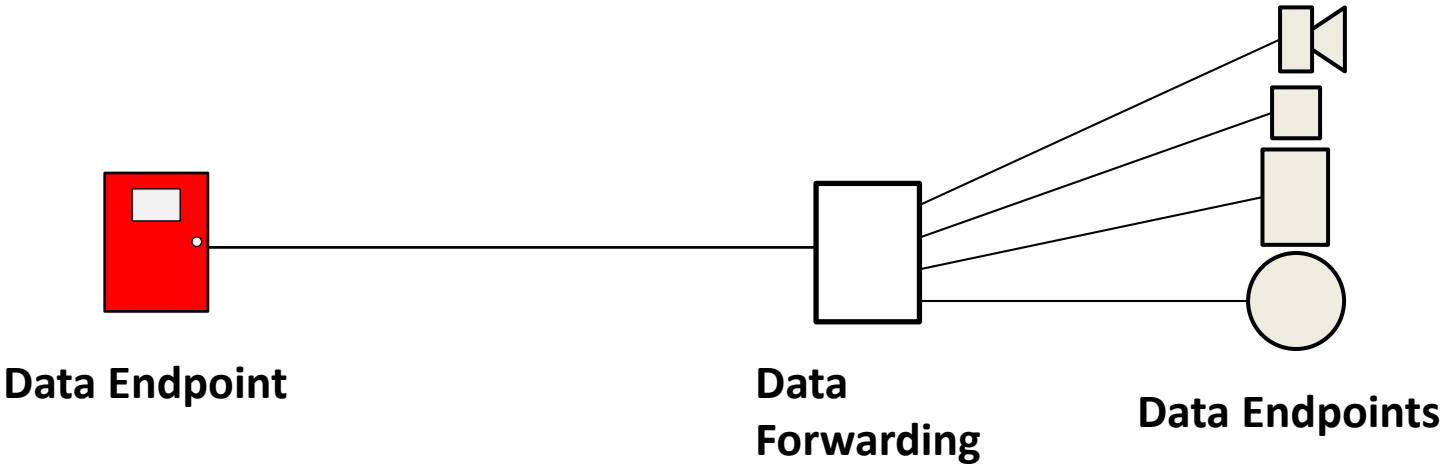
Approved Fire Alarm Pathway

A second ground on a Class B, *multi-drop* signaling line circuit stops all communication, as it is a short-circuit.



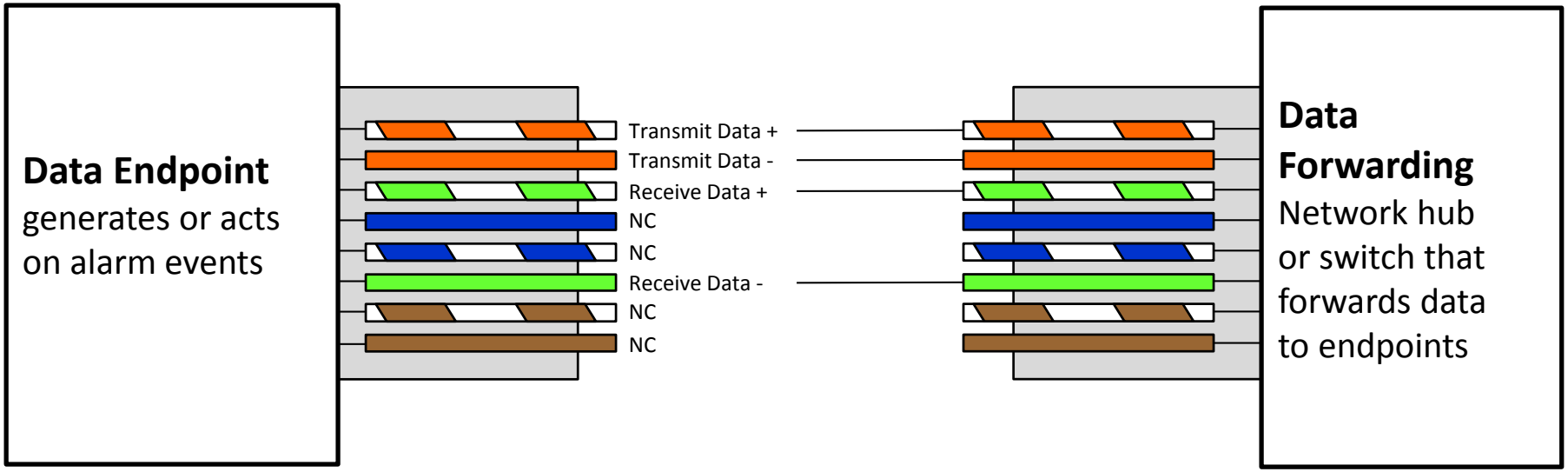
Ethernet Fire Alarm Pathway

Network equipment can be thought of in two basic categories: Data Endpoints and Data Forwarding Equipment.



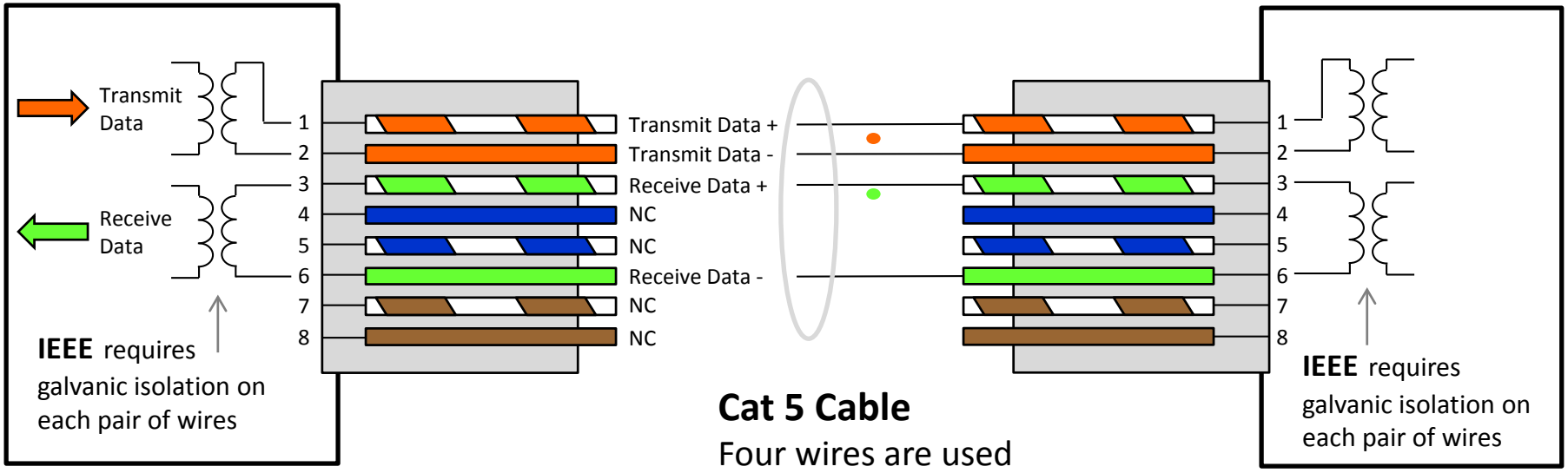
Category 5 Ethernet Cable

In between Data Endpoints and Data Forwarding Equipment, fiber-optic or metallic cable is used. Fiber is not affected by grounds. ‘Cat 5’ is an example of standardized metallic cable.



Category 5 Ethernet Cable

Each Cat 5 cable is galvanically isolated at each end, inside the equipment. The isolation helps prevents transient grounds and shorts on one cable from affecting other components.



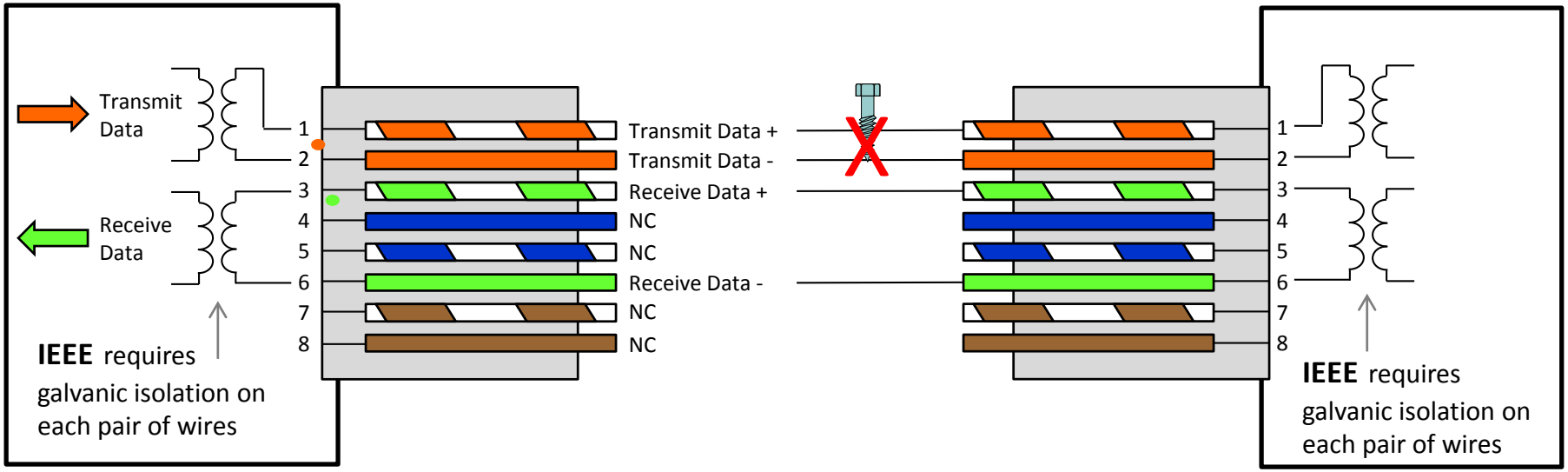
Data Endpoint
generates or acts on alarm events

Cat 5 Cable
Four wires are used for data transmission

Data Forwarding
Network hub or switch that forwards data to endpoints

Category 5 Ethernet Cable

If Transmit Data (+) and (–) or Receive Data (+) and (-) are shorted together, communication stops. In fire alarm systems, a fault condition must be reported within 200 seconds.

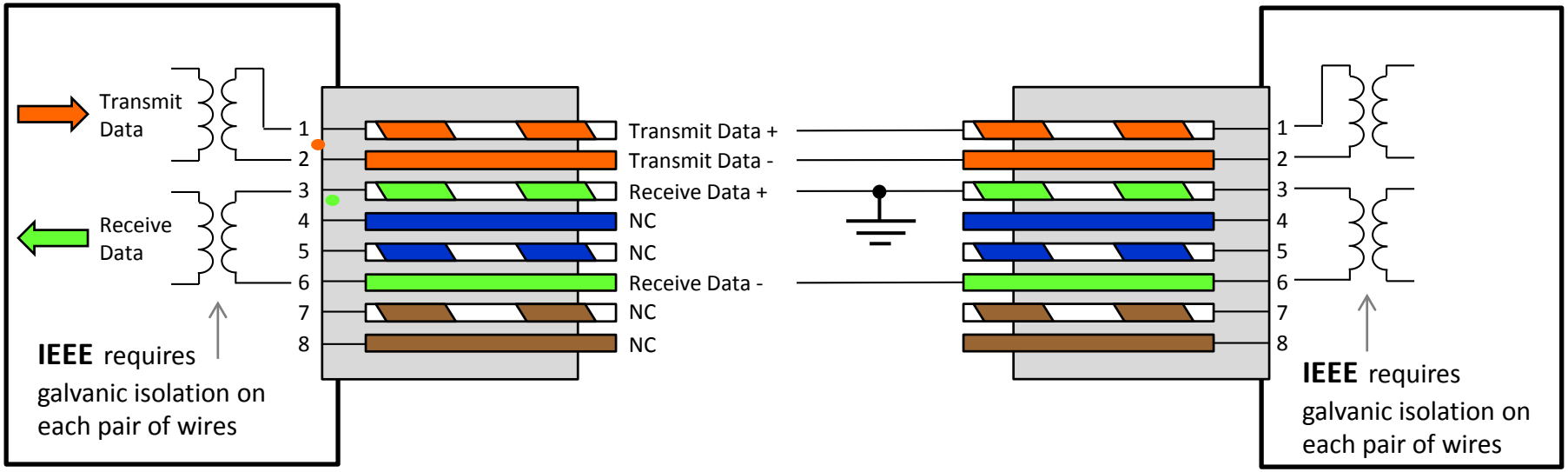


Data Endpoint
generates or acts on alarm events

Data Forwarding
Network hub or switch that forwards data to endpoints

Category 5 Ethernet Cable

A ground connection on any one signal wire does not block communication. IEEE requires isolation at each end of every Cat 5 cable. Every data packet is checked for errors and re-transmitted until verified.

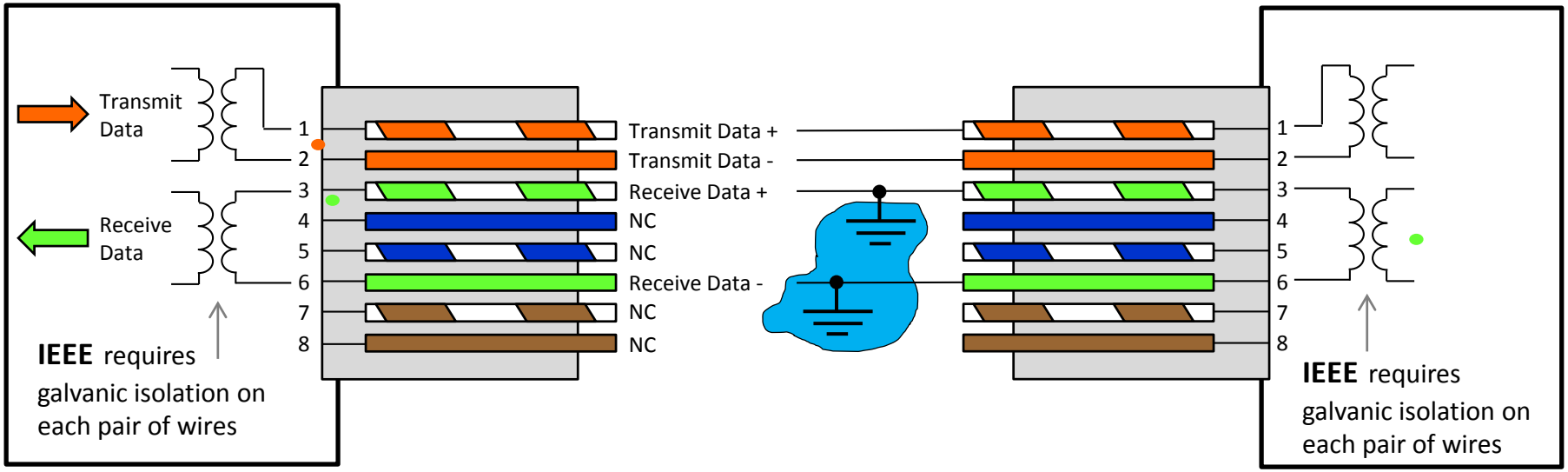


Data Endpoint
generates or acts on alarm events

Data Forwarding
Network hub or switch that forwards data to endpoints

Category 5 Ethernet Cable

A second ground connection, on the other wire of a matched pair, will impair communication if it causes a short. A fault condition must be reported within 200 seconds.



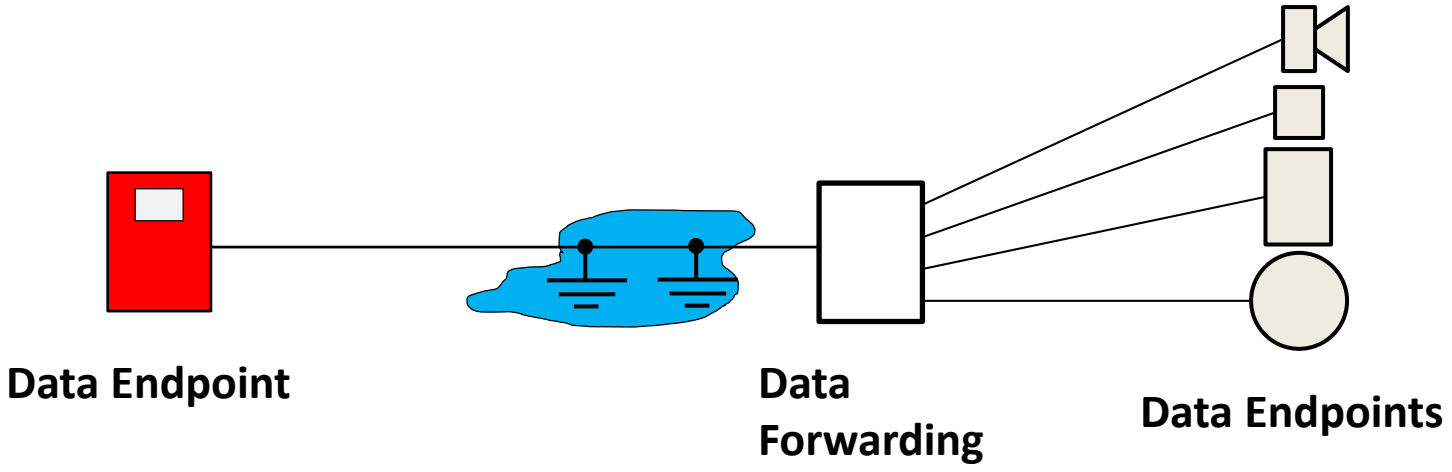
Data Endpoint
generates or acts on alarm events

Data Forwarding
Network hub or switch that forwards data to endpoints

Class N Network

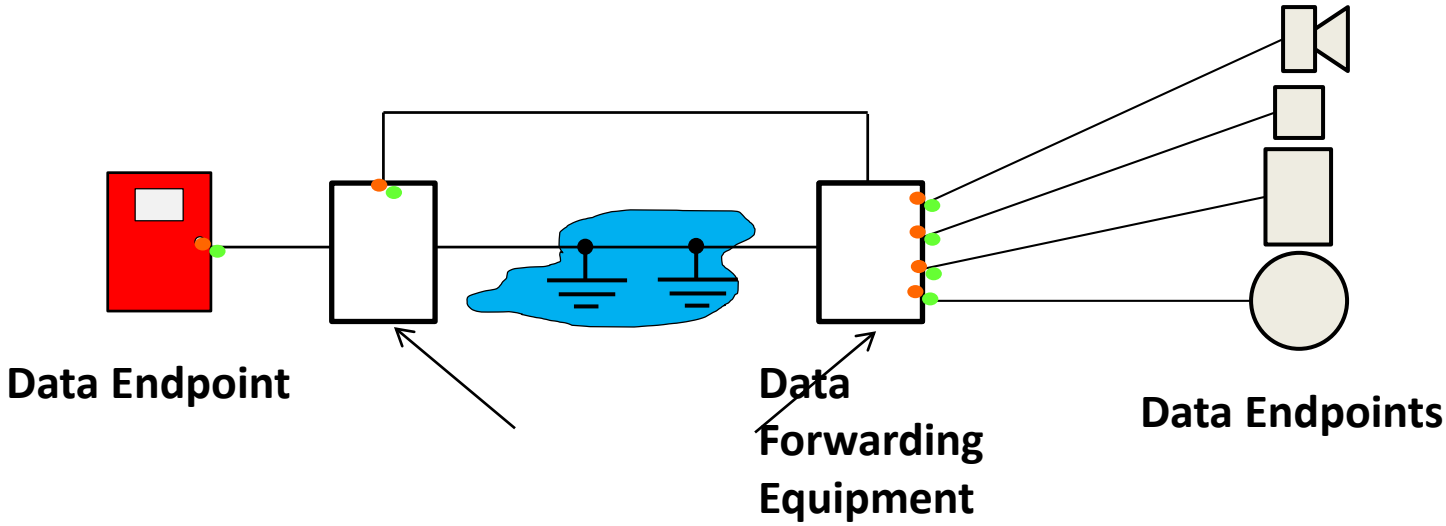
Here you can see a potential vulnerability. If a single path were to become impaired, multiple data endpoints would not communicate with essential equipment.

Good network design prevents a fault on any single cable from making more than one device inoperable.



Class N Network

Class N paths require alternate communication pathways whenever more than one device would be impacted by a fault.



Class N

Ethernet cables do not report grounds. To compensate, a Class N design has these requirements:

- Any segment of a path to more than one field device must be redundant, similar to Class A or X.
- Single paths may be used when only one device is dependent on the path, similar to Class B.

Class N

NFPA 72 allows Class N, with no requirement to report a single connection to ground.

NFPA 72, 2016 Edition

12.3.6 Class N.
A pathway shall be designated as Class N when it performs as follows:
(1) * It includes two or more pathways where operational capability of the primary pathway and redundant pathway to each device shall be verified through end-to-end communication.

Exception: When only one device is served only one pathway shall be required.

(2) A loss of intended communications between endpoints shall be annunciated as a trouble signal.
(3) A single open, ground, short, or combination of faults on one pathway shall not affect any other pathway.
(4) * Conditions that affect the operation of the primary pathway(s) and redundant pathways(s) shall be annunciated as a trouble signal when the system's minimal operational requirements cannot be met.
(5) * Primary and redundant pathways shall not be permitted to share traffic over the same physical segment.

NFPA 72, 2016 Edition Class N Annex

The NFPA 72 Annex has the detail!

A.12.3.6(1) The Class N pathway designation is added to specifically address the use of modern network infrastructure when used in fire alarm and emergency communication systems.

Class N networks may be specified for ancillary functions, but are not required for supplemental reporting described in 23.12.4. [See Figure A.23.12.4.]

Ethernet network devices are addressable, but with an important distinction from device addresses on a traditional SLC multi-drop loop. A device with an Ethernet address is, in most cases, a physical endpoint connected to a dedicated cable. Traditional SLC devices are all wired on the same communication line (in parallel) similar to an old party-line telephone system. By comparison, Ethernet's network switches direct each data packet to its intended recipient device like our modern phone systems.

NFPA 72, 2016 Edition Class N Annex

Figure A.12.3.6(1)(a) Class N Pathway Block Diagrams.

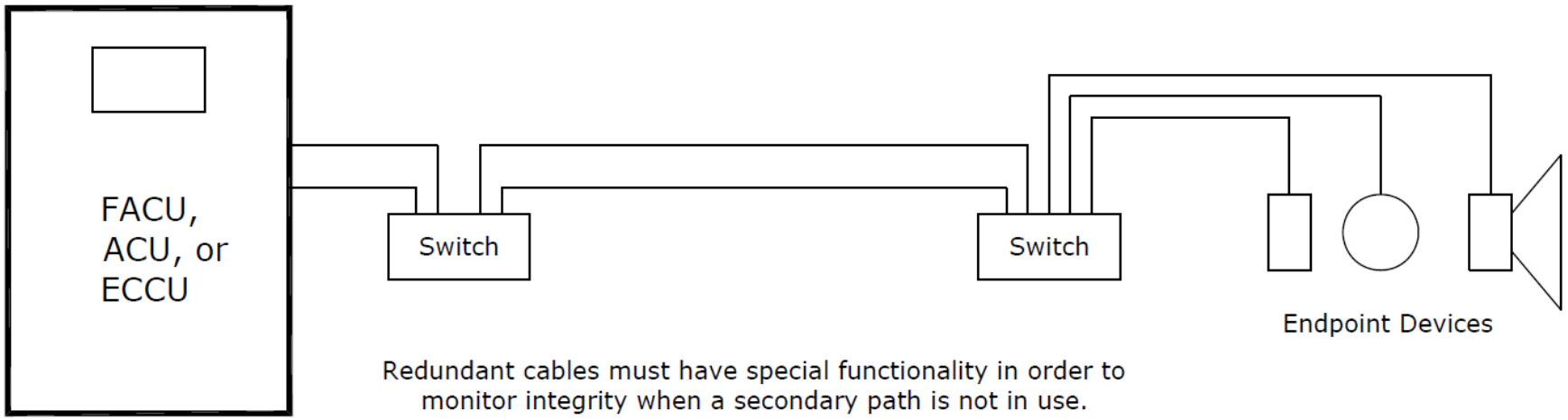


Figure A.12.3.6(1)(a-1)

NFPA 72, 2016 Edition Class N Annex

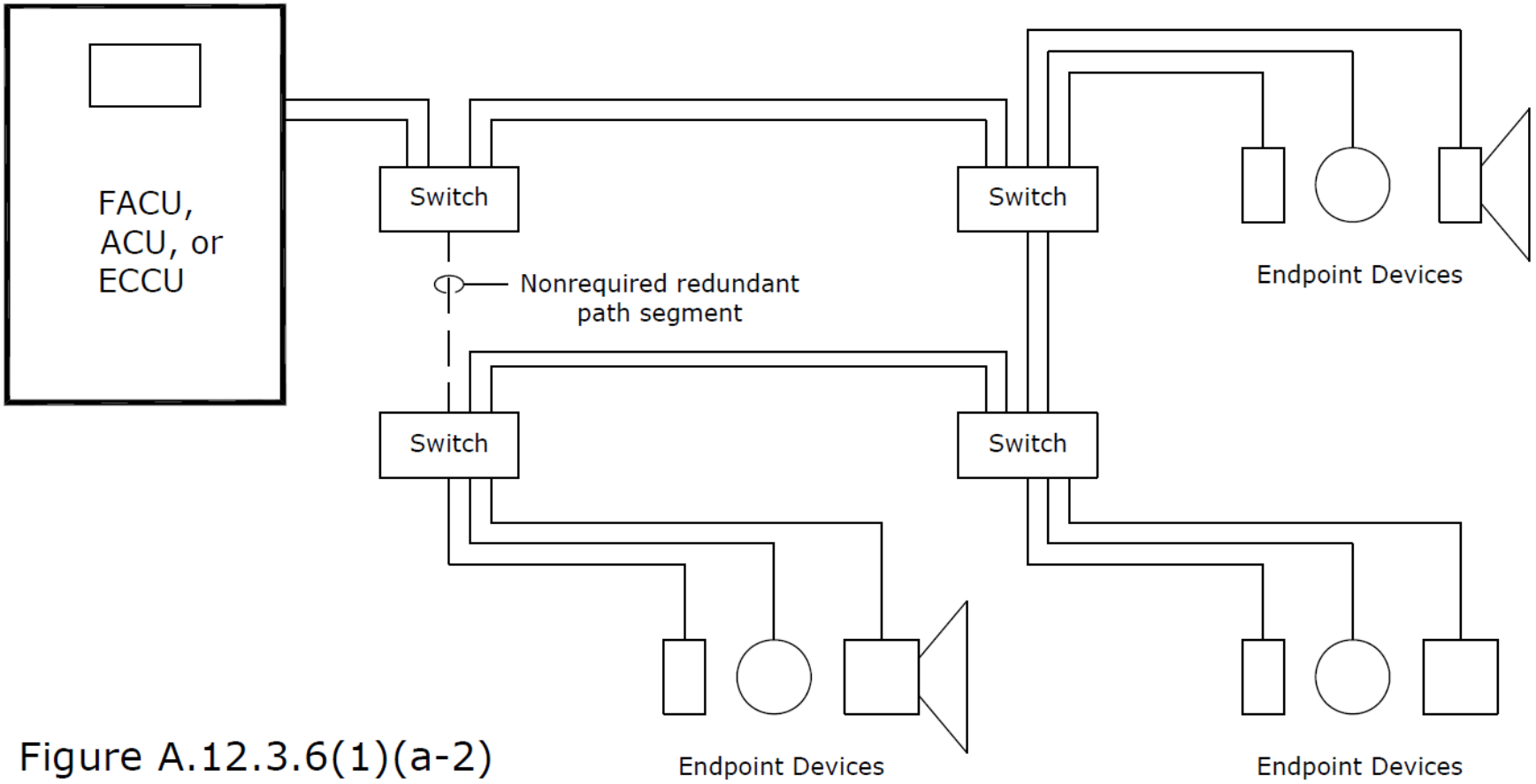
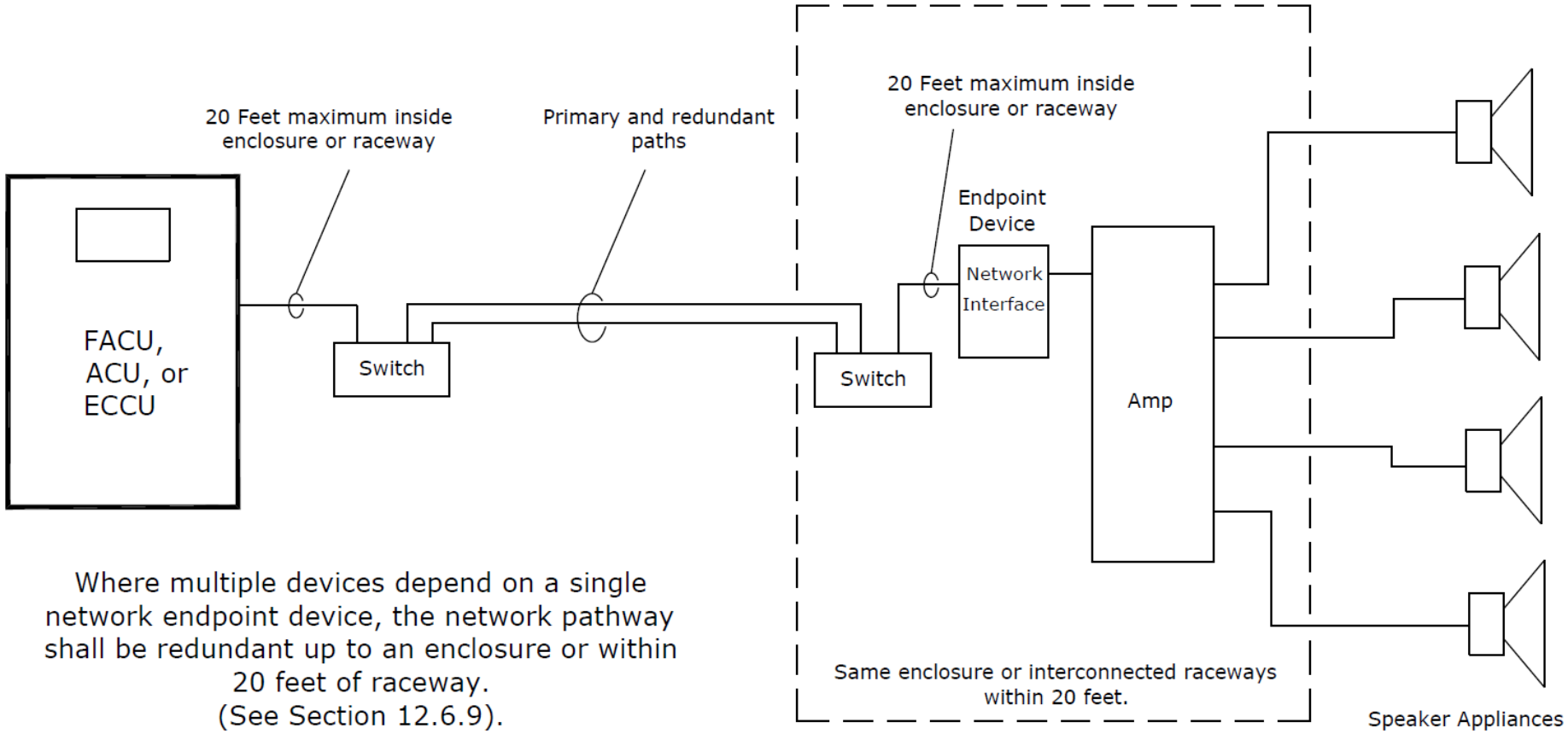


Figure A.12.3.6(1)(a-2)

NFPA 72, 2016 Edition Class N Annex

Figure A.12.3.6(1)(a-3) Class N Pathway to Endpoint with Multiple Devices.



Where multiple devices depend on a single network endpoint device, the network pathway shall be redundant up to an enclosure or within 20 feet of raceway. (See Section 12.6.9).

NFPA 72, 2016 Edition Class N Annex

Class N connections between control equipment are required to have redundant monitored pathway segments if a failure of a primary pathway segment in between control equipment could impair the operation of the control equipment *[see Figure A.12.3.6(1)(b)]*.

Figure A.12.3.6(1)(b) Class N Pathway Block Diagram with Multiple Control Units.

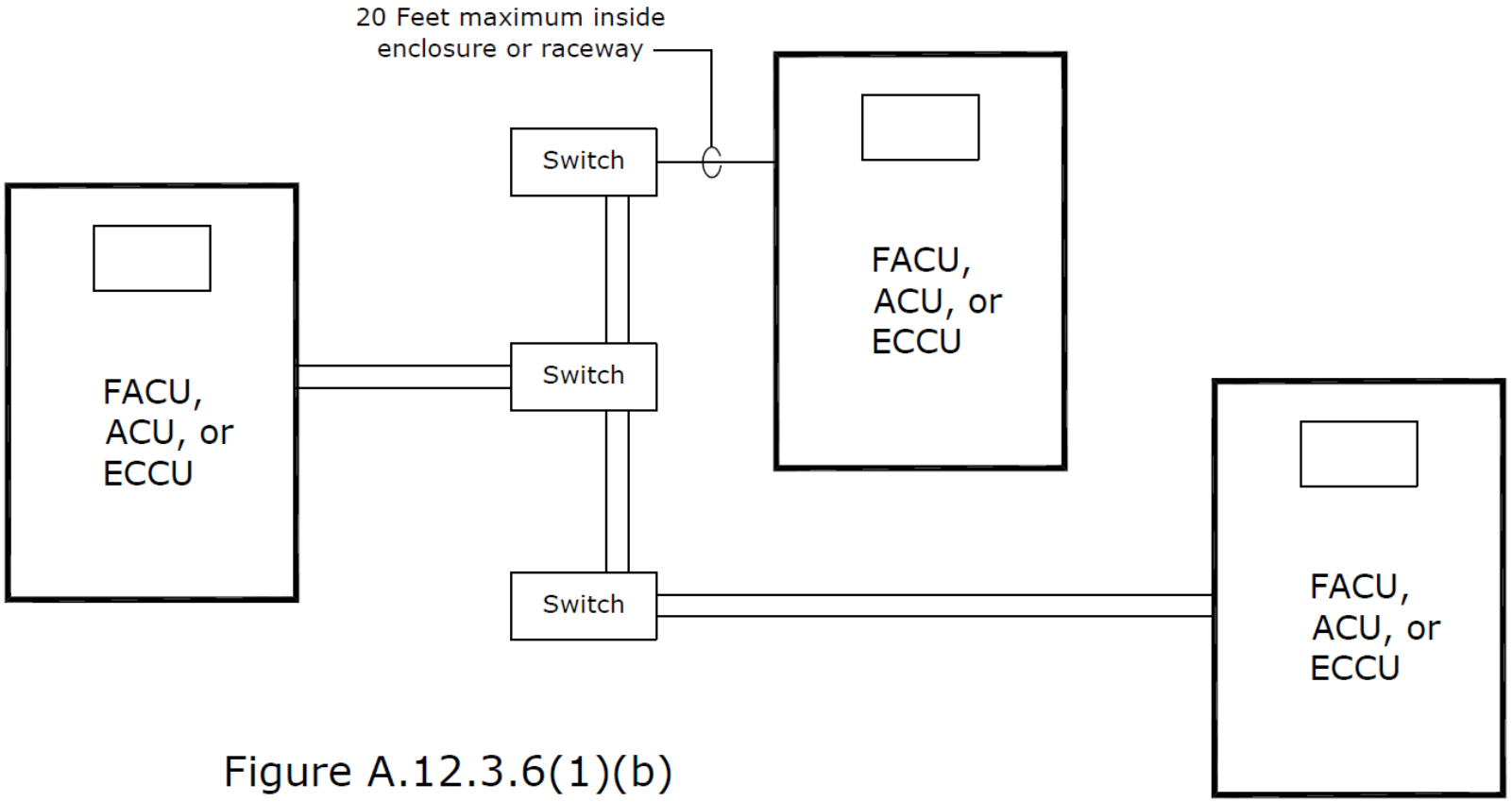
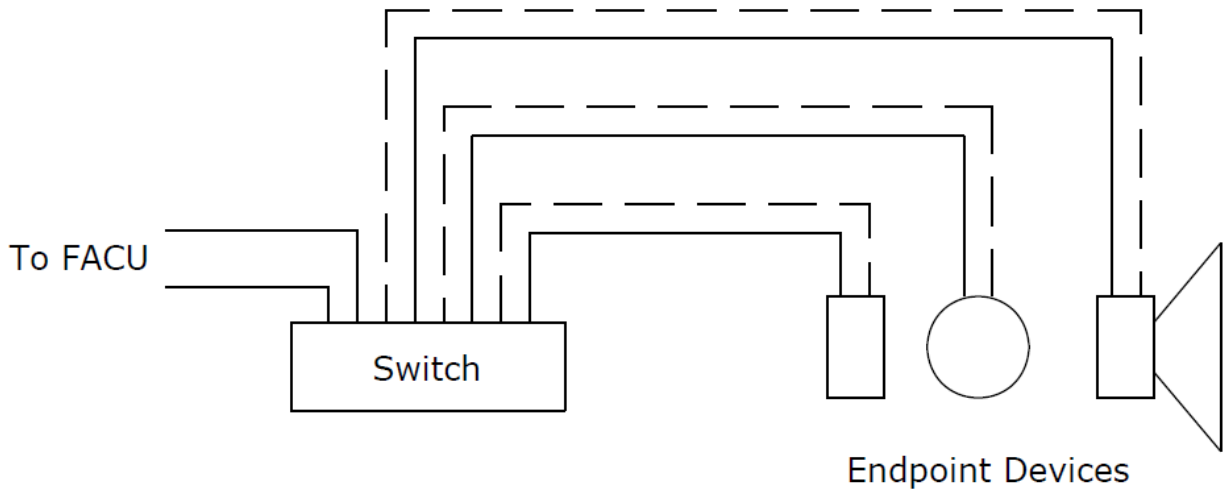


Figure A.12.3.6(1)(b)

Class N is also permitted to include dual port devices that provide both transmission and input/output functions. Endpoint devices may have multiple connection ports and support dual pathway segment connections; thus the term *endpoint device* is not intended to prohibit more than one connection to a device. Even with dual connections, where other devices depend on the path, primary and redundant paths are required. But, where an endpoint device has two connection ports, and when a secondary nonrequired connection is added, there is no requirement to separately supervise the nonrequired redundant pathway segment *[see Figure A.12.3.6(1)(c)]*.

Figure A.12.3.6(1)(c) Class N Pathway Block Diagram with Device with Dual Pathway Connection.



A nonrequired redundant cable to an endpoint device is permitted, and does not require separate supervision.

Figure A.12.3.6(1)(c)

A.12.3.6(5)

Devices with dual path connections are permitted to be connected in a daisy-chain of devices on a ring. Again, where Class N pathway segments support multiple devices, verified redundant pathway segment(s) are required. This can be accomplished with a ring topology, as long as each segment of the ring is verified as functional, and the failure of any one segment does not result in the loss of functionality of more than one device. In this arrangement, primary and redundant pathway segments share the same media, and provide two possible directions of communications in a ring topology *[see Figure A.12.3.6(5)]*. This daisy-chain configuration is also permitted between multiple control units that require verified primary and redundant pathway segments.

Figure A.12.3.6(5) Class N Pathway Block Diagram with Daisy-Chained Devices with Dual Pathway Connection.

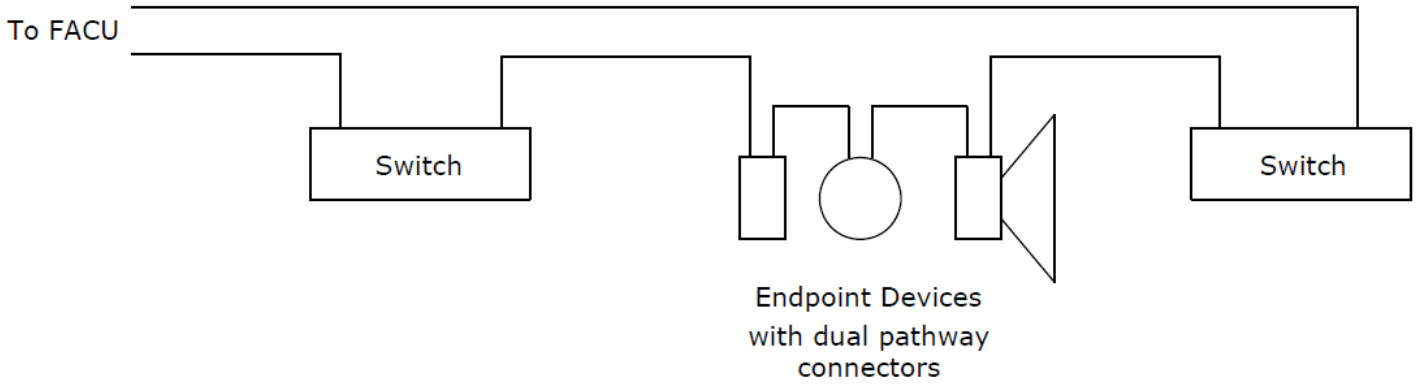


Figure A.12.3.6(5)

Shared Pathways:

Besides ground-fault reporting, another primary concern expressed by the Technical Committee was sharing networks. Typical network components might not be as durable as equipment that is UL-listed for fire alarm systems.

In addition, the code requires backup power, which might not be supplied to typical network components.

NFPA 72

NFPA 72, 2016 Edition

12.5* Shared Pathway Designations. Shared pathways shall be designated as Level 0, Level 1, Level 2, or Level 3, depending on their performance.

12.5.1* Shared Pathway Level 0. Level 0 pathways shall not be required to segregate or prioritize life safety data from non–life safety data.

12.5.2* Shared Pathway Level 1. Level 1 pathways shall not be required to segregate life safety data from non–life safety data, but shall prioritize all life safety data over non–life safety data.

12.5.3* Shared Pathway Level 2. Level 2 pathways shall segregate all life safety data from non–life safety data.

12.5.4* Shared Pathway Level 3. Level 3 pathways shall use equipment that is dedicated to the life safety system.

NFPA 72

NFPA 72, 2016 Edition

23.6.3 Class N Shared Pathways. Class N pathways shall be required to use shared pathway Level 3 as specified in 12.5.4 except as permitted by 23.6.3.1 through 23.6.3.8.

23.6.3.1 Level 1 and Level 2. Shared pathways Levels 1 and 2 shall be permitted subject to a thorough written analysis of the risks, the maintenance plans, roles and responsibilities, and a deployment plan as identified in 23.6.3.3 and when approved by an AHJ in consideration of the analysis, maintenance, and deployment plans.

Planning and Management is required

NFPA 72 2016 Edition

23.6.3.2 Accessibility. Class N pathways shall not be accessible to the general public for any purpose or building occupants for any purpose other than specified in the analysis, maintenance, and deployment plans.

23.6.3.3 Deployment Plan.

23.6.3.3.1 All equipment connected to shared pathways shall be documented in the deployment plan.

23.6.3.3.1.1 The documentation shall include manufacturer, model, listings, and intended purpose and reason for inclusion on the shared network.

23.6.3.3.1.2 The deployment plan shall identify how and where each piece of equipment is connected.

23.6.3.3.2 All connection ports, used or spare, where any unauthorized or unintended equipment may be added to the shared network, shall be identified as for use only by equipment consistent with the deployment plan.

23.6.3.4 Change Control Plan. Configuration upgrades and updates shall be governed by a change control plan, which determines the policy and procedure of the change and ensures that all documentation is correspondingly updated.

23.6.3.5 Management Organization.

23.6.3.5.1 An organization shall be established and maintained to manage the life safety network and shall perform the following tasks:

(1) Contain members appropriately certified by each manufacturer of the equipment and devices deployed on shared pathways to maintain such a network
(2) Service and maintain all shared Class N pathways
(3) Maintain the deployment and shared pathways plan for the lifetime of the shared pathways

23.6.3.5.2 Other service personnel, even when certified to service a specific system (i.e., fire alarm or MNS) shall be authorized and managed by this organization to ensure any outages of any system are planned, managed, and documented and appropriate steps are taken during outages to provide alternate protection of life and property.

23.6.3.6 Analysis.

23.6.3.6.1 The analysis shall be performed to determine and document communications capability as follows:

(1) Calculation of minimum required bandwidth such that all life safety systems can be guaranteed to operate simultaneously and within required time limits
(2) Total bandwidth provided by the network
(3) Future bandwidth requirements
(4) Method of providing and maintaining the prioritization of life safety traffic over non–life safety traffic

23.6.3.6.2 The analysis shall determine and document the power distribution capability as follows:

(1) The methods provided to maintain power to all shared pathway equipment
(2) A calculation of power requirements of all connected equipment
(3) Secondary power capacities provided to maintain all life safety equipment with minimum operational capacity in accordance with 10.6.7.2.1.2
(4) Methods to disengage any non–life safety equipment in the event of emergency operation if required to support the minimum operational capacity requirements

23.6.3.7 Maintenance Plan.

23.6.3.7.1 The maintenance plan shall identify policy and procedures to monitor, maintain, test, and control change of the shared pathways.

23.6.3.7.2 Written procedures shall be presented in maintenance plans to govern the following:

(1) Physical access to all parts of the Class N network equipment (i.e., switches, ports, server, controllers, devices, or components)
(2) Electronic access to all parts of the Class N network (i.e., passwords, addresses)
(3)*Service outage impairment process with notices of impairment and contingency plans for affected systems
(4) Upgrade procedures

When Class N is not required:

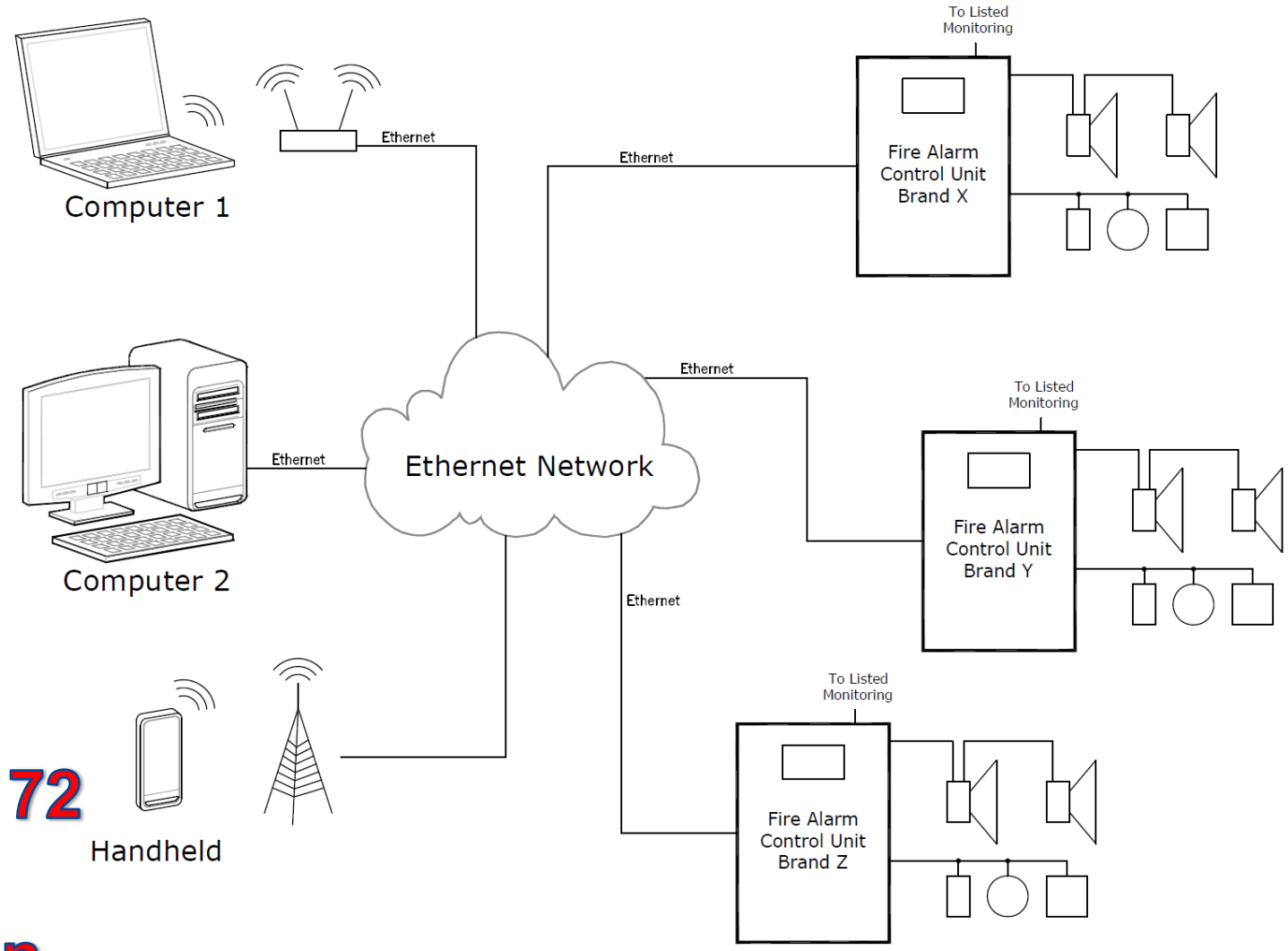
NFPA 72, 2016 Edition

A.12.3.6(1) The Class N pathway designation is added to specifically address the use of modern network infrastructure when used in fire alarm and emergency communication systems.

Class N networks may be specified for ancillary functions, but are not required for supplemental reporting described in 23.12.4. [See Figure A.23.12.4.]

Ethernet network devices are addressable, but with an important distinction from device addresses on a traditional SLC multi-drop loop. A device with an Ethernet address is, in most cases, a physical endpoint connected to a dedicated cable. Traditional SLC devices are all wired on the same communication line (in parallel) similar to an old party-line telephone system. By comparison, Ethernet's network switches direct each data packet to its intended recipient device like our modern phone systems.

New Diagram in Annex



NFPA 72 2016 Edition

Figure A.23.12.4 Supplemental Reporting Network

Supplementary

NFPA 72, 2010 – current Editions

23.12.4 It shall be permitted to provide supplementary transmission of real-time data from the fire system to off-premises equipment.

23.12.4.1 Transmission of real-time data off-premises shall not affect the operation or response of the fire alarm control unit.

23.12.4.2 Any data transmitted shall be consistent with the data generated by the system.

A.23.12.4 Off-site logging of fire alarm data can be useful to preserve information in the face offire or building failure to facilitate accurate reconstruction of the event. It can also be beneficial to send data off-premises to incident command personnel to enhance situational awareness and response decisions and to maintain safe and efficient operations.

Figure A.23.12.4 shows an example of a network to accomplish these goals.