AN EXPERT RESOURCE GUIDE FROM CADGRAPHICS, INC.
MAKERS OF RESCUELOGIC SOFTWARE

CLASS N

NETWORKS FOR FIRE ALARM AND MASS NOTIFICATION SYSTEMS

BY DAN HORON

MEMBER OF THE TECHNICAL CORRELATING COMMITTEE TASK GROUP ON NETWORKS AND CO-AUTHOR OF THE NEW NETWORKING SECTION IN THE NFPA 72 HANDBOOK

CLASS N

NETWORKS FOR FIRE ALARM AND MASS NOTIFICATION SYSTEMS

AN EXPERT RESOURCE GUIDE

CLASS N

For more information about networked fire alarm and
mass notification systems, visit rescuelogic.com or call 612-722-3233.

June 2016
Cadgraphics, Inc.

ISBN-13: 978-0692724125
ISBN-10: 0692724125

CONTENTS

INTRODUCTION

Fire safety technicians have been using computer technology for years. Back in the 1980s, when I was starting my career as a fire alarm designer, resisters and relays were still standard — but some engineers were starting to use CPUs, or processor chips, in new panels.

They were fighting an uphill battle. I still remember fire marshals who said they would never allow CPU-based systems in their district.

Today, almost every fire alarm system depends on CPUs. Lots of them — in networks, addressable smoke detectors, and CPU-based modules. We rely on computer technology to monitor the hard-wired devices in every fire and security system on the market.

In 1987, I started developing software that could receive and interpret the computerized data inside those new the fire panels, by streaming data from the panels through RS232 ports on standard PCs.

After years of study, debate, and development, the NFPA has established parameters for Ethernet connections — which brings fire alarm technology into a brave new world.

Like any technician, I faced a few problems along the way. One of them was ground faults. RS232 data ports use ground as a common reference for the data signal itself. That meant that when I connected a grounded PC to a panel, the panel's ground fault trouble alert would activate. I spent years searching for simple, economical RS232 isolators. There weren't many. It wasn't a huge market.

Eventually, I discovered that I could connect Ethernet devices to RS232 ports. Because Ethernet is isolated from ground, the connection didn't trigger any troubles or faults.

By that time, I was a member of the NFPA Protected Premises Technical Committee. When our committee started studying Ethernet and grounding issues, I was happy to share what I'd learned in the field — and I was pleased to help introduce new parameters for Ethernet connections in the 2016 edition of NFPA 72.

FEATURES AND BENEFITS

When you follow the new Ethernet connection guidelines, you can:

- Safely use standard networks to connect fire alarm devices to control units.
- Use technology more commonly familiar to a broad range of designers, installers, and end users.
- Integrate data collection
- Obtain a special fire protection UL Listing for equipment already on the market.

NETWORKING HISTORY

Here's a brief technical description of networking technology.

Historically, fire alarm technicians have used two-conductor cable to network the electrical components of most fire alarm systems.

That cable connects all of the devices to a control panel as signaling line circuits (SLC), initiating device circuits (IDC), and notification appliance circuits (NAC).

All devices connect to the same two parallel conductors as they traverse a building. Isolator modules can mitigate the potential for faults that could occur between those two wires.

These days, however, we can connect most electronic devices — including fire alarm equipment — to a segmented network with isolation at each device. Highly reliable computer networks already exist in many buildings.

In the past, fire codes required private, proprietary communication networks — both to ensure a high level of integrity and reliability, and to ensure that a fire alarm system wouldn't be compromised by computers or other electronic equipment.

Proprietary networking, however, is costly and time-consuming. It's also outdated.

That's why the NFPA 72 Technical Correlating Committee decided to explore today's technology — and make it possible for building owners and managers to safely use existing network technology to connect fire alarm devices to their control units.

It's a huge leap forward for fire protection, and it's just common sense. When technicians can use standardized networks in a building, wiring costs are greatly reduced, and engineers are free to make changes and additions quickly and economically.

SAFETY CONCERNS

In the past, NFPA code committees were slow to adopt the use of common Ethernet networks, for these reasons:

- Administration. It wasn't clear that technicians could control, test, and document fire systems on a general building network.
- Ground faults. Ethernet technology doesn't report connections to ground because a ground will not affect the isolated Ethernet equipment.
- Network integrity. What would happen if other signal traffic overloaded the capability of the network and prevented the fire alarm system from working?
- Multiple manufacturers. Proprietary networks are a known commodity, but would a fire alarm system have the same integrity if the network was made up of different parts?
- Durability. Typical off-the-shelf network components might not be as durable as equipment that is UL-listed for fire alarm systems.
- Emergency power. Ordinary networks go down when the power goes out. Fire alarm networks need backup power.
- Network Reliability. Even if a network is reliable when the fire alarm system is installed and tested, what will happen when it goes down? Most down-time events happen when information technology personnel are performing upgrades, reconfigurations, rerouting of cables, testing, and maintenance.

Ultimately, NFPA committee members decided that networked systems could be allowed — provided that all of the components meet the standards and requirements of NFPA 72.

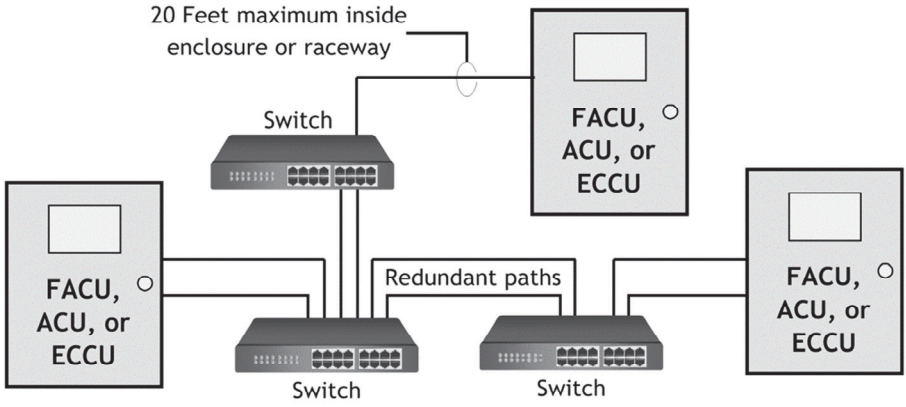
The language of NFPA's new Class N requirements address all of the safety issues we've questioned in the past.

CLASS N SAFETY PROVISIONS

Here's what you need to know about using Ethernet networks for fire safety systems.

REDUNDANT BACKBONES

Your network needs to be redundant. You'll be required to establish alternate communication pathways whenever more than one device could be impacted by a fault.



Two or more paths are required between equipment that serves more than one device. Enclosures or raceway up to 20 feet may contain a single path.

INTEGRITY

You'll need to monitor your Ethernet network for integrity. For the most part, you can do that by monitoring the functionality of the communications.

If a particular device is broadcasting and responding, you can be reasonably sure that the wiring is intact, and the entire pathway will function during an emergency. NFPA 72 says "… a redundant pathway to each device shall be verified through end-to-end communication."

CLASS N CIRCUITS

Class N circuits require that you *know* there are two or more pathways available at all times. So, your monitoring must include a way to verify that at least two paths are viable. That is in addition to just having the pathway capability verified through end-to-end communication.

The NFPA Handbook says, "The redundant path intends to compensate for Ethernet wiring that cannot meet all of the fault monitoring requirements that normally apply to traditional wiring methods used for fire alarm circuits."

NETWORK DROPS

While redundancy is required for the backbone, Class N allows a pathway to branch off to an individual component without redundancy. In Ethernet networking terms, this would be a typical "network drop." In classic fire alarm terms, you might say the path to an individual device can be like a T-Tap on a Class B SLC. Technically, though, the network drop is its own dedicated cable branch with an addressable device at the end.

GROUND FAULT REPORTING

Class N doesn't require ground-fault reporting. As a result, robust and durable Ethernet components can now be listed by independent testing laboratories. They can be tested and listed as code-compliant, without special modification.

TODAY'S TECHNOLOGY

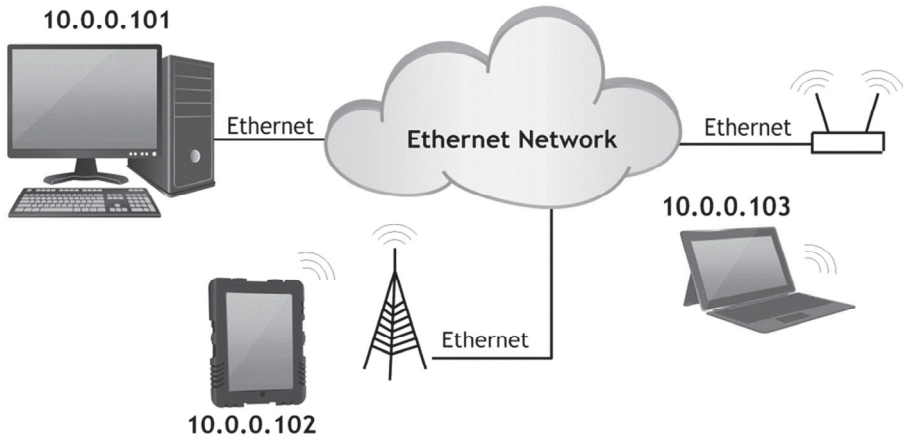
ETHERNET NETWORKS

Until now, most signaling line circuit (SLC) devices have been wired on the same communication line, in parallel. Every device on an SLC communicates on the same wires, like an old party-line telephone system.

When it comes to Ethernet connections, however, devices with Ethernet addresses aren't like those on a standard SLC multi-drop loop. In an Ethernet network, every device is a physical endpoint that's connected to a dedicated Ethernet cable.

In modern construction, Ethernet cable is distributed throughout a building, often in a honeycomb configuration. Network switches and routers send each data packet to its intended recipient device. Each endpoint device has an IP Address. Like our modern phone systems use of phone numbers, devices call each other's IP Address to establish communication. The specific path for that communication isn't material.

A TYPICAL ETHERNET CONFIGURATION



Every computer on a network has a unique IP Address. With communication established, different devices send and receive data to the IP Addresses.

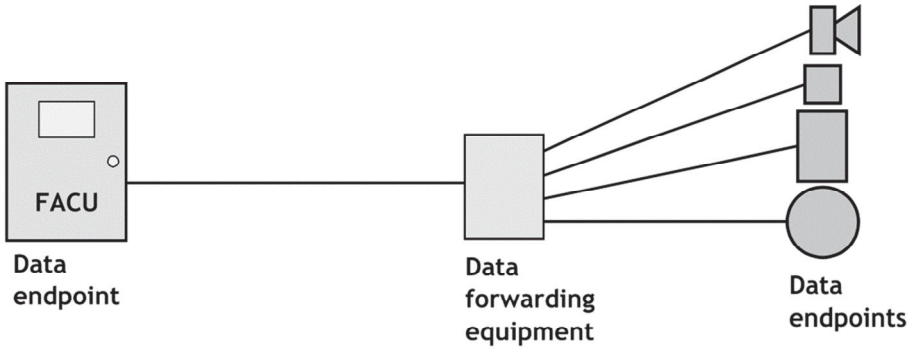
CLASS N HARDWARE

CLASS N DEVICES

When it comes to networking, most of your Ethernet equipment falls into two basic categories —endpoints and data forwarding equipment.

Class N devices are addressable intelligent network components that include input and output devices. Each addressable device is its own endpoint of communication with the system. Examples include:

- Alarm initiating devices, switches and sensors
- Addressable appliances
- Textual appliances
- Addressable amplifiers
- Visible appliances



It is important to understand a distinction between two types of hardware involved in a Class N network: Endpoint devices vs. data forwarding equipment. Data forwarding equipment does not originate data. It is considered part of the path between endpoints.

CLASS N NETWORK EQUIPMENT

Class N network equipment is used to forward packets of data to and from the endpoint devices. The data packets are verified, and retries are requested until the data is established as being valid or a timeout fault occurs. Network equipment is essential to the path, and is considered part of the pathway between devices.

Examples include:

- Routers
- Concentrators, like network switches, or hubs
- Repeaters

You'll need backup power for each network component, as well as for the endpoint devices.

GROUND-FAULT REPORTING

The most important concern in reporting a single connection to ground is the potential failure of the circuit if a second ground were to happen. Because classic SLC wiring could span an entire floor, or even an entire building, there's always a high probability for a second ground.

NFPA codes have required ground-fault reporting since the 1960's. Technology has obviously changed since then, but reporting a single connection to ground has long been considered a necessary function of fire alarm systems.

Ethernet, on the other hand, is designed to remain isolated from ground. Requirements of the Institute of Electrical and Electronics Engineers specify that each and every Ethernet connection isolate the connected cable from earth or chassis ground. In order for wiring to monitor for a connection to ground, it would necessarily have to connect to ground, at least for a moment. That would conflict with IEEE requirements.

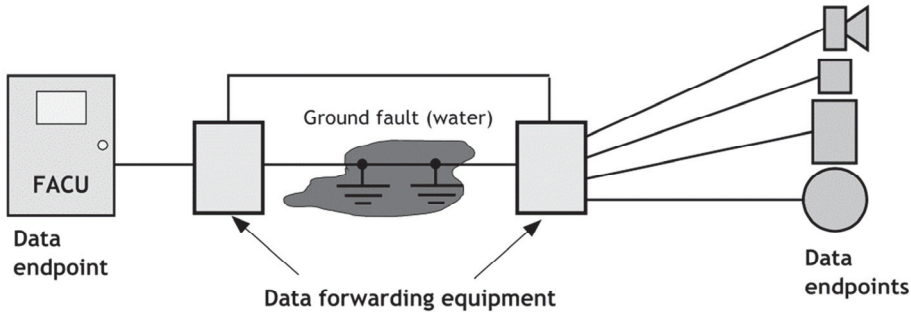
IEEE standards describe similar levels of isolation from ground to those required by independent testing laboratories, but manufacturers test their own equipment for compliance with IEEE. Independent testing laboratories test fire alarm equipment for compliance with NFPA 72 requirements.

How can you comply with both NFPA and IEEE? Just follow the new Class N requirements. Create a redundant backbone and monitor it to make sure it always has two paths. Then, you can have single drops to each device.

Class N does not need to report grounds, but as with all life safety paths, loss of communication must be reported. Make the same provisions you normally would for your life safety system or your high-priority communications network. Plan carefully, and appoint a life safety management group to oversee the implementation and ongoing health of the network.

RECOMMENDED METHODS

TWO GROUNDS ON ONE CABLE

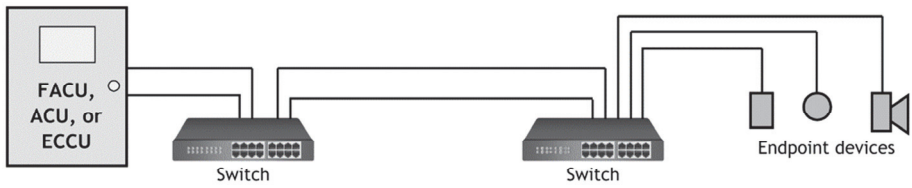


In Ethernet cabling, a ground connection on any one signal wire does not block communication, but two grounds on a matched pair within the same cable would.

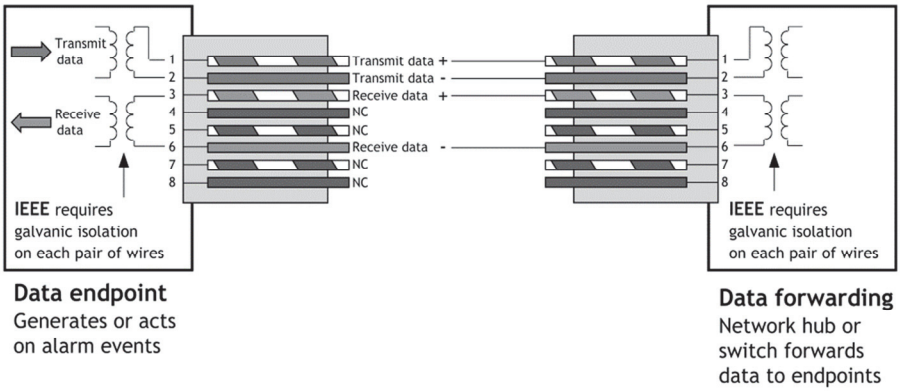
REDUNDANT BACKBONE PATHWAYS

In the field, Class N paths must be designed with redundant backbones — two or more path segments all the way to the final network drop to a single device. This compensates for the lack of ground-fault reporting that has been a fire alarm industry standard. Ethernet designers already plan redundancy into many networks. Life safety designers look for ways to ensure a fault in one path segment of a system won't affect other segments, and network designers must as well.

A SIMPLE CLASS N PATHWAY



ETHERNET CONNECTION



The Institute of Electrical and Electronics Engineers (IEEE) requires isolation at each end of every cable. Also, every data packet is checked for errors and re-transmitted until verified.

In an Ethernet network, the switches pass data packets through each cable segment. If a device is unplugged from one port of a switch and then plugged in to a port of another switch, the Ethernet design allows the route the data takes to change automatically. The technology is fault-tolerant because it adapts to network changes and reconfiguration.

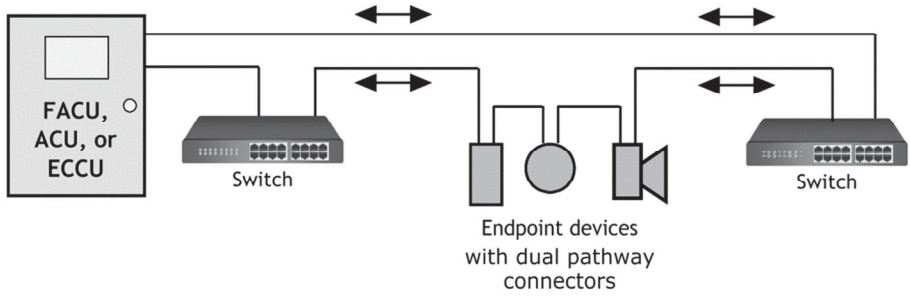
SEPARATE SUPERVISION

In addition, redundant pathways must be separately supervised. In other words: 1) they must exist as separate pathways so they'll continue to function if a primary pathway fails, and 2) a fault must be reported if two paths are not available.

It is a common practice in networking to pull two cables and connect them both to the same network component in hopes that one will cable will work if the other is compromised. That would be simple mesh networking.

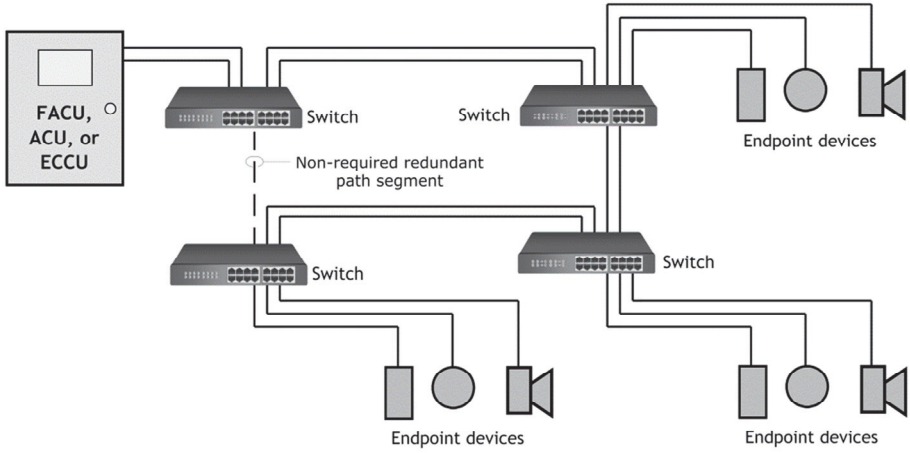
To meet Class N requirements, you'll need to have two separate, independent paths, and you'll need to monitor them both to make sure they're functional.

RING TOPOLOGY



A ring topology is allowed. It is one way to design two paths with an alternate if one path fails.

REDUNDANT PATHWAYS



Class N requires at least two separately monitored paths in the backbone. More paths are allowed, but the system must be able to report a fault if only one path is available — except for the single drop to a device.

SHARED NETWORKS

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.

You'll need to make sure that unauthorized people can't connect external equipment to your life safety network. NFPA 72 includes this cautionary warning:

> ***23.6. .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.*

Class N requires completely dedicated hardware and cables, unless you provide management and ongoing oversight.

Shared networks are defined by NFPA 72 as having 4 Levels, 0 through 3. (See NFPA 72, section 12.5, Shared Pathway Designations.)

Also from NFPA 72:

> ***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.*

LIFE SAFETY NETWORK MANAGEMENT

If you do choose to use a shared network, the planning and management of the life safety network must be well planned and all stakeholders must be involved. A management organization must be created to oversee the interests of the stakeholders. A documented design must be done before it is installed. Testing must be done, and a Change Control Plan must describe the procedures for when any future modifications are to be done to the network. Just like any fire alarm system during maintenance, any planned outages must be reported to anyone that depends on the information and operation of the network.

You can find the requirements for shared network management in the following sections of NFPA 72:

23.6.3.3 Deployment Plan.

23.6.3.4 Change Control Plan.

23.6.3.5 Management Organization.

23.6.3.6 Analysis.

23.6.3.7 Maintenance Plan.

SUPPLEMENTAL NETWORKS

When is Class N not required? For supplemental networks, where all Code requirements are met, but the owner wants to add monitoring capabilities for greater detail or for reporting.

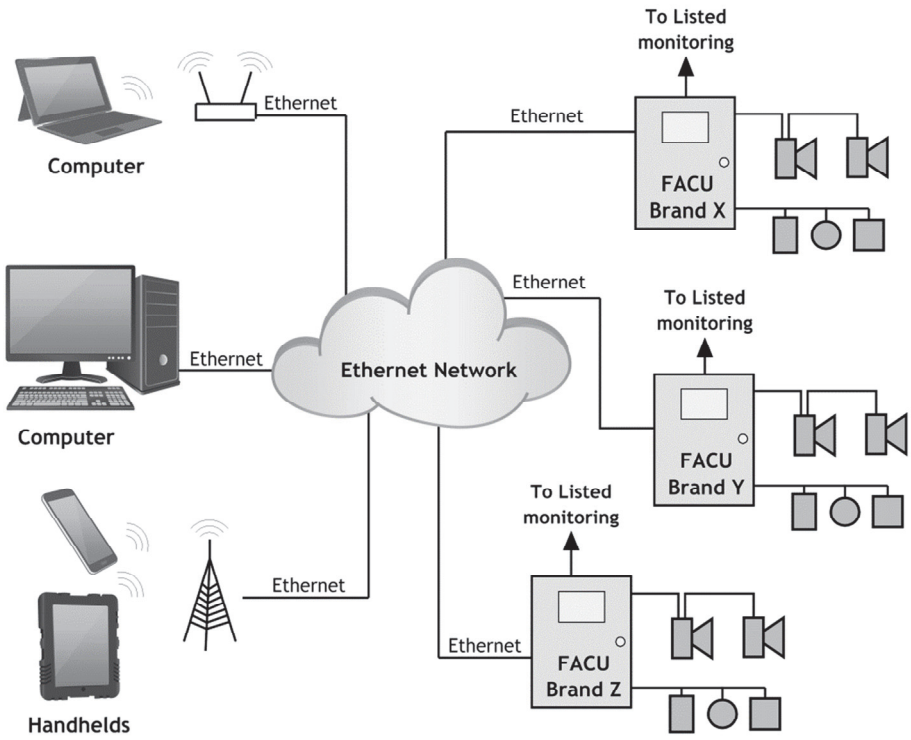
See NFPA 72, section 23.12.4, which was added in the 2010 Edition.

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

Also see the new *Figure A.23.12.4*, which was added in the 2016 edition.

The new drawing shows the difference between Class N and Ethernet networks that are used for supplemental purposes.

You'll notice that supplemental networks are not required to have a redundant backbone, or to report a connection to ground.



CONCLUSION

I hope this guide has helped you understand Class N requirements, so you can take full advantage of new technology in your alarm system.

After I gave a recent presentation on Class N, someone from one of the country's largest fire alarm manufacturers asked me, "Does this mean we should make an Ethernet-based smoke detector?"

I told him they should. The technology is available, it's economical, and it's mainstream.

I'll leave you with a story. I've been connecting computers to fire alarm systems for almost 30 years now. In my early days, I had a customer who owned 300 buildings. The owners wanted a separate fire-alarm display screen on every floor of every building. They also wanted flat screens mounted on the wall to replace the LED annunciator panels they were buying at the time.

Their budget was $5,000 per floor. (In 1987, that was more than in today's dollars.)

Unfortunately, an 8-inch flat panel screen cost $6,000. Today, you could get the same LED screen on clearance for $10.

That's good news for you though. The leaps and bounds we've made in computerization means that you can take advantage of some unbelievable opportunities for your fire and security systems.

Look around, and you'll see that you can find resources and information everywhere.

If you need help, give me a call or come see me in Florida. My phone number is 612-722-3233, and my email address is dan@cadgraphics.net.

— Dan Horon

RECOMMENDED RESOURCES

NFPA 72, Section 12.3.6 Class N, and associated Annex A12.3.6

NFPA 72, Section 12.5 Shared Pathway Designations

The National Fire Alarm and Signaling Code Handbook, 2016: *Supplement 3: Class N Circuits — Using Networks for Fire Alarm and Mass Notification Systems* by Dan Horon and Wayne Moore, P.E.

ABOUT THE AUTHOR

Dan Horon is the founder and president of Cadgraphics® Incorporated, and he's the inventor of RescueLogic® software — a graphical user interface for fire alarm systems.

Dan is a former fire protection engineer, and he's been developing his software for 30 years. Today, it's used to protect some of the world's most important facilities, including the U.S. Department of Homeland Security.

Dan has served on the NFPA Protected Premises Technical Committee since 2001. He was the chair of the NFPA Task Group on Circuits and Pathways when the chapter was added to NFPA 72. He is a member of the Technical Correlating Committee Task Group on Networks, and he co-authored the new networking section in the NFPA 72 handbook.

Dan has been a speaker and presenter at NFPA, NEMA, and other conferences. You can email him at dan@rescuelogic.com.

RESCUELOGIC SOFTWARE

For 29 years, Cadgraphics software has made it easy to monitor safety and security from your desktop. The software automatically imports data from alarm systems and monitors building control systems.

Cadgraphics' newest version, RescueLogic, integrates fully with the industry's most popular fire and security equipment.

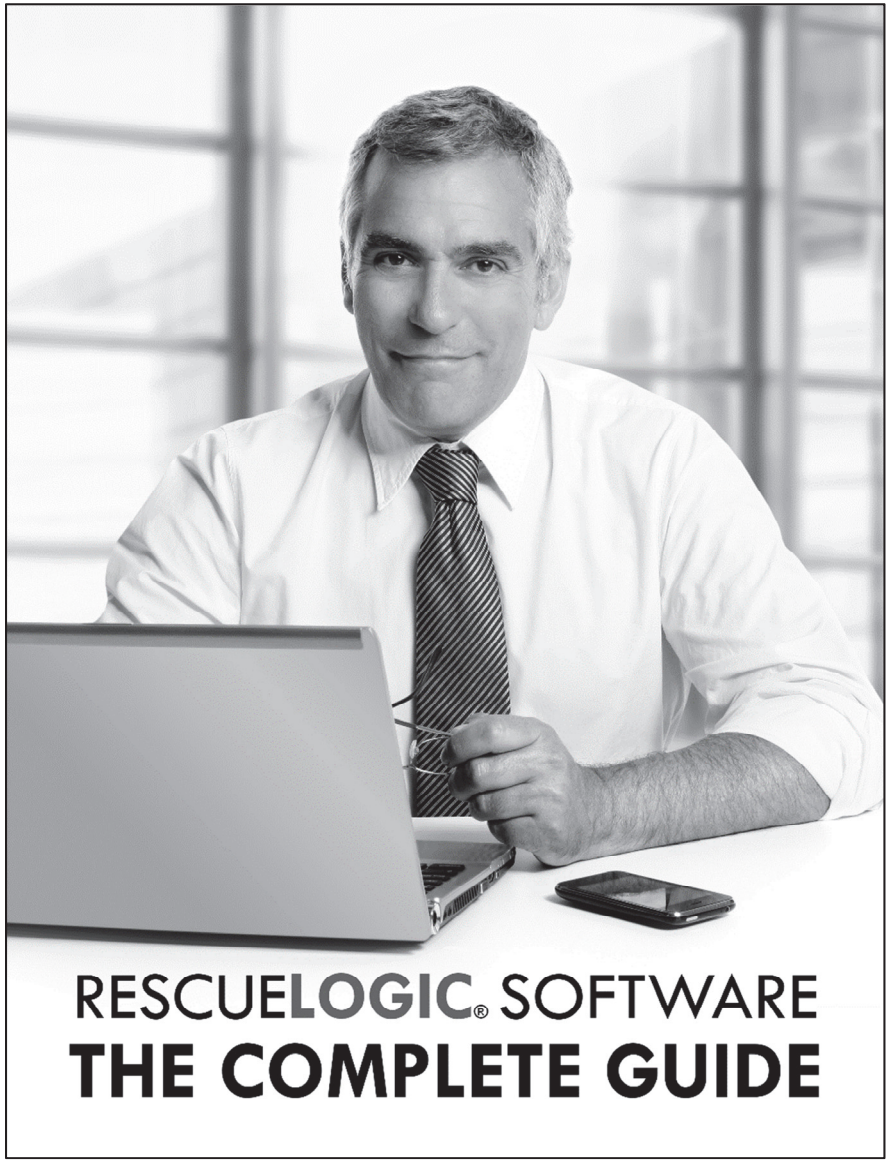
Learn more at rescuelogic.com.

OTHER GUIDES BY DAN HORON

Connections: The RescueLogic Guide to Configuring Ports and Panels
How to Configure a Moxa Device
RescueLogic Software Success Stories
RescueLogic Software: The Complete Guide
RescueLogic System Watch: A Handbook for Guards Dispatchers and First Responders
The RescueLogic Announcer Guide

Download PDF copies from RescueLogic.com
or buy printed copies and Kindle versions on Amazon.com

GET THE COMPLETE GUIDE



Available on Amazon and rescuelogic.com

CLASS N

NETWORKS

MAKE THE MOST OF TODAY'S
FIRE AND SECURITY TECHNOLOGY

AVAILABLE ON AMAZON.COM
AND RESCUELOGIC.COM