

Technical Bulletin

FireWatch™ IP Communicator & NFPA 72-2010

FLTB10-05-01

NFPA72 is the National Fire Alarm and Signaling Code, and it covers most facets of a fire alarm system including alarm reporting functions. Fire-Lite Alarms markets the FireWatch™ IP Communicator (catalog numbers IPDACT-2 and IPDACT-2UD) and Visoralarm™ IP Receiver which enables fire alarm reporting via the internet. The purpose of this document is to explain how these products can be deployed successfully in a code-compliant manner.

1. The IP Communicator - What it is, and is not

The IP Communicator allows fire alarm control panels to use any customer provided IP network connection as a communication path to transmit alarms to central stations. It offers performance & functionality enhancements over traditional communicators. It is designed to work with many of Honeywell's Contact ID/DACT equipped commercial fire alarm panels, as well as virtually all other fire panels through a slave dialer application. The IP Communicator allows faster and more economic alarm transmissions from the protected premises, improved response times to the Central Station; and decreased end-user operational costs. The IP Communicator was introduced over two years ago to positive customer reviews, has received an alarm industry award for innovation, and is today playing an integral role in protecting thousands of commercial installations every day.

The IP Communicator is UL listed, FDNY approved and CSFM listed for signal path communication with no backup phone lines required. The product falls under the "Other Technologies" section in 8.5.4 NFPA 72 2002 and 8.6.4 in NFPA 72 2007. In NFPA 72 2010 it falls under "Single Communications Technology" sections 26.6.3.1.1 and 26.3.1.4.1.

Though the IP Communicator is indeed a fire alarm communicator, it is not a "DACT" even though it has those letters in its catalog numbers. DACT's by definition in the Code connect to the public switched telephone network for communications. Traditional fire panel DACT's are considered in section 26.6.3.2 of the 2010 code and this section has no bearing on the use or installation of the IP Communicator or Visoralarm Receiver.

Technical Bulletin

The IP Communicator is not a DACT, though it does connect to an electronics package that has dual use. In its DACT application this electronics package (unfortunately called a DACT) performs the function of a DACT, and in its IP application this electronics package performs as part of the IP communication path. The IP communicator is not connected at any time to the public switched telephone network and makes no use of its path or its services. It's the name DACT that is causing an understanding problem. To clarify; in the IP configuration this electronics is not a DACT because it does not connect to the public switched network. Therefore section 26.6.3.2 does not apply. A parallel example can be seen with private radio. It uses the DACT electronics package as well, but the section 26.6.3.2 does not apply when a radio is being used.

2. Reliability of the IP Communicator

The Plain Old Telephone System (POTS) lines that we have come to rely on in the fire alarm business form a hub and spoke system. When you loose a spoke, communications is lost, and so is the message. The IP Communicator uses packetized communications to move data at extremely high speed. The packet is assembled at the start of its journey by the IP Communicator. The packet contains its origin address, its destination address, a "check sum" (more on this later) and the message or "payload". So, an IP message always "knows" where it is going and where it began, as it travels to its destination.

The World Wide Web is a true mesh network in that there are many paths between all origin and destination addresses. Messages traverse the network through an almost infinite combination of routes to arrive at the proper destination within a matter of a second or two. This mesh allows messages to route around all manner of obstacles, making the message transmission method more reliable than a POTS hub and spoke. Now once the message arrives it is taken apart and the "check sum" we talked about earlier contained in the message body allows the integrity of the message to be verified at the destination. This is a significant advantage over POTS.

Some people feel the outages experienced using the internet in their homes (when the system was in its infancy) means the internet is not reliable enough for fire alarm communications. First, the IP communicator doesn't use a PC-based operating system like your home. We have all grown to fear the common "blue screen" when PC operations cease to function, or even worse, the seemingly random "lock-ups" a PC user experiences with email or a web page. The IP Communicator does not use a PC so the most common form of computer network

Technical Bulletin

communications failure has been eliminated. Second, the IP Communicator just uses the internet communication path (really just the wire of the internet) and any routers in the path. Wire is subject to breaks, but no more than POTS wire. Routers are really miniature telephone digital switches and have similar reliability of POTS “central office” digital switches.

So the part of the internet used by the IP Communicator is no less reliable than POTS lines. With message integrity checks and more rapid notification it could be said that it's even more reliable.

3. Code Compliance for the IP Communicator

The IP Communicator meets or exceeds all requirements for a single communication line (no redundant phone lines required) under the 2002 edition of NFPA 72, section 8.5.4 and section 8.6.4 under the 2007 edition. Section 8.5.4 (from the 2002 edition) refers to communication Integrity. Note that although the numbered subsections have been incremented in the 2007 edition, the content has not changed.

There was however, a substantial change in the 2010 code, and allowance of alternative communications methods (such as the IP Communicator) was actually broadened. Chapter 23 titled “Protected Premises Fire Alarm Systems” states in 23.14 that transmission of alarm signals to continuously-attended supervising stations shall meet the requirements of Chapter 26.

In NFPA 72-2010, Chapter 26 speaks directly about alternative communications methods to the Digital Alarm Communicator Transmitter. Section 26.6.2.2 states that alternative communications methods are not prohibited as long as they provide a level of reliability and supervision consistent with the basic functions of a fire alarm system, and are listed. Under “Single Communications Technology” section 26.6.3.1.1 states communications methods operating on principles different than what's covered in the standard are permitted as long as they comply with the performance requirements of the section. Section 26.6.3.1.4.1 states a single communications technology needs to report within 5 minutes. The IP Communicator reports every 90 seconds.

The IP Communicator therefore meets all of the above requirements of a fire alarm remote communications system, and is Listed for this purpose, so the IP Communicator meets the requirements of NFPA72-2010.

4. So it meets NFPA72-2010, what else do I need to know?

As required by section 12.6.3.11, all on-premise communications equipment needs to be Listed. Also, secondary power is required in section 26.6.3.1.12 for the router/switch or whatever device is used to achieve Internet connectivity for the IP Communicator and Visoralarm Receiver. In practice, most commercial communications equipment is Listed, and many installations have their Internet gateway already powered by a UPS so these needs may already be in place.