NETWORKED FIRE DETECTION CONTROL AND INDICATING EQUIPMENT

> Prior to 2015 if AS 1670.1 talked about networks it meant the Telecommunications network, the Aspirated SD pipe network or the fire monitoring network.

AS1670.1 treated the connection of FIPs and SIPs in a similar way whether they were in one or multiple fire detection and alarm systems. Manufacturer's data sheets promoted the technical benefits of their product but there was little information on how they should operate.

In 2015 the first networking clauses were introduced focusing on how networks should operate with the actual details of what the physical connection would look like being handled by the transmission path (TP) requirements.

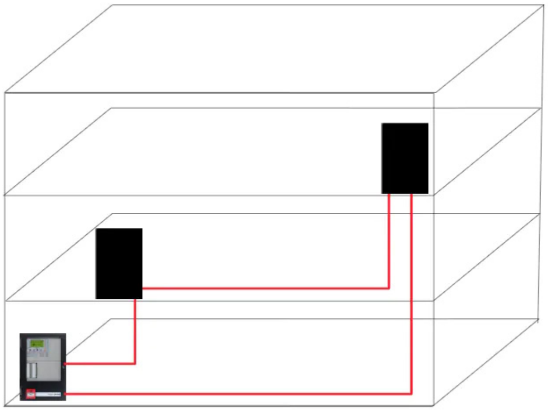
A new definition was introduced for networked fire detection control and indicating equipment (FDCIE)

NETWORKED FDCIE

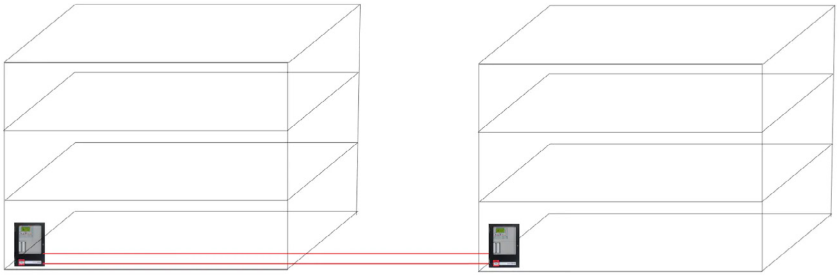
FDCIE WHICH RECEIVES OR TRANSMITS INFORMATION FROM OTHER FDCIE

This connection is still considered a Transmission path and subject to all the standard requirements as well as the additional requirements for networked FDCIE

For the first time, the standard differentiated between Distributed systems, where parts of the FDCIE are distributed within a single fire detection and alarm system (FDAS) and networked systems, where FDCIE across multiple FDAS are interconnected.



DISTRIBUTED SYSTEM



NETWORKED SYSTEM

The 2015 edition gathered the existing practices together in a dedicated clause without really imposing new requirements. However. there were some notable changes:

- Network applied to connections between FDCIE whether they were high or low-level TP.
- Applied uniform requirements to these connections which were re-classified as TP
- Required all networks to be fire rated
- Clarified that TP using fibre optic cable was acceptable
- Provided a means to achieve fire rating using fibre.

The 2018 edition introduced some important additional requirements on network operation. There are two important changes worth discussing.

1. An alarm on a network can only be reset or disabled on the main FDCIE or on the FDCIE on which it was initiated. Previously an alarm could be controlled from any FDCIE on the network which could present significant safety issues. The change was designed to force better network design and to reduce the annunciation of alarms on FDCIE which were not required to react to the alarm. This change may affect some manufacturers who can only configure full control on networked FDCIE.
2. A maximum 10 second delay period was introduced to apply to transferring alarms between FDCIE on a network. This delay includes the operation of any outputs such as AADs, VADs and smoke mode control. It is somewhat surprising that there was no defined requirement in previous editions of the standard which relied on the delay contained in the FDCIE product standard. Unfortunately, this did not apply across FDCIE in different FDAS. 10 seconds may appear generous, but it can be difficult to achieve if custom scripts are used and there are many existing installations which would struggle to meet this requirement.

To understand the detail requirements applying to networks I suggest you read up on transmission paths in AS 1670.1 because a network is simply a transmission path connecting FDCIE.

Hope you found this blog informative and a blog on Distributed CIE will be posted soon and I recommend that you read it.

For more information
www.notifier.com.au

Notifier by Honeywell
9 Columbia Way
Baulkham HIlls
NSW 2153

**THE
FUTURE
IS
WHAT
WE
MAKE IT**

Honeywell