TOP TIPS

Network Infrastructure Readiness For Physical Security Devices

SMART BUILDINGS TECHNOLOGY

TOP TIPS

Network Infrastructure Readiness For Physical Security Devices

Introduction

A broad set of physical security devices are being incorporated into smart buildings at an unprecedented rate. These devices must always be operational which can be a challenge as they are often deployed in harsh indoor and outdoor environments. Using a converged network infrastructure approach, devices such as security cameras, door controllers, and physical safety IoT sensors are connecting to IP networks via wired Ethernet in enterprise settings. The problem, however, is that existing or newly installed twisted pair copper cabling does not meet best-practice guidelines for a host of reasons. This can lead to situations where these devices become unusable or unreliable, defeating the purpose of the technology and potentially endangering building occupants.

Let's look at five reasons why infrastructure readiness for physical security is so important and how proper cable specification types, power-sourcing verification and endpoint testing becomes a critical part of any smart building security/safety device install.

Use of Older Cabling That Does Not Meet Modern Specification

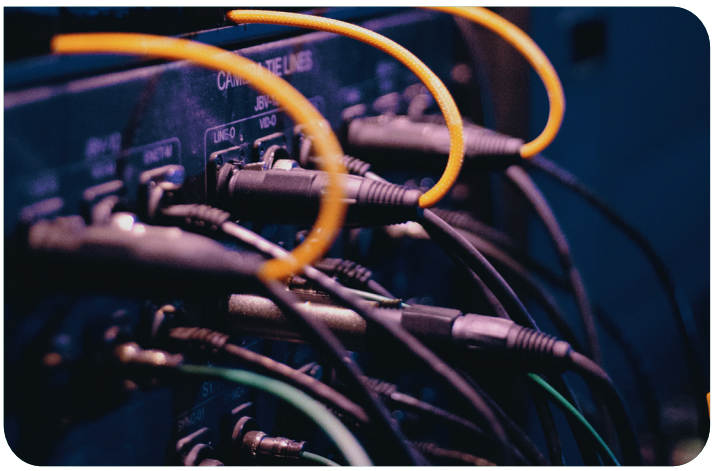
In buildings that are a decade or older, the existing copper plant often consists of a mixture of Category 5e and 6 cabling. While these cable specification types may have been sufficient for transporting Ethernet frames at up to gigabit speeds and power over Ethernet (PoE) up to 30 Watts it's not up to the task when multi-gigabit transport and high-power PoE is required. While this cabling may seemingly operate at these higher levels for a short period of time, the cabling will likely fail at the most inopportune times, causing significant problems to a smart building's physical safety posture.

Power Over Ethernet Sourcing Shortcomings

Physical security devices including ultra-high-definition (UHD) and pan/tilt/zoom (PTZ) cameras push the capabilities of power delivery over copper cabling far beyond traditional PoE devices. In some instances, problems can occur with PoE delivery of these devices that can either shutdown the physical security device – or significantly degrade their capabilities. Troubleshooting these types of problems without the proper test equipment can be time consuming as the problems can be related to many different factors including the cabling itself, the power sourcing equipment (PSE) or the endpoint.

Exceeding Cable Distance Limitations

Smart building security devices and IoT sensors often stretch physical cabling distance limitations. Because security cameras and sensors are deployed at entryways, rooftops and parking areas, cable installers sometimes must extend cable runs to their maximum. This in turn can cause intermediary issues when transporting Ethernet frames or when attempting to deliver PoE to far-off endpoints.



DC Resistance Unbalance

Another issue with deploying security devices that require higher-wattage power delivery resides in the fact that for Ethernet and Power to coexist in the same cable pairs, these pairs must be nearly equal in resistance values to avoid problems with power delivery and disruption of data flow. If the resistance between pairs and between conductors within a pair is not within tolerance specified by the standards, this is known as DC resistance unbalance which can result in insufficient power delivery to the powered device, transformer saturation and data disruption as well as EMI issues for nearby cables. This is becoming increasingly common now that PoE is being used more frequently and with devices that require up to 90 Watts of power to operate. While higher quality and specially shielded cabling does help, DC resistance unbalance should be tested as a measure of pre-deployment assurance, that the cabling should be able to support PoE running alongside data within the same cable.

TCL and ELTCL Tests

Because Ethernet requires a balanced electrical signal to transmit data reliably from one end of a twisted pair cable to the other, a verification of both transverse conversion loss (TCL) and equal level transverse conversion transfer loss (ELTCL) is often necessary. Keep in mind, however, that even when cables are tested using a cable certification test kit, both TCL and ELTCL are optional tests and must be enabled manually. When these tests are included as part of the cable certification process, however, it tests against external electromagnetic interference to be sure that external noise on transport pairs will not disrupt the electromagnetic balance required to successfully transport data.

For more information, contact us at:

US Headquarters
AEM International (US)
5560 West Chandler Blvd, Suite 3
Chandler, AZ 85226
Toll Free: 833-572-6916 | 480-534-1232

Global Headquarters
AEM Singapore Pte. Ltd.
52 Serangoon North Ave. 4
Singapore 555853
T : +65 6483 1811 | F: +65 6483 1822