Physical Infrastructure Planning for Electronic Safety and Security Systems

Today's communications infrastructure is an ever-changing landscape as more previously proprietary and disparate applications, such as security cameras and access control devices, referred to as ESS (Electronic Safety and Security) systems, are attached to a common network. More like an IP "explosion" than "convergence," this creates challenges for IT professionals who must plan physical infrastructures that can expand exponentially in bandwidth and physical equipment. Planning for telecommunications rooms (TRs) includes upgrading hardware such as servers, switches, patch panels, and cable management racks. Smart IT professionals are working with security experts to understand these new applications and infrastructure requirements. And security professionals are learning network requirements and the value of a well-planned structured cabling system.

Security systems rely on mission-critical life safety information in real time. The first step is deployment of a reliable common structured cabling layout for all ESS devices to assure that, even if they are not IP-enabled today, they can easily be converted to a network-attached system later on. A common infrastructure offers significant savings compared with separate traditional systems. As devices become "edge devices," also known as "smart devices," these previously separate systems will become integrated on the same network to communicate directly with the device through a common user protocol.

Cabling choices for security and surveillance systems

IP, digital video, and networking have ushered in new cable media for transporting images and data from the device to the end user through the communications infrastructure. Where once analog cameras solely were connected with coax cable, today both analog and IP cameras use high-speed Ethernet twisted-pair cabling and fiber optic, known as structured cabling. What are the advantages of these cabling choices?

The selection of unshielded twisted-pair (UTP) or fiber is based on several factors, including:

- Location of the camera (indoors or outdoors).
- Distance from the termination equipment to the device.

>> BY CAROL EVERETT OLIVER, RCDD, ESS, BERK-TEK, A NEXANS COMPANY

- Diameter of the cable.
- Power and bandwidth requirements.
- Cost.

Twisted-pair cabling is the most cost-effective. It allows power over Ethernet (PoE) through the spare pairs and delivers power through midspan injectors or an endspan (powered switch). Twisted-pair cabling has a distance limitation of 100 meters for Ethernet, so location of the camera and distance from TRs and termination equipment need to be factored into the cabling selection. Twisted-pair cable types and bandwidth capacities are category 5e (100 MHz), category 6 (250 MHz), and category 6A (500 MHz). Depending on the type of security camera and the life expectancy of the surveillance system, the highest grade of category cable is recommended for the longest span of network usage and to avoid recabling in the near future.

Fiber optic cable offers longer distances, temperature stability, highest bandwidth, and longest service life. It is impervious to EMI, RFI, or crosstalk. And, although fiber cable is economical, the active equipment increases its cost above that of copper. Fiber cannot transmit power, but PoE is possible over a copper/fiber composite cable and through powered media converters.

Standardization to the rescue

In the structured cabling world, industry standards provide guidelines for media selection and installation practices based on cable type and associated electrical characteristics. Existing standards, such as the ANSI/TIA-568-C series, were written for generic, primarily data and voice applications for office environments. But what about instances in which the environment and application define the work area and termination?

Help is on the way for IT system designers and installers, as well as security integrators, through a new standards committee that has emerged from BICSI, a professional information technology systems/telecommunications association. Working with the American National Standards Institute, this committee has researched standards development activities of organizations such as SIA, ASIS International, NFPA, and IEEE to ensure there are no conflicts and that similar standardization work is not in progress. The new standard, upon proposed completion in late 2011, will be designated ANSI/BICSI 005: Electronic Safety and Security System Design and Implementation Best Practices. It will provide guidelines for media selection, pathways, and installation specific to each ESS application, as well as guidance on topics such as meeting the IP needs of fire detection and alarm systems.

Given how fast convergence is progressing, network infrastructure standards are vital. They also will make it easier for all the devices finding their way to the network to co-exist in a scalable network.

Carol Everett Oliver serves on the BICSI ESS Standards Committee as a co-chair and also as a chapter leader. She can be reached at carol.oliver@nexans.com. Learn more about BICSI at www.bicsi.org.

"Factors to consider when selecting unshielded twisted-pair (UTP) or fiber include camera location, distance from the termination equipment to the device, cable diameter, power requirements, and, of course, cost."

>> **TRANSPARENT CLUSTER USED FOR SECURITY CABLING.** *PHOTO COURTESY BERK-TEK, A NEXANS CO.*