Specialty Systems Installation

Introduction

Unlike information and communications technology (ICT) systems infrastructure that supports traditional voice and data networks, specialty systems support varying aspects of the occupancy, usage, and supporting infrastructure of a building or premises. Traditionally, many of these specialty systems were proprietary to a specific manufacturer. Today's specialty systems incorporate a number of standards that enable the use of a common ICT infrastructure and an increased ability to integrate with other systems.

In addition to providing general specialty system information and installation guidelines, this chapter also covers security and wireless systems.

While other specialty systems (e.g., building automation, digital signage and wayfinding, asset tracking) are increasing in deployment and use, these systems share many common elements and design practices as applied to the ICT infrastructure.

Many specialty systems can have specific licensing requirements and should be verified with the authority having jurisdiction (AHJ). Follow manufacturer's installation guidelines and BICSI® best practices in all installation activities.

Structured Cabling Differences for Specialty Systems

Overview

Because specialty systems may originate from a different industry or trade (e.g., building automation system [BAS] from the building heating, ventilation, and air-conditioning [HVAC] system), they may have differences compared with a structured cabling system (SCS). These differences include:

- Allowed topologies.
- Different cabling and termination practices.
- Code and AHJ requirements (e.g., conductor temperatures, cabling separation) for the safe implementation and function of the system.
- Use of industry standards not normally associated with ICT (e.g., ASHRAE 13, NFPA 72).

Topologies

Unlike the voice and data work area, specialty system cabling infrastructure allows different coverage area topologies, which means that the coverage area may be extended to connect multiple devices on the same horizontal cable run (e.g., chained, bridge connection, multipoint branch [bus or ring]).

Horizontal Connection Point (HCP)

A horizontal connection point (HCP) is to specialty cabling what a consolidation point is to voice and data cabling. An HCP allows coverage area connections to be reconfigured (e.g., bridged, chained, added, removed). No more than one HCP should be placed in a single horizontal cabling link—an outlet typically is not needed when using an HCP.

NOTE: When cross-connections are used at the HCP, an outlet/connector should not be installed as part of the horizontal cabling link. This requirement ensures that the horizontal channel contains no more than four connections.

An HCP should be readily accessible and its location visibly marked allowing for ease of routine maintenance and reconfiguration. HCPs should be located in fully accessible, permanent locations and not in obstructed areas. Administration for HCPs should be handled in the same manner as telecommunications cabling, hardware, pathways, and spaces.

NOTE: For balanced twisted-pair cabling, the HCP should be located at least ≈15 meters [m (50 feet [ft])] from the telecommunications room (TR). This is designed to reduce the effect that multiple connections in close proximity can have on near-end crosstalk loss or return loss.

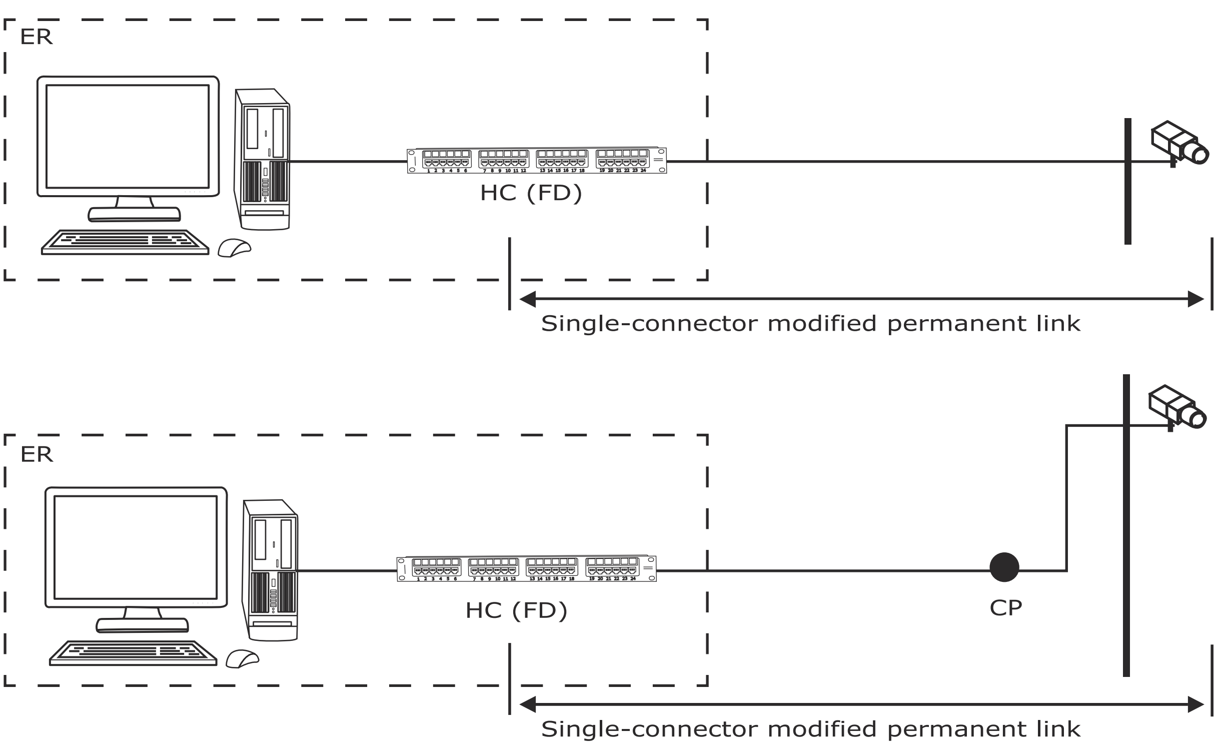
Modified Permanent Links (Direct Attach)

The single-connector modified permanent link model (see Figure 9.1), also known as direct attach, represents a set of scenarios where the cabling link attaches directly to electronic safety and security (ESS) field devices, BAS controllers and sensors, security cameras, and wireless access points (WAPs).

In such scenarios, the installation of a telecommunications outlet/connector is not feasible and may not be allowed because of safety/security concerns. In the single-connector modified permanent link model, the device side of the horizontal cabling is terminated by an 8-position, 8-contact (8P8C) modular plug or optical fiber connector and attached directly to the field device. Where balanced twisted-pair cable is used, solid conductor cabling typically is specified.

It is recommended to provide appropriate cable slack for the devices in order to relocate a connected device.

Figure 9.1
Examples of single-connector modified permanent links


ER
HC (FD)
Single-connector modified permanent link
ER
HC (FD)
CP
Single-connector modified permanent link

CP = Consolidation point
ER = Equipment room
HC (FD) = Horizontal cross-connect (floor distributor)

Terminations and Connectors

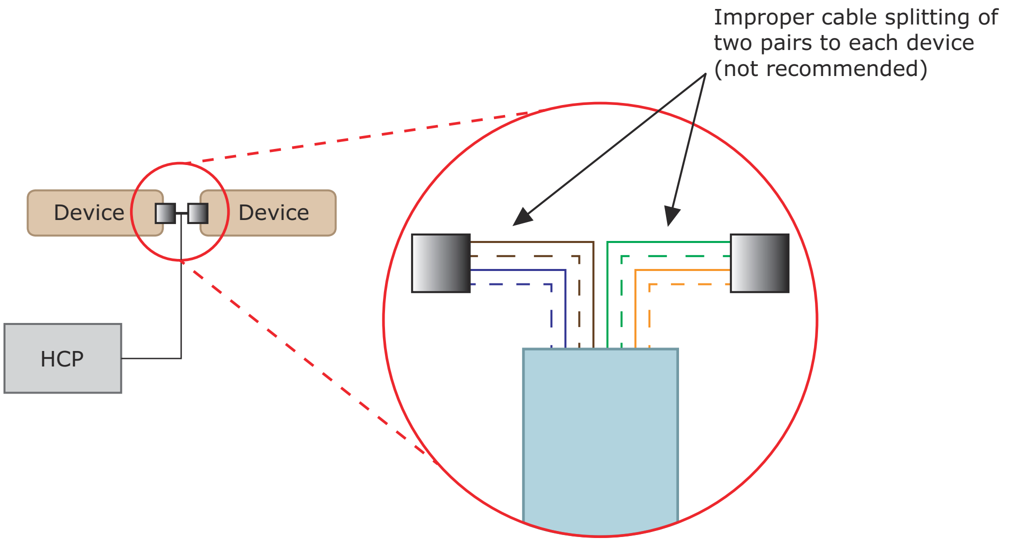
Many specialty systems use the common connectors (e.g., modular plug/jack, LC optical fiber connector) found within SCS. However, an ICT systems cabling installer may find other types of connectors and termination strategies in use. Many of these strategies utilize balanced twisted-pair cable as the connective media for a non-standardized ICT termination.

The most common example of a non-standardized ICT termination is the splitting of the pairs within one balanced twisted-pair cable between two or more devices (see Figure 9.2). While the system may perform as expected, this is not a recommended practice as splitting pairs:

- May not comply with code or AHJ requirements.
- Prevents the proper testing and certification of cabling performance.
- Increases the difficulty in troubleshooting link cabling performance issues.
- Reduces options when upgrading equipment.
- Increases the work required for moves, adds, and changes.
- Often invalidates cable warranties.

When installing new systems and replacing existing cabling, the splitting of pairs should be avoided and only performed if the system manufacturer requires the practice.

Figure 9.2
Example of improper ICT termination



Improper cable splitting of two pairs to each device (not recommended)

HCP = Horizontal connection point

Hybrid Cabling

Some specialty systems may utilize common ICT cables (e.g., balanced twisted-pair, optical fiber), while others utilize hybrid cables. A hybrid cable contains two or more different transmission media within a common cable sheath or jacket. Examples of different transmission media within a common sheath include:

- Different types of balanced twisted-pair cable (e.g., category 5e and 6A).
- Different multimode classes of optical fiber (e.g., OM3, OM4).
- A balanced twisted-pair cable and a coaxial cable.
- Different styles of optical fiber cable (e.g., tight buffered, ribbon).
- Optical fiber cable and balanced twisted-pair cable.
- Optical fiber cable and copper conductors (stranded or solid core conductor used for electrical power transmission).

Power over Ethernet (PoE)

Power over Ethernet (PoE) technology allows network PoE-enabled devices to draw power from the same generic cabling used for data transmission. This concept traditionally applies to WAPs, webcams, video cameras, and Internet protocol (IP) telephones, but the number of devices using PoE increases as new technologies are developed.

Combining power and data onto a single cable provides many benefits, including:

- Eliminating the need to provide power outlets at the same location.
- Ability to detect loss of power to device.
- In the event of a power failure, the network backup power system can service PoE devices and systems, as well as other network devices.

Power Source

Power source equipment may deliver direct current (dc) power over the two unused pairs in 10BASE-T or 100BASE-TX (e.g., pins 4-5, pins 7-8). Alternatively, the standard allows for delivering power over the signal pairs (e.g., pins 1-2, pins 3-6) directly through switch ports.

Standard PoE-powered devices are designed to accept power over both options, whichever is being used by the power source. The maximum source power output level is 15.4 watts (W) at 44 to 57 volts (V [nominally 48 V]). PoE + devices provide up to 25.5 W at 50 to 57 V.

Three practical power source options for PoE are available:

- PoE switches can be used to provide power to PoE devices via the cabling system.
- Midspan devices are installed between a non-PoE switch and the PoE device to add a dc signal to the data signal, allowing the existing network to power up the PoE device. The advantage of midspan devices is that they offer power to PoE devices using legacy switches.
- A growing minimum standard in the networking industry is to install PoE capable switches as a basic standard. Thus, if devices are added in the future, they will be able to accommodate PoE capabilities.

NOTE: Follow manufacturer's instructions when installing PoE power source equipment.

Security Systems

Overview

Three major areas in security may be part of an installer's work:

- Intrusion detection system (IDS)
- Access control system (ACS)
- Video surveillance system (VSS)

Intrusion Detection System (IDS)

An IDS can be a standalone system, generating simple local or paging alarms. An IDS also can be integrated with other systems such as an ACS to provide more active responses (e.g., turning on cameras, lighting).

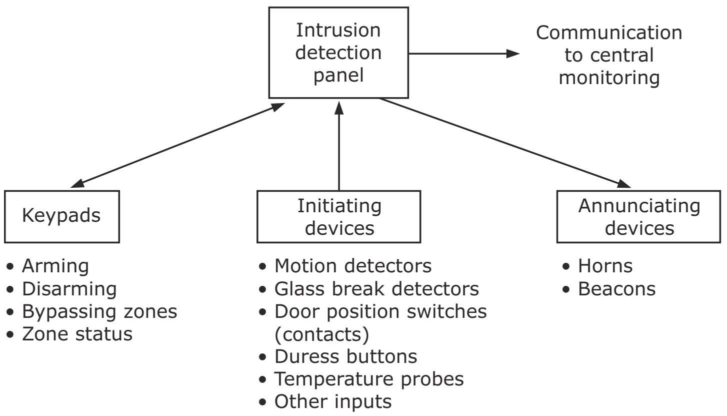
Purpose and Characteristics of Devices

An IDS generally detects unauthorized entry into a protected area. Its methodology of operation is to detect an intrusion and provide some form of notification that a breach has occurred in the area under protection (see Figure 9.3).

An IDS is an integration of the following components and devices:

- Detection sensors—Devices that monitor and detect forced and unauthorized entry into a protected area, including:
  - Door contacts
  - Window contacts
  - Motion detectors
- Processor controllers—Systems that receive and process outputs from connected sensors and use predefined parameters to generate alerts based on the information received from each sensor.
- Notification console—Devices that monitor events and system alerts that operators can use to make informed decisions as to the operational status of the entire system.
- Power source—Low-voltage transformer and backup batteries.

Figure 9.3
Logical intrusion detection system (IDS) diagram



Intrusion Detection System (IDS), continued

Installation Guidelines

The guidelines to consider when installing an IDS are:

- Perform a site survey of all areas of installation.
- Verify that the installation matches the installation drawings and manufacturer’s guidelines.
- Verify that signal and power wires are routed in conduit or cable tray as specified.
- Verify proper power levels (voltage and amperage).
- Verify correct wire connections.
- Verify wireless system functionality, if present within the system.

Process controllers (control panel) installation guidelines shall be as follows:

- Ensure that the room housing the control panel is a secured location.
- Ensure that there is backup power or batteries are properly connected to the control panel.
- Perform a systems test once all devices are installed.

Access Control System (ACS)

Access control is the process by which access to an asset or location can be limited to those individuals expressly authorized for its use. Access control is important for overall personal safety and the protection of physical and intellectual property.

Purpose and Characteristics of Devices

Access control devices can include entry point locks, integrated electronic devices controlling a single door or room, or a complex system of interconnected electronic devices controlling a zone, building, or campus.

The basic components of an ACS include the following:

- Computer
- One or more control panels
- Peripheral devices:
  - Sirens
  - Locks
  - Access cards
  - Card readers
  - Motion sensors
  - Turnstiles
  - Security gates

Access Control System (ACS), continued

Installation Guidelines

The installer will normally be responsible for the installation of control panels and peripheral devices.

When installing an ACS:

- Perform a site survey of all areas of installation.
- Verify that the installation matches the installation drawings and manufacturer's guidelines.
- Securely mount all control panels and peripheral devices.
- Verify installation of tamper prevention methods (e.g., receptacles, enclosures) per design specifications.
- Verify correct wire connections.
- Verify wireless system functionality, if present within the system.

When installing a control panel:

- Ensure that the room housing the control panel is a secured location.
- Ensure that there is backup power or batteries are properly connected to the control panel.
- Perform a systems test once all devices are installed.

When installing peripheral devices, adhere to manufacturer's instructions and owner's guidelines.

Video Surveillance System (VSS)

Video surveillance is a widely used technology within ESS systems and involves the use of cameras for monitoring and controlling assets. Video surveillance is the process of image:

- Capturing
- Transmitting
- Processing
- Viewing
- Recording

This technology requires knowledge of cameras and their installation, image transmission, and recording principles.

Video Surveillance System (VSS), continued

Purpose and Characteristics of Devices

Video surveillance is the extension of human vision to areas requiring surveillance. A VSS can be both analog and digital IP in nature.

The components of a VSS include the following:

- Cameras
- Transmission media:
  - Balanced twisted-pair cable
  - Optical fiber cable
  - Wireless
- Connectors:
  - RS232
  - 8P8C
  - Optical fiber cable connectors
- Processors
- Recorders
- Monitoring and control devices

Installation Guidelines

When installing a VSS, the installer will normally be responsible for the installation of security cameras and their supporting cabling and connectors. The guidelines to consider when installing a VSS include:

- Perform a site survey of all areas of installation.
- Verify that the installation matches the installation drawings and manufacturer’s guidelines.
- Ensure that each camera has the proper mounting material and the mount can handle the camera’s weight.
- Ensure that each camera is properly connected to the provided power source.
- Perform a systems test once all devices are installed.

When installing the supporting cabling and connectors, adhere to the manufacturer’s instructions and owner’s guidelines.

Wireless Systems

Overview

This section provides an overview of wireless systems and the materials and installation practices necessary to support a wireless LAN (WLAN) infrastructure and a distributed antenna system (DAS). The WLAN is an extension of a facility's data network, and a DAS is typically deployed into areas where cellular or other radio frequencies cannot reach or may interfere with existing devices.

Wireless Signals

While wireless systems can support a multitude of signal types, the most common wireless signals within ICT include:

- Cellular—This refers to the range of bandwidths used within mobile communications. Frequency ranges vary, depending on the transmission technology and encoding being used, but typically are between 700 megahertz (MHz) and 2700 MHz.
- WLAN—Commonly termed Wi-Fi, WLAN signals and protocols are defined by IEEE 802.11 and operate in the 2.4 gigahertz (GHz), 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands.
- Microwave—A term that typically is applied to point-to-point (PTP) systems that are licensed and operate within parts of the radio spectrum designated by the Federal Communications Commission (FCC), such as:
  - 4.9 GHz (public safety)
  - 6 GHz
  - 11 GHz
  - 18 GHz
  - 23 GHz
  - 80 GHz (E-Band millimeter [mm] wave).
- Land mobile radio (LMR)—LMR systems are used by emergency first responder organizations, public works organizations, companies with large vehicle fleets, campus or regional security staff, maintenance and operation crews, construction workers, and the military, among others. LMRs use defined sets of frequency bands between 30 to 50 MHz and 150 MHz to 900 MHz.

Wireless System Types

There are generally three types of wireless systems:

- PTP
- Point-to-multipoint
- Mesh

PTP systems connect two locations together through line-of-sight, operating in unlicensed/licensed radio frequencies or through free space optics, and are typically used for higher-powered systems or for long-range transmission of radio signals. A PTP can also be used for building-to-building connectivity.

Wireless System Types, continued

Point-to-multipoint systems are primarily used for wireless Internet and IP telephony that have a large number of nodes, end destinations, or end users. They are usually lower in power and used for in-building applications, although some high-powered systems incorporate a point-to-multipoint architecture when simulcasting radio signals to multiple antenna locations.

Mesh wireless networks are comprised of radio nodes organized in a mesh topology and are a form of a wireless ad hoc network. As connected objects may serve as nodes, a wireless mesh system can provide the ability to send and receive data to other connected objects without need of an Internet connection.

For the ICT installer, the most commonly encountered wireless systems are point-to-multipoint systems in the form of a WLAN or DAS.

Wireless LAN (WLAN)

WLAN connections replace the cabling used to link stations and shared peripherals to one or more LANs in diverse environments, including:

- Offices.
- Residential units.
- Public sites (e.g., schools, hospitals, airports).
- Retail and industrial sites (e.g., stores, warehouses, manufacturing plants).

In general, WLANs are used to provide flexibility and mobility to groups of users within a common area. A WLAN enables connection to a network from any location in the zone covered by a wireless network access point (AP).

One or more APs can be used to provide a standalone WLAN environment to users. Alternatively, APs can be connected to existing cabled networks and servers as wireless extensions in a hybrid environment.

Distributed Antenna System (DAS)

A DAS consists of an infrastructure of electronic devices, including:

- Amplifiers

  NOTE: Amplifiers typically are labeled as Node A or Node B devices.
- Cabling
- Connectors
- Antennas

A DAS retransmits and receives frequencies within a building or complex by means of antennas that are distributed throughout to provide even and usable coverage (see Figure 9.4). One or more DASs are typically used in large venues (e.g., arenas, airports, multi-story buildings) or locations with inadequate radio reception (e.g., mines, underground transit).