How smart infrastructure can become dangerously dumb

Get smart about connectivity choices by being "in the know" about cable hazards that impact lives.

BY TIM COPP and **CAROL EVERETT OLIVER,**

Communications Cable and Connectivity Association

Cable and connectivity are the necessary, basic building blocks and foundation for transmitting and receiving all communications. Cable connects everyone to everything through the wired and wireless network infrastructure—from healthcare and educational institutions to conferencing, entertainment and social media. The 2020 pandemic taught us, or reinforced for us, that the internet is a required utility and priority number one for dependable communications. Every bit of data that is stored in the cloud—i.e. in a data center—cannot be secure or functional without a robust cabling system.

If the internet is the common bond that keeps everyone and everything connected, then the cable is the glue. Moving forward into the next generation of the Internet of Things (IoT), artificial intelligence (AI), 5G and smart cities/building applications, reliable data transmission in real time becomes critical to how modern society functions. This data transmission, which was once simply a means of communication, is evolving into a core necessity, relying solely on the infrastructure and the sum of its parts.

The evolution and growth of applications and new technologies are driving the need for high-performance and high-value cable, a crucial infrastructure necessity that is often overlooked or thought of as a commodity. Today's critical applications require 100% reliability and ever-higher data transmission rates over this new cable, now with the added duty of supporting Power over Ethernet, which is also coined "Power over Everything," in smart building applications. Pushing power over the same conductors as data can also increase heat within the cable, potentially causing signal degradation and a fire hazard if inferior cabling is installed.

Poor-quality cable and installation practices are often not a priority or much of a concern to building owners and end users until a system goes down. Because cable infrastructure is installed behind the walls and out of sight, few people give a second thought to the criticality of cabling infrastructure until it is too late. And don't

This image, taken from video footage of a test conducted at a nationally recognized test laboratory, shows flame spreading through a plenum space, fueled by cable that is not plenum-rated.

forget, wireless devices are in fact connected by wires to transmitters and routers. It is generally accepted that approximately 70% of network downtime is due to cabling improprieties, which can include low-quality cable or poor termination practices. But, even worse than network failure is the safety risk due to a cable's poor design, substandard material makeup and/or manufacturing deficiencies.

Cables produced using deficient manufacturing processes and substandard materials pose a serious safety risk. Without oversight and proper construction, inferior cables running throughout a structure can act as fuses that accelerate the spread of fumes, flames and smoke. This can potentially lead to a significant reduction in evacuation capability, loss of life and a serious destruction of equipment and structures. When substandard cabling is bought and installed, who's to blame and what's the recourse? Action and awareness is crucial now to avoid future catastrophic events.

The Communications Cable and Connectivity Association (CCCA) continues to educate installers, contractors and other ICT professionals on key issues affecting the structured cabling industry. As a result, there are many programs and methods to discern good cabling from bad. Recently this awareness has resulted in legislative actions and law-enforcement initiatives.

Wolf in sheep's clothing

Reputable cable manufacturers design and produce products to yield the highest performance while meeting specific safety requirements. These products go through rigorous testing scrutiny to be independently certified and then are classified as intellectual property owned by the manufacturer. All communications cables, such as Category 5e or Category 6, may look the same on the surface, but unless buyers take a closer look at the construction and materials of the cable or investigate their specific certifications, disastrous outcomes are possible. Unscrupulous manufacturers looking to take advantage of the perception that communications cables are a commodity—and all look the same to the average consumer—employ cost-cutting measures that pose serious threats to safety and performance. These violators produce counterfeit cables and mislead buyers, putting the entire ICT industry and all consumers at risk.

There are several important criteria used to differentiate and classify communications cables. These include the National Fire Protection Association *National Electrical Code* (NFPA 70/NEC), industry performance standards such as ANSI/TIA-568.2-D Balanced Twisted-Pair Telecommunications Cabling and Components, and UL 444 Standard for Safety – Communications Cable.

When adopted by a state or local municipality, the *NEC* becomes law and carries the power of enforcement. The *NEC* is updated every three years. The most recent edition states that each communications cable must comply with Chapter 8 in meeting applicable flame and smoke testing to earn the rating of CMP (plenum), CMR (riser), or CM (general purpose). In doing so, cable is required to be tested and certified ("listed") by a designated third party independent nationally recognized testing laboratory (NRTL) such as Underwriters Laboratories or Intertek.

CMP plenum-rated cables, for example, are specifically designed to meet the demanding fire/life safety requirements outlined under the NFPA 90A/NFPA 75 standards and mandated by the *NEC*. Plenum cables, which are allowed to be safely installed in a building's air-handling spaces above ceilings or below floors, are more expensive to manufacture than CMR or CM cables because of their unique component materials and design configurations.

Plenum cables that carry the CMP listing on the box typically are manufactured with fire-retardant compounds, such as low-smoke polyvinyl chloride (LSFR PVC), fluorinated polymers, or other specific materials designed to minimize ignition and reduce flame spread and smoke generation.

Unfortunately, some manufacturers are marking their cables as being plenum rated when in fact the cables are not officially listed. Unless a cable has been tested and certified by an NRTL as CMP, it is not permitted to bear the CMP mark. Any cable that does this—marks a cable as CMP without first having passed the stringent testing required to mark it as such—is using a counterfeit listing mark. Because the listing marks are included in a simple text string on the cable jacket, these substandard and mismarked cables can go undetected through the supply chain. In some cases, installed cables that do not meet the NEC requirements have acted like a fuse, spreading large fires, often undetected through enclosed spaces in properties including hotels and commercial businesses. These examples prove that installing non-compliant or counterfeit cable in a plenum space can be costly both in lost lives and the destruction of property.

Covert indicators

Sometimes it can be very difficult to discern between reputable and inferior cables. Ensuring a cable meets strict

codes and standards is an expensive and arduous commitment for manufacturers, thanks to a combination of the cost of materials needed to meet *NEC* requirements combined with the intricate testing and ongoing certification follow-up processes required to maintain the listings.

One obvious warning sign of substandard or counterfeit cable is an unusually low price. If a cable's price is more than 30% below that of a reputable cable's, then it is likely that this low-cost cable is constructed of substandard raw materials, or the cable has not been through certification testing. Cables meeting this low-cost, low-quality profile frequently are found through online retail sites, and usually are purported to be manufactured by private-label brands. Sometimes these cables are priced so unrealistically low that in reality, the price would barely cover the manufacturing cost—let alone the actual costs of raw materials and compliance testing—of legitimately manufactured cables.

Another indicator of an unacceptable and inferior cable design is the use of aluminum versus copper conductors. In some consumer circles, cables with copper-clad aluminum (CCA) conductors are being promoted and sold as equivalent to cables with copper conductors. In actuality, CCA cables contain only a thin layer of copper over aluminum, which is less costly than copper. CCA cannot transmit power for Class 2 or Class 3 circuits as efficiently as copper.

"Aluminum has a different malleability so when it gets terminated into the connector, it is brittle and often breaks, leading to intermittent signal and power," explains Todd Harpel, director of standards for Berk-Tek. "Cable constructions containing CCA conductors are an even-more catastrophic hazard when used in PoE or powering over communications cable. Aluminum heats up more than copper when both data and power are put over the conductors, which results in higher insertion loss and DC resistance, leading to cable-performance deficiencies. And since aluminum conductors in communications cable cannot be listed, they do not meet the *NEC*. This makes it a critical safety issue," Harpel adds.

One deceptive tactic often found online is for the seller to claim that a Category-rated cable contains CCA, implying that this is the basis for the lower cost. However, they are also assuming you are ignorant of the fact that CCA in network cable is forbidden by the *NEC*. In a way, these unscrupulous sellers are sending the message, "I am enabling you to break the law," should you install this cable in buildings that must comply with *NEC* requirements. And be aware, if the seller is stating the cable contains CCA conductors, it is extremely likely that the cable also uses less-costly and often inferior materials along with poor packaging. Additionally, CCA is not permitted by the American and Canadian National Standards ANSI/UL 444 and CSA C22.2 No. 214. Therefore, cable constructions employing CCA conductors cannot be certified or listed.

If you are uncertain if the cable contains aluminum conductors, you should be able to differentiate good cable from bad cable by comparing the weight between two boxes of similar communications cable. Cable with CCA weighs approximately 30% less than cable with legitimate copper conductors. Additionally, you can clearly identify CCA conductors by scraping the thin layer of copper off the conductor to see if aluminum is exposed.

Third-party certifications

An obvious telltale indicator of a counterfeit cable is the misleading label on the box or the legend on the cable jacket—or lack thereof. In some cases, the seller of the noncompliant cable often does not provide the required certification markings, safety listings or transmission-performance indicators on the cable or packaging, so they cannot be accused or held accountable for misinforming the buyer. Even though these markings are either required by code or for the critical application system performance, buyers must beware and perform their own due diligence to verify these cable attributes before completing the purchase and delivery of the cable. One way to confirm the cable is legitimate is by finding their listing information on the website of the NRTL.

> What if an MRI image from a remote healthcare provider was distorted while you were in the ER?

Through some internet-only channels, sellers may indicate a cable's safety and performance characteristics in their cryptic descriptions. But the cable that shows up on your doorstep may or may not have any such indications. Always ask, in advance of the purchase, for the name and location of the manufacturer, as well as the warranties, for the cable. In addition, listing information for every reputable supplier of legitimately made and certified cable should be easy to find on the website of the third-party NRTL. If you are unable to identify the manufacturer, the supplier should be able to produce verifiable evidence/paperwork of their third-party NRTL

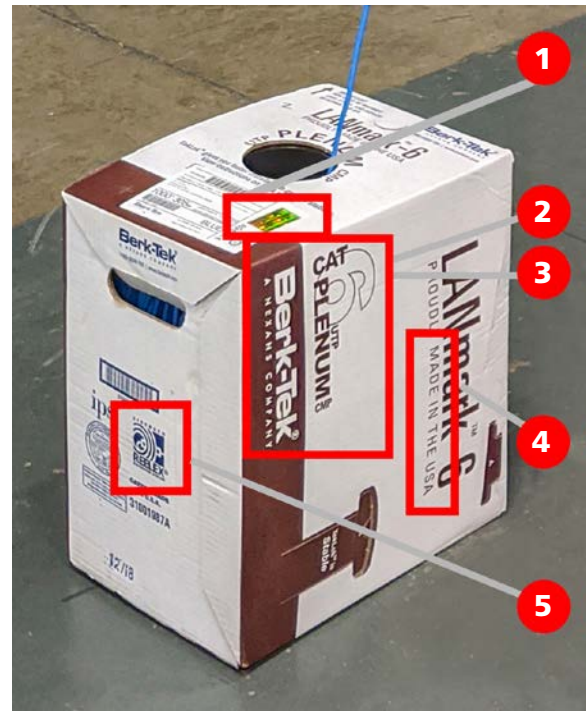
certifications and independent performance testing results. If they struggle with answers or delay producing this information, walk away.

As a vital measure of protection for their own certification marks, UL provides a holographic label for each cable that it has tested and certified. These labels verify that the manufacturer and cable meet the description of the UL surveillance documents, which help to differentiate authorized products from counterfeit cables.

"UL has been requiring holographic labels for cables since 2009 and has been training installers, inspectors, retailers and others to look for the holographic label on the product to ensure these cables are authorized as Certified by UL," states Anthony Tassone, UL principal engineer. The holographic label is required on each box or reel of UL-listed cable. It has multiple security features similar to the technology used in U.S. monetary currency in the background, with embedded code and proprietary color-changing ink, which can be authenticated using a business-card-size reader that is available from UL and CCCA.

"To earn the certification label, UL has an ongoing inspection and market-survey program to ensure that the cables use the authorized compounds with the necessary smoke-suppression and flame-retardant properties as well as continue to comply with the required large-scale flame tests. Testing is performed in both our labs, as well as on production samples at the cable-manufacturing factories, and witnessed by UL field engineers," Tassone explains. Every UL certified cable subscriber has a unique UL file number, tradename, or trademark printed on the surface of the cable.

The holographic label should be the first point of reference for all suppliers, installers and end users to know that the cable has been tested and is certified for safety. The holographic label, with a unique number specific to each manufacturer and each cable, is changed on a regular basis to avoid having them counterfeited.



These five indicators on a cable box can provide confidence that the cable inside meets safety and performance requirements: 1) a holographic label provided by UL that is unique to the cable manufacturer; 2) a statement of the cable's performance rating; 3) the manufacturer's logo; 4) a statement of the country in which the cable is manufactured; 5) the REELEX packaging logo.

Packaging

If a counterfeit cable is being produced, it likely is being packaged in an inferior box and payout mechanism. While most installers identify the packaging of low-voltage cabling as a "pull box," you may not know that these boxes are packaged using a unique and highly specialized coiling method called REELEX. Originally developed during World War II as a means for deploying communications cable, the figure-eight wind by REELEX has become the standard package for most last-mile lengths of cable.

Knockoff pull boxes do not use precision REELEX coils, but rather feature what are sometimes called "scramble winds." These boxes look identical to any other box of cable on the outside, but are very different inside. Improper coiling of the cable can lead to kinking, cable damage and poor cable-installation practices, which impacts both performance and safety. Manufacturers that used REELEX equipment and patented technology are licensees of REELEX, and are required to have the trademark logo printed on the box. This logo signifies to the installer that not only is the process genuine, but also that the cable will pay out from the box twist-free and without tangles. It also verifies that the manufacturer has not damaged the cable during packaging. REELEX has found that most knockoff brands will tangle and become damaged because the manufacturer does not have the proper coiling equipment or the REELEX software that precisely controls the coiling process.

Taking ownership and action

The onus to avoid buying and installing counterfeit or noncompliant cable that does not meet the applicable *NEC*

requirements or industry standards ultimately is on the installer. The legal ramifications and liability fall on the installer of the cable, not the person or company that manufactures or ultimately sells the cable. But all parties in the supply chain should understand the cause and serious life-safety impacts of these bad cables being installed. It is imperative for everyone involved to know the differences between certified/reputable cable and substandard or bogus cable. If each stakeholder in the supply chain is confirming the legitimacy of the cables prior to final installation, then the confidence levels are significantly improved. Specific safeguarding activities include validation from cable and component suppliers, distributors, system designers and integrators, building owners, construction inspectors, law enforcement, legislators and users.

Suffice it to say methods are in place to differentiate the good from the bad. CCCA is collaborating with UL and supply-chain partners on compliance and quality assurance. Recently, CCCA and UL took their findings to global law-enforcement agencies and customs officials to thwart the influx of unauthentic cabling and to protect the intellectual property rights of reputable cable and connectivity manufacturers. CCCA, representing the cable and connectivity industry, formed a task group to bring to the attention of the U.S. National Intellectual Property Rights Coordination Center (IPR Center) in Washington D.C. the dangers of counterfeit cables in the marketplace. Our industry is one of four strategic industries—along with pharmaceutical, microelectronics, and automotive—selected as part of a pilot initiative to educate law enforcement, customers/border protection and homeland security on the mission-critical impacts and perils that counterfeit products have on consumer safety.

More and more consumers and contractors are shopping online, which substantially increased in 2020 due to the COVID pandemic. "Much of the commercial substandard, mismarked, and counterfeit cable is ordered through e-commerce, and buyers think they are getting a bargain," states David Kiddoo, executive director of CCCA. "But a bargain in this sense can lead to severe repercussions and unintended consequences. Not only would purchasing and installing unsafe and non-complying cable in your project destroy your company's reputation, this could also lead to expensive lawsuits and liabilities for health, safety and network performance as a result."

The illegal sales of counterfeits, knockoffs, falsified products and other intellectual property-infringing items not only damages legitimate U.S. businesses, but also fuels other illicit crimes and poses other significant safety risks for all consumers. The CCCA is also a part of an industry consortium that includes other trade associations, including the Transnational Alliance to Combat Illicit Trade (TRACIT), to support efforts to introduce the SHOP SAFE Act of 2020 in the U.S. House of Representatives. These legislative proposals will serve to address this problem by incentivizing online e-commerce platforms to adopt best practices, keeping consumers informed, and imposing penalties on sellers of potentially harmful products.

It is also important to note that network integration is critical to provide for the safety and performance of emerging technologies, such as smart buildings and 5G. Each state or local jurisdiction adopts different regulations and licensure requirements regarding the installation of cable that delivers both data and power for Class 2 or Class 3 circuits. These include applications such as LED lighting, sensors, fire alarms, security and surveillance, building/home automation, audio visual systems, digital electronics and entertainment, and other emerging technologies.

Alternating-current (AC) electrical lines are installed by licensed electricians. Today, many intelligent building devices and applications are powered by low-voltage PoE circuits. These cabling for systems must be installed by trained low-voltage contractors, or integrators, to allow network systems integration and software programming. As a result, integrators should not be restricted by proposed legislation that would exclude or significantly limit their ability to perform installation projects that they have successfully carried out for years. Well-trained integrators understand installation best practices for low-voltage network cabling and connectivity. CCCA is assisting an industrywide consortium of connected technology stakeholders representing the ICT industry to address these legislative issues as they arise.

Whack-a-mole, keep your guard up

The path to raise awareness for these counterfeit and noncompliant cables with the general public, as well as with law enforcement, is a long road consisting of ongoing and increased training efforts. It is a never-ending battle, as once one offender is found, there are surely more undiscovered to unmask.

But while there are legal steps taken by CCCA members and other associations, it is a constant endeavor to continuously educate stakeholders including suppliers, contractors, installers and users. Following is a summary

checklist to follow in the quest to avoid installing bad cable and protect all low-voltage integrators and consumers, one box at a time.

- Buy known brands
- Specify better cable than you think you need to meet the minimum requirements of your project. Considering the cost of replacing cable buried in walls, plenums, etc., the extra expense now can be considered insurance against having to replace cable that becomes obsolete in the future.
- If the price is significantly below the average competitive market value by 30% or more, beware.
- Review the packaging label. If it is a questionable brand without a stated manufacturer, country of origin, fire performance rating (such as CMP or CMR), transmission performance (such as Category 5e or 6), and NRTL certification, investigate and require written proof of the safety listing and performance verification through an NRTL.
- Look at the product specifications to see if the cable conductor is solid copper or contains copper clad aluminum (CCA). Cables with CCA conductors are unsafe to be installed in ICT network applications.
- Inspect the packaging and payout. Is it the cable kinking when pulled out of the box or are there thin spots or inconsistencies in the cable geometry? If it is in a pull box, does it feature the REELEX logo?
- Look for the holographic label on each box of cable and recheck with UL to confirm the product brand name and certification.
- If you suspect a counterfeit cable, look up UL and ETL public notices that list known fraudulent suppliers. You can also report suspect cable products to UL or ETL, depending on the referenced NRTL certifications provided by the seller.
- Use the CableCheck application from the CCCA website, which is a free downloadable app for your smart device to detect suspicious cable. The app is available at cccassoc.org/news/free-apps/

Suppliers can also assist their customers, integrators, and ultimately consumers by periodically following these important steps to assure their cable is compliant and to protect their own intellectual property rights and technologies.

- Record all trademarks and trade names with the U.S. Customers and Border Protection (CBP) at iprr.cpb.gov.
- Ensure all products have been certified (listed and verified) by an NRTL and make sure that all registration information and tests are up to date, with reports available for your customers and enforcement authorities.
- Ensure the packaging is printed with all updated information, required certifications, safety listings, performance verifications and logos, such as the UL holographic label.
- Provide cabling system warranties through certified installers who provide passing test results with every installed channel.
- Engage with the CCCA and become a member (cccassoc.org/membership/)

A last thought

In today's competitive world, having an infrastructure that is scalable and can respond quickly to technology changes is vital. As our industry is moving forward globally toward intelligent building integration, it is imperative that the entire ICT community, from manufacturers to installers to consumers, understand the consequences when the basic building blocks of the infrastructure are compromised. Once a structured cabling system is installed, it is expected to last and support many technology upgrades. This can only be accomplished if the core network is safe and sound, which starts and ends with quality cable and connectivity, and smart installers.

The CCCA is the voice of the structured cabling industry. Leading manufacturers of cable and connectivity products, distributors, and material suppliers have joined together in CCCA to inform, educate and provide thought leadership on vital issues and topics. CCCA's members include: 3M, Alphagary, Anixter, Belden, Berk-Tek, Cable Components Group, Chemours, CommScope, Daikin America, Dow, Graybar, Hitachi Cable America, Leviton, OCC, Prsymian Group, REELEX, Sentinel Connector Systems, Superior Essex, Wonderful Hi-Tech. ◆

Timothy Copp *is chair of the Compliance/Anti-Counterfeit Committee for the Communications Cable and Connectivity Association, which serves as a major resource for well-researched, fact-based information and education on issues and technologies that are vital to the structured cabling industry. Tim has more than 15 years of experience in packaging for the wire and cable industry and holds the position of vice president of business development at REELEX Packaging Solutions.*

Carol Everett Oliver, *RCDD, DCDC, ESS is an industry freelance consultant to CCCA with 25 years of experience helping a variety of organizations deliver relevant, authoritative information on a variety of topics. Carol also is currently President-Elect of BICSI, a professional association supporting the advancement of the information and communications technology (ICT) profession. Carol also chairs BICSI's Intelligent Building Standard Subcommittee.*