

*There are growing concerns in the network equipment industry about the significant amount of multi-conductor communications cables containing copper coated aluminum (CCA), copper coated steel and other non-standard conductors masquerading as Category 5e or even Category 6 cables.*



## APPLICATION NOTE: COPPER CLAD ALUMINUM (CCA) CABLES

*The existence of these non-standards compliant, and often counterfeit, cabling products in the market can present serious problems for the companies using them, as well as the cabling installers and engineers who place these products within their customers' network environments.*

*While these products might look like standard cable and appear to perform like them in some situations, there are significant differences that could present network problems and safety hazards.*

## Introduction

The presence of counterfeit cabling is not a new problem for the industry; fake or non-standard cable products have existed in the market for several years, according to experts. It has been a persistent issue for the industry that does not seem to be going away. Part of the reason for this is many companies are looking for inexpensive networking solutions, and these cable products tend to be less costly.

Existing methods for identifying these non-standard products have only been partially successful. In order for the industry to effectively address the concerns of CCA and other non-standard cable products, new methods are needed.

Testing solutions from Fluke Networks show promise in accurately identifying such products. While these solutions can not immediately identify counterfeit cable products with the push of a button, Fluke Networks is determined to develop capabilities to make it easier for organizations to identify these less-than-standards compliant products.

## Ongoing Challenge for the Industry

CCA cable products have been showing up on the market for several years, in large part because there is demand for less expensive cable from companies looking to save money. Since aluminum is less costly than copper, CCA cable is typically less expensive than all-copper products. Many buyers working with tight budgets therefore find the cheaper cable products appealing. They might not realize that they are not receiving standards compliant solid copper cable

“It’s not difficult to find these products on the Internet through wholesalers and distributors,” says Frank Peri, executive director of the Communications Cable & Connectivity Association (CCCA), an organization that provides best practices and educational information about quality communications cables, connectivity devices and related products. Providers are offering the non-standard cable products at significantly lower prices than compliant products. Some sell both compliant and non-compliant cable. Peri points out that there are industries and applications where CCA is approved and suitable, but it’s the cases where CCA is not suitable that need to be addressed.

## A Common Problem

It’s difficult to quantify the market for counterfeit cables, Peri says, but he thinks the number of distributors and CCA cables represent significant enough share to be a major concern. “We tend to find more of these on the west coast [of the United States], because Long Beach [Calif.] is a huge port of entry,” he says.

According to sources that are both knowledgeable and reliable, about 300 kilometers of CCA cable masquerading as Category 5, 5e and 6 is being sold in the U.K. each month by certain wholesalers and distributors, says Mike Gilmore, managing director of e-Ready Building Ltd. and technical director of the Fibreoptic Industry Association (FIA), who is involved in standardization of the design, implementation and operation of telecommunications facilities and infrastructures in the U.K., Europe and other regions.

“The cables are generally sold through the electrical wholesaler market rather than the data market, so I only see them after a problem has been identified,” Gilmore says.

Gilmore attributes the demand for CCA cabling to commoditization of the products and the “de-skilling” of the data cabling industry. “Electrical contractors are now an obvious supplier for small data cabling tasks and they are very cost-driven,” he says. “The wholesalers know this and react accordingly. On many occasions the install is not tested using ‘industry standard’ test equipment, so the problems are not found out until too late.”

Efforts are underway in the industry to address the problem of counterfeit cables. For example, in November 2013 CCCA and BICSI, an association supporting the IT systems (ITS) industry with information, education and knowledge assessment, announced that they will collaborate on an international effort to stop counterfeit and non-compliant cables.

All ITS industry stakeholders are affected by counterfeit and substandard products, said Jerry Bowman, president of BICSI. “Everyone in the supply chain has a duty of care to ensure that the product they are purchasing or installing conforms with safety and quality standards and regulations,” Bowman said. “When a counterfeit product is installed it’s more than a performance issue—it can threaten the safety of the workplace and put the consumer at risk.”

CCCA has made significant strides in educating the ITS consumer and U.S. law enforcement in order to ensure consumers are not deceived into buying cabling that is counterfeit or does not meet advertised standards, Bowman added. And while the work of CCCA is outside of BICSI's charter, CCCA member cabling manufacturers and distributors have banded together to serve as the industry watchdog for these quality and safety issues, he said.

Peri called it "an excellent example" of CCCA and BICSI leadership working together to educate international law enforcement on counterfeit cables that threaten the global industry and risk public safety.

Peri says. "It's very unfortunate that copper clad aluminum products are being marketed as compliant to North America codes and standards for low voltage communications when in fact, they are not. This is particularly concerning if the cable is being used to support power-over-Ethernet devices. These cables should not be called category cable because they do not meet the standards" that require solid copper conductors for multi-conductor communications cables, including the National Electrical Code, UL 444, CSA 22.2 and TIA 568C.2.

Cables made with CCA conductors do not have a valid safety listing per the National Electrical Code (NEC), and can't be legally installed into areas of buildings that require CM, CMG, CMX, CMR or CMP rated cables, according to CCCA. The consequences of installing these types of cable can be reduced network performance and a potential safety hazard.

In some cases, there might be legal risks of installing counterfeit cable. CCCA has published a white paper entitled "Potential Liability for Contractors Installing or Manufacturers Marketing Falsely Labeled Copper Clad Aluminum Cable". The paper is intended to educate the industry about the legal risks assumed by installers of communications cables that are specifically not allowed by the National Electrical Code.

CCCA's research indicates that many contractors are not aware that cables marked as Category 5e or 6 and made with CCA conductors cannot be legally installed into any area that requires a National Electrical Code fire safety rating. The National Electrical Code, which has been incorporated into law for virtually all states and local municipalities in the U.S., defines requirements for cables installed in buildings, residences and other structures, according to CCCA. Any installation of multi-conductor communication cables made with CCA conductors behind walls or in enclosed spaces is likely to be a code violation in every jurisdiction in the country. Depending on the jurisdiction, violation of building codes can result in significant fines or imprisonment.

Another main concern is that these cables do not support PoE applications due to their increased DC Resistance. Resistance of a solid aluminum cable is about 55% greater than for a copper cable of the same diameter. The greater resistance will result in greater heating of the cable and lower voltage available at the powered device. With compliant solid copper cabling, the resistance heating of cabling bundles led to a reduced ambient temperature specification for higher current applications. Within IEEE Std 802.3, the statement "Type 2 operation requires a 10 °C reduction in the maximum ambient operating temperature of the cable when all cable pairs are energized" is included in Clause 33.1.4.1. No allowance is made for the much greater heating that would occur in a CCA cable.

## Methods of Identifying CCA Cables

There are several methods for detecting counterfeit cable products. One way companies can test for the presence of CCA cables is by weighing the cable box. Because aluminum is lighter than copper, boxes of CCA cable tend to be noticeably lighter than their all-copper counterparts.

However, CCA cable vendors are aware of this, and there have been reports of installers finding "ballast" in the cabling boxes designed to make them feel as heavy as all-copper cables. Furthermore, there are heavier versions of CCA that can closely approximate the weight of real copper cabling.

"Weighing the box is not foolproof," Peri says. He says a more effective method for identifying CCA is to snip off a piece of the cable to expose the conductor, then scrape it with a knife to remove the top layer of copper. If there's a silver color beneath that indicates the presence of aluminum.

The scraping method is fine if a company suspects that a new cable is counterfeit, Peri says. If the cable is already installed in a building and the company is not pleased with performance, cutting the cable is not as easy and probably not the preferred method for most companies.

Cable testing is another way to identify fake cable, but field testing these CCA cables to either ANSI/TIA or ISO/IEC might not catch the fact that they are CCA cables. Testing to the ANSI/TIA-568-C.2 standard is deferred to ANSI/TIA-1152 Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling, where DC resistance is not required to be included in a field test. Even if TIA required DC Resistance as a field test, it would not guarantee finding CCA cable.

We know this from looking at ISO/IEC results, where DC Resistance does have a field test limit. Using a particular CCA cable, a Class D Channel Link less than approximately 71 m (233 feet) would almost certainly issue a pass because the DC resistance test limit is fixed at 25 ohms regardless of the length of the channel.

At first glance, the solution might seem obvious: Make DC resistance a field test requirement and pro-rate the limit based on length. Practically speaking, the measurement uncertainty associated with length measurements would increase the probability of failing a link that is compliant. Limited data from the field suggests that CCA cable fails DC Resistance Unbalance, regardless of length. That's a parameter that can be found in both ANSI/TIA and ISO/IEC cabling standards as well as IEEE standards.

This is also a measurement that can be carried out with Fluke Networks' Versiv DSX-5000 CableAnalyzer. The DSX-5000 is designed to improve the efficiency of copper certification for testing Cat 6A and Class F<sub>A</sub>. When testing a CCA cable with the addition of DC Resistance Unbalance, Fluke Networks found the DC Resistance Unbalance to be clearly out of specification. As can be seen in the example below, the resistance unbalance limit is calculated for each pair based on that pair's measured loop resistance.

The Resistance Unbalance measurement verifies that both wires in a pair have equal resistance and will, therefore, carry equal amounts of current in a PoE application. As can be seen in the example below, the resistance unbalance limit is calculated for each pair based on that pair's measured loop resistance.

RESISTANCE		RESISTANCE UNBALANCE	
VALUE	Ω	VALUE	LIMIT
	Ω	Ω	Ω
1,2	18.2	2.62	0.55
3,6	16.1	0.04	0.48
4,5	17.3	1.81	0.52
7,8	16.1	0.07	0.48
LIMIT	25.0		

DSX CableAnalyzer Test Limit Name	DC Resistance Unbalanced(Ω)	
	Channel	Permanent Link
TIA Cat 5e Perm. Link (+PoE)	0.20 or 3.0%	-
TIA Cat 6 Perm. Link (+PoE)	0.20 or 3.0%	-
TIA Cat 6A Perm. Link (+PoE)	0.20 or 3.0%	-
ISO11801 PL Class D (+PoE)	0.20 or 3.0%	0.15 or 3.0%
ISO11801 PL Class E (+PoE)	0.20 or 3.0%	0.15 or 3.0%
ISO11801 PL2 Class Ea (+PoE)	0.20 or 3.0%	0.15 or 3.0%

With the field testing standard ANSI/TIA-1152 now open for review, there might be just cause in defining DC Resistance Unbalance as a field test and setting test limits in ANSI/TIA-568-C.2 or its revision ANSI/TIA-568-D.2, to help deal with the CCA cable issue, and provide greater assurance for meeting IEEE PoE requirements.

## Buyer Beware

Despite the efforts underway to educate the industry about the presence of counterfeit cable, and the methods for identifying CCA, the problem remains a serious one for the network cable market.

To avoid potentially serious problems and legal repercussions, it's important that companies ensure they're putting in reliable, standard cable products, regardless of their budget. The temptation to purchase and install inexpensive cable in order to stay in line with budgets is strong. But this is clearly a case of "buyer beware."

Because the installations of non-standard products are “cheap”, tests are frequently not undertaken in line with normal practice, according to Gilmore. “So the connections’ reliability problems are usually the first alert one receives—generally weeks after the install is completed,” he says.

Fluke Networks understands that no single, all-encompassing solution to the problem exists today, and is trying to develop a test regime that actually invokes the requirements of the existing standards for length dependent parameters, focusing on DC loop resistance.

“In Europe, I have repeatedly drawn the attention of installers and their clients to the existence of length-dependent limits, since they were included in the international and European cabling standards over 10 years ago,” Gilmore says. “Therefore, from my perspective I am really pleased to see the effort currently underway by Fluke [Networks].”

Fluke Networks, as a leader in the cable testing market, clearly has the experience and expertise to help tackle this issue.

## About Fluke Networks

Fluke Networks is the world-leading provider of network test and monitoring solutions to speed the deployment and improve the performance of networks and applications. Leading enterprises and service providers trust Fluke Networks’ products and expertise to help solve today’s toughest issues and emerging challenges in WLAN security, mobility, unified communications and datacenters. Based in Everett, Washington, the company distributes products in more than 50 countries.

For more information, visit [www.flukenetworks.com/rft](http://www.flukenetworks.com/rft)

## CertiFiber® Pro - Accelerates every step of the fiber certification process

The CertiFiber Pro improves the efficiency of fiber certification with a 3 seconds, two fibers at both wavelengths. The Taptive user interface simplifies set-up, eliminates errors and speeds troubleshooting. A set reference wizard ensures correct reference setting and eliminates negative loss errors. Built on the future-ready Versiv platform, CertiFiber Pro provides merged Tier 1 (Basic) / Tier 2 (Extended) testing and reporting when paired with OptiFiber Pro module. A convenient quad module supports both singlemode and multimode and is multimode Encircled Flux compliant. Copper certification and Wi-Fi Analysis and Ethernet troubleshooting modules are also available. Analyze test results and create professional test reports using LinkWare Management Software.



## DSX-5000 CableAnalyzer™ - Accelerates every step of the copper certification process

The DSX-5000 CableAnalyzer improves the efficiency of copper certification with unmatched speed for testing Cat 6A and Class FA while meeting draft IEC Level V – the most stringent accuracy requirement. The ProjX Management System helps ensure jobs are done correctly the first time and helps tracks progress from set-up to systems acceptance. Versiv platform supports modules for fiber testing (Both OLTS and OTDR) and Wi-Fi Analysis and Ethernet troubleshooting. The platform is easily upgradeable to support future standards. Troubleshoot faults faster with the Taptive user interface which graphically displays the source of failures including crosstalk, return loss and shield faults. Analyze test results and create professional test reports using LinkWare™ Management Software.

## OptiFiber® Pro OTDR – Built for the Enterprise

OptiFiber Pro is the industry's first OTDR built from the ground up to meet the challenges of enterprise fiber infrastructures. This troubleshooting and certification tool combines uncomplicated power, unparalleled efficiency and the exact functions needed for troubleshooting campus, data center and storage fiber networks.

The OptiFiber Pro OTDR elevates fiber testing with the industry's only smartphone interface that turns a technician into a fiber expert. The DataCenter OTDR configuration eliminates uncertainty and errors that occur when testing data center fiber. Its ultra-short dead zones enable testing of fiber patchcords in virtualized data centers. These capabilities, plus the fastest-in-the-industry trace times, make the OptiFiber Pro OTDR a must-have tool.



## OneTouch™ AT- Network Assistant - An automated all-in-one tester for understanding end-user network performance

The OneTouch AT Network Assistant is an all-in-one Gigabit Ethernet troubleshooter for copper, fiber optic and Wi-Fi networks. It provides a client view of network performance so you can resolve problems fast and complete deployment projects on time.

More information at: [www.flukenetworks.com/content/versiv](http://www.flukenetworks.com/content/versiv)

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to [www.flukenetworks.com/contact](http://www.flukenetworks.com/contact)

**Corporate Office:**  
Fluke Networks  
P.O. Box 777 Everett, WA USA 98206-0777  
**1-800-283-5853**  
e-mail: [info@flukenetworks.com](mailto:info@flukenetworks.com)

**European Office:**  
Fluke Networks  
P.O. Box 1550, 5602 BN Eindhoven  
Germany **0049-(0)682 2222 0223**  
France **0033-(0)1780 0023**  
UK **0044-(0)207 942 0721**  
e-mail: [sales.core@flukenetworks.com](mailto:sales.core@flukenetworks.com)