

Verkupferte Aluminiumkabel (CCA)

Überblick

In der Netzwerkgerätebranche wächst die Besorgnis über die bedeutende Menge an mehradrigen Kommunikationskabeln mit verkupferten Aluminium (CCA), verkupferten Stahl und anderen nicht standardmäßigen Leitern, die als Kategoriekabel ausgegeben werden.

Das Vorhandensein dieser nicht konformen und häufig gefälschten Kabelprodukte im Markt kann ernste Probleme erzeugen für die Firmen, die sie verwenden, wie auch für die Kabelinstallateure und Ingenieure, die diese Produkte in die Netzwerkkumgebungen ihrer Kunden platzieren.

Während diese Produkte wie Standardkabel aussehen können und in manchen Situationen wie sie zu arbeiten scheinen, bestehen bedeutende Unterschiede, die Netzwerkprobleme und Sicherheitsrisiken aufwerfen können.

Gefälschte Kabel sind kein neues Problem für die Branche; gefälschte oder nicht standardisierte Kabelprodukte existieren nach Ansicht der Experten schon seit einigen Jahren auf dem Markt. Es ist ein hartnäckiges Problem für die Branche, das nicht wegzugehen scheint. Ein Teil des Grundes dafür ist, dass viele Firmen nach preiswerten Vernetzungs-Solutions suchen, und diese Kabelprodukte neigen dazu, weniger teuer zu sein.

Vorhandene Methoden zur Erkennung dieser nicht standardmäßigen Produkte waren nur teilweise erfolgreich. Inspektion und für UL nachvollziehbare holographische Etiketten, UL oder ETL-Einträge, Hersteller-Teilenummern oder manuelle Kontrollen durch Wiegen, Kratzen oder Schmelzen des Kabels sind subjektiv und unpraktisch. Zum effektiven Identifizieren von CCA und anderen nicht standardmäßigen Kabelprodukten muss die Branche sich um neue Methoden bemühen.

Die Test-Solutions von Fluke Networks sind viel versprechend für die Identifikation solcher Produkte. Während diese Lösungen gefälschte Kabelprodukte nicht sofort durch einen einfachen Tastendruck identifizieren können, ist Fluke Networks entschlossen, die Fähigkeiten zu entwickeln, die es den Unternehmen vereinfachen, nicht standardkonforme Produkte zu identifizieren.

Andauernde Herausforderung für die Branche

CCA-Kabelprodukte tauchen seit einigen Jahren auf dem Markt auf, hauptsächlich aufgrund der hohen Nachfrage nach preiswerteren Kabeln seitens der Firmen, die Geld sparen wollen. Da Aluminium preiswerter als Kupfer ist, ist CCA-Kabel gewöhnlich billiger als solide Kupferprodukte. Viele Käufer mit begrenzten Budgets finden daher billigere Kabelprodukte attraktiv. Sie erkennen möglicherweise nicht, dass sie kein konformes solides Standard-Kupferkabel erhalten.

„Es ist nicht schwierig, diese Produkte auf dem Internet durch Großhändler und Verteiler zu finden“, sagt Frank Peri, Geschäftsführer der Communications Cable and Connectivity Association (CCCA), einer Organisation, die optimale Verfahren und pädagogische Informationen über Qualitäts-Kommunikationskabel, Konnektivitätsgeräte und verwandte Produkte bereitstellt. Anbieter bieten die nicht standardmäßigen Kabelprodukte zu erheblich niedrigeren Preisen als konforme Produkte an. Manche verkaufen konforme und nicht-konforme Kabel. Peri betont, dass es Branchen und Anwendungen gibt, in denen CCA genehmigt und passend ist, aber es die Fälle sind, in denen CCA nicht geeignet ist, die behandelt werden müssen.

Ein geläufiges Problem

Es ist schwierig, den Markt für gefälschte Kabel quantitativ zu definieren, sagt Peri, aber er meint, dass die Anzahl von Händlern und CCA-Kabeln einen ausreichend bedeutenden Anteil haben, dass sie ein großes Problem darstellen. „Wir finden mehr dieser Produkte an der Westküste [der USA], weil Long Beach [Kalif.] ein enormer Importhafen ist“, sagt er.

Sachkundigen und zuverlässigen Quellen zu Folge werden in Großbritannien jeden Monat ungefähr 300 Kilometer CCA-Kabel maskiert als Kategorie 5, 5e und 6 von bestimmten Großhändlern und von Vertriebshändlern verkauft, sagt Mike Gilmore, Managing Director von e-Ready Building Ltd. und technischer Direktor der Fibreoptic Industry Association (FIA) für Standardisierung von Design, Implementierung und Betrieb der Telekommunikations-Anlagen und -infrastrukturen

in Großbritannien, Europa und in anderen Regionen.

„Die Kabel werden im Allgemeinen über den elektrischen Großhandel anstatt über Datenmarkt verkauft, daher sehe ich sie nur, nachdem ein Problem festgestellt worden ist“, sagt Gilmore.

Gilmore schreibt die Nachfrage nach CCA der Kommoditisierung der Produkte und der Dequalifizierung der Datenverkabelungsbranche zu. „Elektriker sind jetzt ein offensichtlicher Lieferant für kleinere Datenverkabelungsaufgaben und sie sind sehr kostengesteuert“, sagt er. „Die Großhändler wissen das und reagieren dementsprechend. Oft wird die Installation nicht mit „Industriestandard“-Testgeräten geprüft, und daher werden die Probleme erst herausgefunden, wenn es zu spät ist.“

Die Industrie bemüht sich, das Problem der gefälschten Kabel zu beheben. Zum Beispiel kündigte im November 2013 CCCA und BICSI, eine Vereinigung, die die IT-Branche mit Informationen, Ausbildung und Wissensbewertung unterstützt, an, dass sie auf internationaler Ebene zusammenarbeiten werden, um gefälschte und nicht-konforme Kabel zu unterbinden.

Alle an der ITS-Industrie Beteiligten werden von gefälschten und minderwertigen Produkten beeinträchtigt, sagte Jerry Bowman, ehemaliger Präsident von BICSI. „Jedes Mitglied in der Versorgungskette hat die Pflicht, sicherzustellen, dass das Produkt, das er kauft oder installiert, den Sicherheits- und Qualitätsstandards und -vorschriften entspricht“, sagte Bowman. „Wenn ein gefälschtes Produkt installiert wird, bedeutet dies mehr als ein Leistungsproblem – es kann die Sicherheit des Arbeitsplatzes bedrohen und den Verbraucher gefährden.“

CCCA hat bedeutende Fortschritte in der Aufklärung von ITS-Verbrauchern und der Strafverfolgungsbehörde gemacht, um sicherzustellen, dass die Verbraucher nicht zum Kauf von Kabeln verleitet werden, die gefälscht sind oder nicht die vorgegebenen Standards erfüllen, fügte Bowman hinzu. Und während die Arbeit von CCCA außerhalb der Charta von BICSI liegt, haben sich die Kabelhersteller und -Großhändler unter den Mitgliedern von CCCA zusammengetan, um als Wächter für die Industrie bezüglich dieser Qualitäts- und Sicherheitsfragen zu fungieren, sagte er.

Peri nannte das „ein ausgezeichnetes Beispiel“, wie die Führungen von CCCA- und BICSI zusammen arbeiten, um die internationalen Behörden über gefälschte Kabel aufzuklären, die die globale Industrie und die öffentliche Sicherheit bedrohen.

sagte Peri. „Es ist sehr bedauerlich, dass verkupferte Aluminiumprodukte als konform zu nordamerikanischen Codes und Standards für Niederspannungskommunikationen vermarktet werden, wenn das tatsächlich nicht der Fall ist. Dies ist besonders besorgniserregend, wenn das Kabel zum Unterstützen von PoE-Geräten verwendet wird. Diese Kabel dürfen nicht Kategoriekabel genannt werden, weil sie nicht den Standards entsprechen, die solide Kupferleiter für mehradrige Kommunikationskabel erfordern, einschließlich des National Electrical Code, UL 444, CSA 22.2, TIA 568C.2 und ISO/IEC 11801Ausg. 2.2

Kabel, die mit CCA-Leitern hergestellt werden, haben keine gültige Sicherheitsbescheinigung gemäß National Electrical Code (NEC) und können legal nicht in Bereichen von Gebäuden installiert werden, die Kabel mit CM-, CMG-, CMX-, CMR- oder CMP-Zulassung erfordern, laut der CCCA. Die Konsequenzen der Installation dieser Kabelarten können verringerte Netzwerk-Performance und ein mögliches Sicherheitsrisiko sein.

In manchen Fällen könnten rechtliche Risiken bei der Installation von fälschlich ausgezeichneten Kabeln entstehen. CCCA hat ein Whitepaper mit dem Titel „Potential Liability for Contractors Installing or Manufacturers Marketing Falsely Labeled Copper Clad Aluminum Cable“ (Mögliche Haftung für die Installateure oder die Hersteller von fälschlich ausgezeichnetem verkupferter Aluminiumkabel) veröffentlicht. Das Papier soll die Branche über die legalen eingegangenen Risiken durch Installateure von Kommunikationskabeln informieren, die durch den National Electrical Code untersagt werden.

Die Untersuchungen von CCCA haben gezeigt, dass viele Vertragsarbeiter sich nicht bewusst sind, dass Kabel, die als Kategorie 5e oder 6 markiert und mit CCA-Leitern hergestellt sind, nicht legal in Bereichen installiert werden dürfen, für die eine National Electrical Code Brandschutzklasse erforderlich ist. Der National Electrical Code, der in praktisch allen Bundesstaaten und Städten in den USA Gesetz ist, definiert laut der CCCA die Anforderungen für die Kabel, die in Gebäude, Wohngebäude und andere Strukturen installiert werden. Jede Installation von mehradrigen Übertragungskabeln mit CCA-Leitern, die in Wänden oder in umschlossenen Räumen durchgeführt wird, ist wahrscheinlich eine Codeverletzung in jeder Rechtsprechung im Land. Abhängig von der Rechtsprechung kann ein Vergehen gegen die Bauvorschriften zu bedeutenden Geld- oder Gefängnisstrafen führen.

Eine andere bedeutende Sorge ist, dass diese Kabel wegen ihres erhöhten DC-Widerstands keine PoE-Anwendungen unterstützen. Der Widerstand eines soliden Aluminiumkabels ist ungefähr 55 % größer als der eines Kupferkabels des gleichen Durchmessers. Der größere Widerstand führt zu einer höheren Erhitzung des Kabels und einer niedrigeren verfügbaren Spannung am versorgten Gerät. Mit der standardkonformen soliden Kupferverkabelung führt die Widerstandsaufheizung der Kabelbündel zu einer verringerten Umgebungstemperatur für höhere Stromanwendungen. Zweitens können Methoden zur Bestimmung der physikalischen Eigenschaften des Kabels durchgeführt werden. Das Gewicht, der Nachweis von Aluminium und die elektrische Leistung des Kabels sind sichere Methoden zum Identifizieren von CCA-Kabeln, aber nicht narrensicher. Ein Beispiel: Es befinden sich jetzt mehrere Standards in Entwicklung, die ähnliche Anforderungen haben. Innerhalb IEEE-Norm 802.3 wurde die Aussage „Betrieb Typ 2 erfordert eine 10 °C-Verringerung in der maximalen Umgebungstemperatur des Kabels, wenn alle Adernpaare mit Energie versorgt werden“ in Klausel 33.1.4.1 aufgenommen. Keine Berücksichtigung erfolgt für die viel höhere Aufheizung, die in einem CCA-Kabel verursacht würde.

Methoden zur Erkennung von CCA-Kabeln

Es gibt einige Methoden zum Erkennen von gefälschten Kabelprodukten. Die erste Methode zum Bestimmen, ob ein CCA-Kabel anderweitig beschriftet sein könnte, ist, sich die Beschriftung anzusehen. Inspection should be made for a reference to UL, ETL or a holographic label on the packaging or a cable part number that isn't listed on the UL or Intertek website. Eine Methode zum Testen auf das Vorhandensein von CCA-Kabeln ist das Wiegen des Kabelkastens. Da Aluminium leichter als Kupfer ist, sind CCA-Kabelkästen gewöhnlich merklich leichter als ihre Gegenstücke aus solidem Kupfer.

Jedoch sind sich die Verkäufer von CCA-Kabeln dessen bewusst, und Installateure haben berichtet, „Ballast“ in Kabelkästen gefunden zu haben, durch den die Kästen sich so schwer wie Kästen mit solidem Kupfer anfühlen sollten. Außerdem gibt es schwerere Versionen von CCA, die dem Gewicht des echten Kupferkabels nahe kommen können.

„Das Wiegen des Kastens ist nicht narrensicher“, sagt Peri. Er sagt, dass eine effektivere Methode für die Feststellung von CCA sei, ein Stück Kabel abzuschneiden, um den Leiter abzuisolieren, und ihn dann mit einem Messer zu schaben, um die obere Kupferschicht abzukratzen. Wenn es dann darunter silbern schimmert, ist Aluminium vorhanden.

Diese Methode ist in Ordnung, wenn ein Unternehmen vermutet, dass ein neues Kabel eine Fälschung ist, sagt Peri. Wenn das Kabel bereits in einem Gebäude installiert ist und das Unternehmen nicht mit der Leistung zufrieden ist, ist das Ausschneiden des Kabels nicht so einfach und vermutlich nicht die bevorzugte Methode für die meisten Unternehmen. Manche Installateure verwenden einen Zigarettenanzünder, um den Leiter zu schmelzen, aber diese Praxis hat offensichtliche Sicherheits- und praktische Einschränkungen.

Eine weitere Möglichkeit, kupferverkleidete Aluminiumkabel zu finden, ist das Testen der Kabel. Auf den ersten Blick scheint die Lösung offensichtlich: Den DC-Widerstand zu einem Pflicht-Vor-Ort-Test machen und die Grenze basierend auf der Länge anteilmäßig festlegen. In praktischer Hinsicht würde die mit den Längenmessungen verbundene Messunsicherheit die Wahrscheinlichkeit erhöhen, dass ein Link den Test nicht besteht, der tatsächlich konform ist. Daten vom Feld deuten darauf hin, dass CCA-Kabel den DC-Widerstand-Unsymmetrietest nicht besteht, unabhängig von der Länge. Das ist ein Parameter, der in den Kabelstandards ANSI/TIA und ISO/IEC sowie den IEEE-Standards gefunden werden kann.

Das ist auch eine Messung, die mit dem Versiv DSX CableAnalyzer von Fluke Networks durchgeführt werden kann. Es soll die Effizienz der erweiterten Kupfer-Zertifizierung einschließlich Category 8 und Klasse I & II verbessern. Beim Prüfen eines CCA-Kabels mit dem Zusatz des DC-Widerstand-Unsymmetrietests fand Fluke Networks, dass die DC-Widerstand-Unsymmetrie klar außerhalb der Spezifikation lag.

Die Widerstands-Unsymmetriemessung bestätigt, dass beide Drähte in einem Paar den gleichen Widerstand haben und daher den gleichen Strom in einer PoE-Anwendung führen. Wie aus dem folgenden Beispiel ersichtlich ist, wird die Grenze für die Widerstands-Unsymmetrie für jedes Paar basierend auf dem gemessenen Schleifenwiderstand des Paares berechnet.



Der Feld-Prüfstandard für ANSI/TIA 1152 enthält nun DC-Widerstand-Unsymmetrie als Feldtest. Die Limits sind in ANSI/TIA-568-C.2 enthalten. Es ist keine obligatorische Zertifizierungs-Anforderung, sie lässt sich einfach integrieren, wenn Sie einen fähigen Kabeltester wie den DSX-CableAnalyzer haben. Aber die Sache hat einen Haken. Während ISO/IEC 11801Ausg. 2.2 die Grenzen für die DC-Widerstand-Unsymmetrie für die Kanal- und Permanent Link-Definitionen vorgibt, stellt ANSI/TIA-568-C.2 nur Testgrenzen für die Kanal-Definition zur Verfügung.

DSX CableAnalyzer Testlimit-Name	DC-Widerstand-Unsymmetrie (Ω)	
	Kanal	Permanent Link
TIA Cat 5e Perm. Link (+PoE)	>0,20 oder 3,0%	–

TIA Cat 6 Perm. Link (+PoE)	0,20 oder 3,0 %	–
TIA Cat 6A Perm. Link (+PoE)	0,20 oder 3,0 %	–
ISO11801 PL Class D (+PoE)	0,20 oder 3,0 %	0,15 oder 3,0 %
ISO11801 PL Class E (+PoE)	0,20 oder 3,0 %	0,15 oder 3,0 %
ISO11801 PL2 Class Ea (+PoE)	0,20 oder 3,0 %	0,15 oder 3,0 %

Caveat emptor (Gewährleistungsausschluss)

Trotz der Bemühungen, die Branche über die Existenz von gefälschten Kabeln und die Methoden zum Erkennen von CCA zu informieren, bleibt das Problem ernst für den Netzwirkabelmarkt.

Um möglicherweise ernste Probleme und rechtliche Auswirkungen zu vermeiden, ist es wichtig, dass Unternehmen sicherstellen, dass sie zuverlässige standardmäßige Kabelprodukte installieren, unabhängig von ihrem Budget. Die Versuchung, billiges Kabel zu kaufen und zu installieren, um ein Budget einzuhalten, ist stark. Es ist auch verlockend, alte Tester zu verwenden, die nicht in der Lage sind, die heutigen Kabeltestanforderungen zu erfüllen. Aber das ist eindeutig ein Fall von „falscher Sparsamkeit“.

Da die Installationen von nicht standardmäßigen Produkten „billig“ sind, werden Tests häufig nicht gemäß normaler Praxis durchgeführt, sagt Gilmore. „So sind die Zuverlässigkeitsprobleme der Verbindungen normalerweise der erste Hinweis, den man erhält - im allgemeinen Wochen, nachdem die Installation abgeschlossen ist“, sagt er.

Fluke Networks versteht, dass heute keine umfassende Lösung für das Problem existiert, und versucht, eine Testabfolge zu entwickeln, die wirklich auf den Anforderungen der vorhandenen Standards für längenabhängige Parameter beruht, mit Konzentration auf dem DC-Schleifenwiderstand.

„In Europa habe ich wiederholt die Aufmerksamkeit von Installateuren und ihren Kunden auf das Bestehen von längenabhängigen Grenzen gelenkt, da sie in den internationalen und europäischen Verkabelungsnormen vor über 10 Jahren eingeschlossen wurden“, sagte Gilmore. „Deshalb freue mich ich wirklich, die Bemühungen seitens Fluke [Networks] zu sehen.“

Widerstand-Unsymmetrie ist jetzt eine praktische Methode, die Leistung der Verkabelung für die neuesten PoE-Anwendungen zu gewährleisten und eine gute Möglichkeit, Nicht-Standard-Kabel zu identifizieren.



Über Fluke Networks

Fluke Networks ist ein weltweit führender Anbieter von Tools zur Zertifizierung, Fehlersuche und Installation für Experten, die wichtige Netzwerkverkabelungsinfrastrukturen installieren und warten. Von der Installation der fortschrittlichsten Rechenzentren bis hin zur Wiederherstellung von Diensten bei schlechten Wetterbedingungen – unsere Kombination aus unschlagbarer Verlässlichkeit und unvergleichlicher Leistung stellt sicher, dass Aufträge effizient erledigt werden können. Zu den Top-Produkten des Unternehmens zählt das innovative LinkWare™ Live, die weltweit führende, Cloud-verbundene Lösung für Kabelzertifizierung mit bisher über vierzehn Millionen hochgeladenen Messergebnissen.

+ 1-800-283-5853 (US & Canada)

1-425-446-5500 (International)

<http://www.flukenetworks.com>

Descriptions, information, and viability of the information contained in this document are subject to change without notice.

Revised: 1. Oktober 2019 7:51 AM

Literature ID: 6002212

© Fluke Networks 2018