FLUKE networks

White Paper

Many of us will remember the days when the standard question at presentations and workshops on structured copper cabling was whether a shielded or unshielded system was preferable and whether it is true that incorrectly connected shielding made a shielded system worse than an unshielded one.

SHIELDING INTEGRITY

Some staunchly held technical clichés were brought out in the battle between the two technologies. One was that the open shielding acted like an antenna and therefore sent and received amplified interference.

With the introduction of the IEEE 10GBASE-T application standard in 2006, which allowed transmission at speeds of up to 10Gb/s over a Cat 6A or Class EA cabling system, the concerns became more specific and two different opinions emerged.

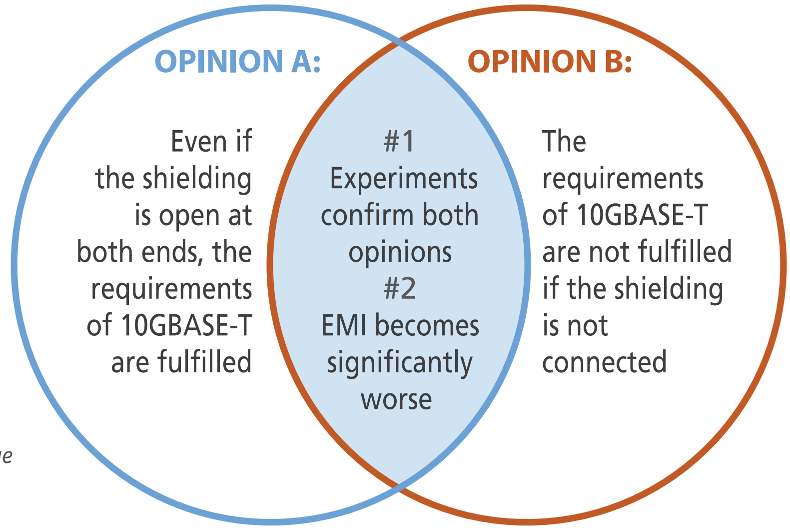


Figure 1: Opinions on the issue of "open shielding"

Opinion A pushed by the supporters of shielded cabling solutions, stated that even if the shielding was incorrectly connected at both ends of the transmission line, transmission still functioned correctly in accordance with 10GBASE-T.

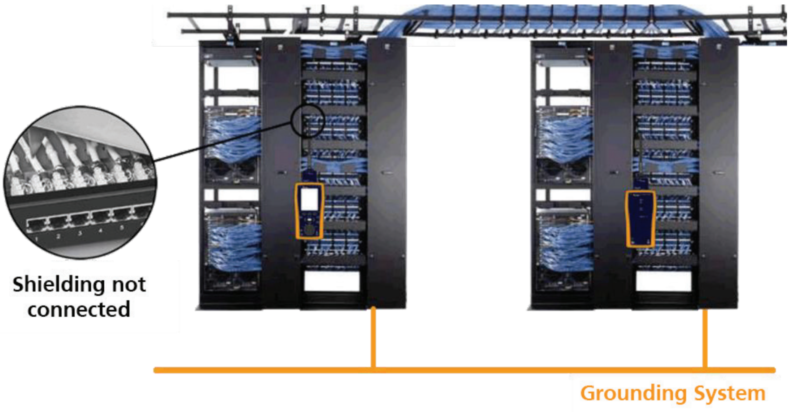
Camp B questioned this, and often employed a simplified comparison with an antenna in order to illustrate the problem and make it more easily understood.

It was also interesting that both camps substantiated their theories with practical experiments. The two passionately held opinions that were a long way away from a consensus. Agreement could be found on just one point, namely that immunity to electromagnetic interference was reduced by a good 15-20 dB. But there was no consensus on whether the remaining immunity was sufficient. The cause for concern was Alien Crosstalk (A-NEXT), or in other words, the crosstalk between one cable and the nearest parallel cable. At the lower transmission speeds in 1000BASE-T, this effect—although present and understood—could be ignored, and it was sufficient to turn the focus to the normal crosstalk between the four wire pairs within a cable. The frequency was multiplied by five with 10GBASE-T, and the increased attenuation and crosstalk that occur as a result mean that Alien Crosstalk plays an important role. There are two different ways to control Alien Crosstalk.

1. Improve the twisting and increase the distance between the cables
2. Use a braided shield, metal foil, or both

The latter is now the most common method for implementing Cat 6A or class EA cabling systems.

In this case, the shielding functions as a Faraday cage, protecting the four wire pairs from external influence. But in such a scenario, the shielding must be grounded so that the collected energy can be discharged. Without this discharge route, the shielding can become a coupling medium for crosstalk. Here, we are talking about contact between the cable shielding and 360-degree shielding contact in the RJ-45 jack. The general assumption is that a cable tester is able to test the shielding in a structured cabling system. When we group the potential environments in which a structured cabling system is used—offices, homes, data centers and in industrial automation—the latter two are clearly highly critical. In data centers, we also find the largest bundles of cables, and therefore the biggest challenge for shielding in terms of avoiding Alien Crosstalk and other electromagnetic interference. What cabling in data centers and industrial automation also have in common is that the connectors on each end of the cable are both grounded. This is what has so far prevented cable testers from checking that the wire shielding is connected correctly.



The cable tester is not able to determine whether the measured current is flowing correctly through the shielding or alternatively through the grounding system. It is not possible to determine the path by observing ohmic resistance, since one path or another may exhibit lower resistance depending on the design and the particular situation. Nor is it possible to determine the path using the transit time by comparing it with transit time in the cable pairs. This is because the transit time cannot be measured where a path is grounded at both ends. In order to do this, the ground connection would have to be interrupted. It would be necessary to remove the RJ-45 jack from the panel and isolate it.

If you want to know whether the cable tester you are using is able to measure shielding even in a grounded system, there is a simple test you can run. Take a metal patch panel, plug in two shielded modules and connect them to an unshielded cable. If the cable tester still says that the shielding is OK, we know that it is not able to test shielding correctly. This raises the question of whether such a tester is able to test cabling according to standards, or whether it meets the standard specifications for cable testers.

The standard specifications for cable testers can be found in ISO/IEC 61935-1 and TIA 1152a. In the chapter on testing cabling, earlier editions used to state that it was sufficient to test whether a galvanic connection existed between the two bushings (at each end of the transmission line).

In other words, measurement technology was not required to provide information on something for which there was no measurement solution at the time. In the latest edition of TIA 1152a from 2016 and the latest draft of ISO/IEC 61935-1, we find an additional note for testers that meet the new Accuracy Level VI or Accuracy Level 2G: "In addition, for Accuracy Level 2G testers it is understood that the screen continuity is tested along the path of the cabling". Those that define the Standards therefore assume that there is now a technical solution available for this measurement problem where there previously was none.

From a purely theoretical standpoint, it would be possible to determine whether the shielding was correctly connected by measuring the coupling attenuation in accordance with EN50289-1-15 "Coupling Attenuation Setup for Channels". However, the complexity of the measurement setup makes it undesirable. A Clamp Meter weighing approx. 15 kg and a square meter of copper plate would have to be installed in front of the patch panel, with a hole in the middle through which a patch cable is then fed. This method is also unfavorable because it is only suitable for channel measurements and not for the common permanent link measurements. On top of that, experts concluded that the method has a poor repeatability and is only suited to execute qualitative, not quantitative measurements. It would therefore only to be possible to determine whether the properties of the connection and shielding are acceptable or questionable compared to other links within the project.

Resourceful technicians and scientists have taken a completely different route to solve the problem. It is a methodology that has already been in use for several years in medicine. To detect an illness, the patient is given a full assessment and many parameters that seem barely relevant at first glance are measured, quantified and linked. Research is then conducted to see whether there is any association with an early-stage illness. This association is what physicians call a marker.

A similar approach is possible when testing shielding. When certifying a cabling system, a variety of transmission parameters are measured in accordance with the standard specifications, including insertion loss (IL), near-end crosstalk (NEXT), reflection loss (RL), attenuation-to-crosstalk ratio far-end (ACR-F), ACR, etc. The integrity of the shielding cannot be determined from these parameters. However, the previous generation of measuring devices were able to record other parameters that were not measured against a standard limit value, but were primarily used in the event of a fault — or in other words, in the event of noncompliance with the aforementioned parameters. In such cases, these additional parameters helped the user while troubleshooting and resolving the fault. Typically, it is an expert or leading technician that performs those tasks.

A twisted-pair cabling system uses four pairs of wires with a characteristic impedance of 100 Ohm. However, it is also possible to see a shielded system as eight coaxial wires, each with 50 Ohm. Other parameters are then available and the number actually triples. The latest generation of testers are also able to plot impedance and impedance variations along the cable in 100-Ohm as well as 50-Ohm systems. There are therefore an enormous number of potential markers available to test the integrity of the shielding. Developers and scientists analyzed a very large number of links with correctly and incorrectly connected shielding and it was possible—by making a connection with the complex parameters mentioned above—to isolate markers for detecting incorrectly connected shielding. The results of this research, which lasted several years, are described conceptually in patent documents and the details can of course not be published. Although the above approach is unquestionably complex, it does not increase the workload of field technicians.

As an example, Figure 2 shows open shielding 64.9 m from the main device and 0.0 m from the remote. The standard specifications for a new category of cabling system have recently been defined in TIA Cat. 8 and ISO/IEC/EN Class I. This category describes the requirements for use in the frequency range of up to 2000 MHz in order to enable data transmission rates of up to 40 Gbit/s in accordance with IEEE 40GBASE-T. In this case, the requirement from Cat. 6A/Class EA has been extrapolated from 500 MHz to 2000 MHz. The only exception is Alien NEXT, which was not extrapolated upwards from 500 MHz; instead, new and much stricter values from 1–2000 MHz were defined.

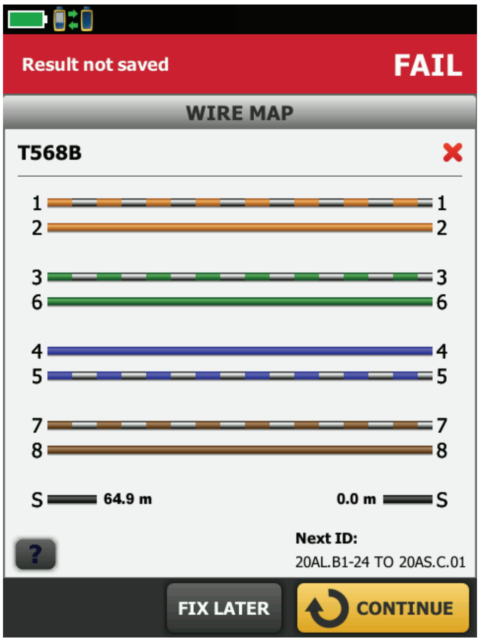


Figure 2: DSX8000/5000 WireMap

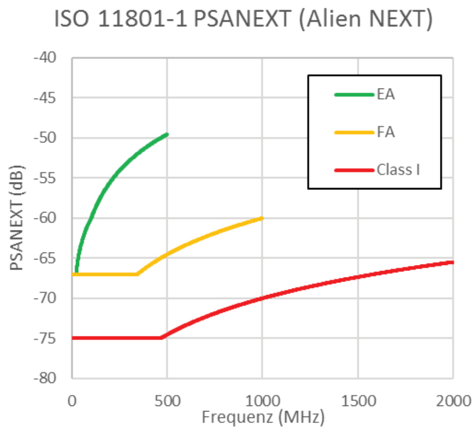
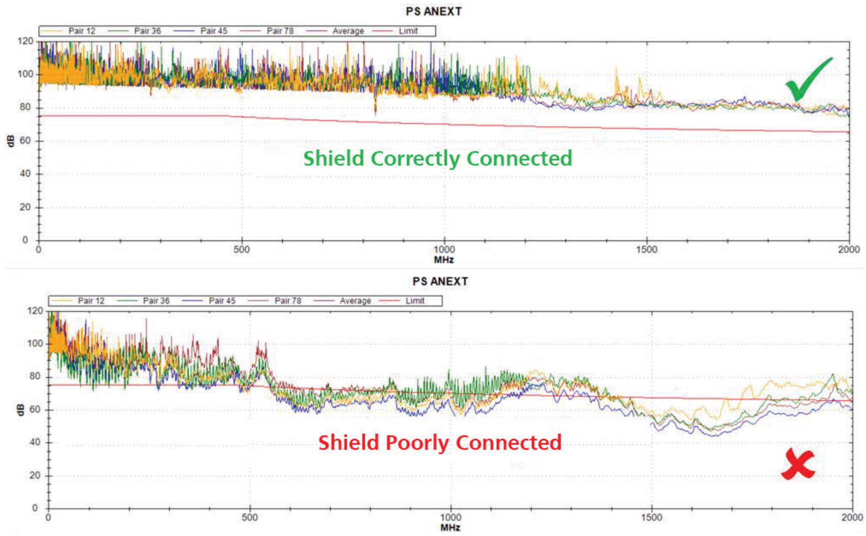


Figure 3: Requirements for Alien NEXT in Classes EA, FA and I

The importance of a correct shielding connection has become much greater. This can be demonstrated very clearly using an example.

Figure 4: Alien NEXT experiment — correct versus poorly connected shielding.



We can see that the effects of incorrectly connected shielding are fatal for Alien NEXT and the standard limit values are significantly exceeded in such cases.

In Summary:

The metallic shielding of a cabling system is comparable to a safety belt in a car: It only works when it is used correctly. Recent developments have led to a field measurement technology that is able to test whether this is the case.

About Fluke Networks

Fluke Networks is the worldwide leader in certification, troubleshooting, and installation tools for professionals who install and maintain critical network cabling infrastructure. From installing the most advanced data centers to restoring service in the worst weather, our combination of legendary reliability and unmatched performance ensure jobs are done efficiently.

For more information, visit **www.flukenetworks.com/versiv**

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

The CertiFiber Pro improves the efficiency of fiber certification with a 3 second, dual wavelength, dual fiber, test time. 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-8000 CableAnalyzer™ - Accelerates every step of the copper certification process.

The DSX-8000 CableAnalyzer improves the efficiency of copper certification with unmatched speed for testing Cat 6A, 8 and Class FA, I/II while meeting draft IEC Level VI– 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.

FI-7000 FiberInspector™ Pro - 2-second automated PASS/FAIL certification of fiber end-faces.

Graphical indication of problem areas due to contamination, pits, chips, and scratches.

Certify to industry standards - IEC 61300-3-35 and eliminate human subjectivity from end-face measurements.

More information at: ***www.flukenetworks.com/versiv***

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **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**

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**