

BECAUSE YOUR BUSINESS RUNS THROUGH US

A BERK-TEK WHITE PAPER |

Cabling for *Secure Government Networks*

Berk-Tek[®]
A NEXANS COMPANY

www.berktek.com

Cabling for Secure Government Networks

Government networks, both public and private, require cabling systems that are robust, manageable, and secure. Security forms the biggest difference between government and commercial networks since national security issues require levels of protection beyond those found in commercial applications. Both government and commercial networks use standard IT strategies such as firewalls, passwords, and restrictions on physical access to protect information. Such levels of security are sufficient for the day-to-day operations of many government agencies; but even higher levels of security are required for the private networks carrying sensitive military, security, and diplomatic communications. These types of networks are typically classified as SIPRNET (Secure Internet Protocol Router Network) or NIPRNET (Non-Classified but Sensitive Internet Protocol Router Network).

As government budgets are tightened and subject to closer scrutiny, agencies look for ways to reduce operating costs while installing secure network infrastructure to support SIPRNET and NIPRNET. There are several approved, cost-effective cabling options that meet the TIA-568C specifications while at the same time meeting the security requirements of the government.

For fiber-optic cabling networks, pre-terminated solutions and armored cabling provide the security of fiber with cost savings features over traditional fiber networks. Conversely, FTP (foil-shielded twisted pair cable) provides the most secure form of data transmission over copper networks at a cost advantage over most fiber installations. This paper will review the following:

- ▶ The advantages/disadvantages of fiber optic vs. copper cabling solutions
- ▶ Available cost savings for each type of solution
- ▶ Additional network security measures

SECURE GOVERNMENT NETWORKS

SIPRNET (Secure Internet Protocol Router Network) and NIPRNET (Non-Classified but Sensitive Internet Protocol Router Network) are private government-run networks used for exchanging sensitive information in a secure manner. SIPRNET in particular carries classified information up to the level SECRET (a medium level clearance). These systems use a protected distribution system (PDS) of copper or optical cables that are protected from unauthorized physical or electronic access.

A PDS uses RED/BLACK engineering criteria: RED media carry classified material, while BLACK media carry either unclassified or encrypted material. RED and BLACK systems are treated as separate systems, requiring them to be physically separated—different cables, different work area outlets, and different patch panels.

When the cabling infrastructure is within a secure room (e.g., SIPRNET Café), a simplified PDS can be used since the room itself is secure.

The Army's Technical Criteria for the Installation Information Infrastructure Architecture (I3A) is a leading example of standards that define, among other things, the cabling systems for Department of Defense installations. Since the manual also covers installation rules for secure systems such as SIPRNET, it is widely used by other government agencies.

One thing to note about I3A: it does not allow use of Category 6a or 7 cables as of the latest revision (February 2010). The reason is that the DoD has not fully evaluated the impact of these cables larger diameter on rules for conduit and tray fills. So the preferred copper cable for data networks is currently Category 6. Even so, Category 6a cables have compelling performance advantages—including support for higher data rates and better crosstalk performance—that make them a better long-term choice. Once evaluation is complete, Category 6a cables will undoubtedly be approved for use.

When installing the infrastructure for SIPRNET or NIPRNET, it is important to review both fiber and copper cabling options.

THE CASE FOR FIBER

Optical fibers are the most secure cabling choice since they neither emit nor receive electromagnetic energy. Fibers do not experience internal or alien crosstalk, which could allow unauthorized access to the data being transferred. Eavesdropping on a fiber-based network would require physical access to the fiber and, even then, presents a more challenging task to tap the fiber undetected.

Single-mode fiber in backbones and outside plant and multimode fiber in horizontal runs are standard deployment for optical fiber. Laser-optimized multimode fiber (OM3/OM4) is the most flexible choice, combining high bandwidth and compatibility with low-cost transceivers to support 10 Gb/s transmission beyond standards-based 300 m to 550 m for OM4 fiber. Figure 1 shows allowable cable distances for both copper- and fiber-based cables.

The drawback is that fiber-based systems, including the electro-optic transceivers in the equipment, are usually more expensive than their copper counterparts based on material costs and installation costs. You should, however, carefully evaluate both initial and lifetime costs between fiber and copper. Highly secure copper networks have additional considerations, such as electrical metallic conduit, shielded cables, and other factors, that can make copper networks more expensive. Optical prices are moderating. The bottom line is that conventional wisdom—copper is cheaper than fiber—merits a more careful look.

Category 6A UTP	100 m	<i>Maximum cabling Distance at 10 Gb/s</i>
OM3 MMF		300 m
OM4 MMF		550 m

Figure 1. The choice of cable affects the maximum distance of the channel.

PRETERMINATED FIBER OPTIC CABLES SPEED INSTALLATION

Even with the advances made in fiber-optic connectors to allow fast termination—including versions requiring no epoxy and no polishing—field termination of optical cable is often considered a costly burden and something many contractors wish to avoid. The fiber-termination toolkit typically includes multiple stripping tools for jackets and fibers, scissors for cutting jacket and strength members, crimping tool, polishing pad, polishing puck and plate, such consumables as polishing papers and epoxy, inspection microscope, and tester.

Factory-terminated cable assemblies (Figure 2, page 4) offer a cost-effective alternative to field termination. The assemblies offer faster installation by eliminating the termination procedure. Time savings typically run 20% to 30%, but can range as high as 75% with epoxy/polish connectors that require oven curing of the epoxy.

The best suppliers of preterminated assemblies not only used advanced processing to ensure the precision end-face geometry required for high-quality terminations, they also test 100% of the assemblies to ensure they meet performance requirements. Assemblies are supplied fully documented and labeled. This combination of advanced processing and final testing yields

cable assemblies with performance headroom above the minimum requirements of standards. Not only is performance improved, but is more consistent from one assembly to the next: there is much less variation in performance than you typically experience with field termination. The improved performance means lower end-to-end attenuation and improved link budgets.

Ready for immediate deployment, they can also lower installation costs. There's no on-site termination, no cable or connector scrap, and no termination errors.

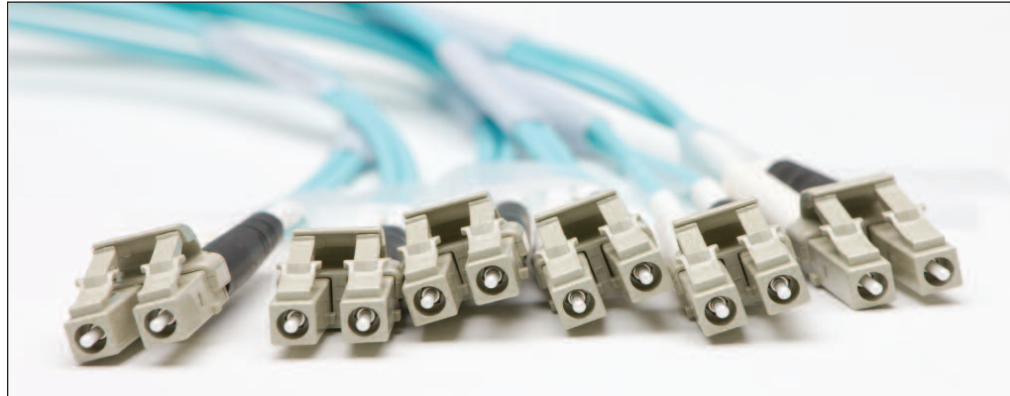


Figure 2. Preterminated cable assemblies offer superior performance and faster installation.

ARMORED OPTICAL CABLES PROVIDE PHYSICAL PROTECTION

Another cost savings can be the use of armored fiber-optic cables (Figure 3, page 5). These cables are manufactured in a sturdy, intruder-resistant interlock armor. Armored cables can be used in place of innerduct and conduits, providing a user-friendly, one-pull alternative to the expensive and labor-intensive installation process of conduits. By installing armored fiber cables instead of plenum innerduct or conduit, savings can run from 25 to 50% in materials, and reduce costly installation time and labor costs as much as 60%—a significant advantage over traditional installation methods. Additionally, armored fiber optic cables are not governed by fill ratios because they are UL listed as cable assemblies, allowing a higher concentration of cables in an area compared to conduit.

High-quality armored cable, using either steel or aluminum spiral-wrapped armor with a plastic UV-resistant sheathing, also remains flexible for easy installation and on-going maintenance. Plus, they are available in a wide range of fiber types and counts.

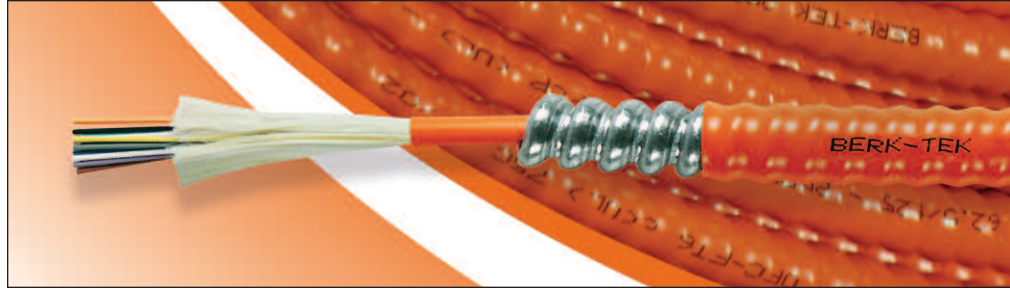


Figure 3. Armored cables prevent access and can replace the cost and complexity of innerduct.

ALARMED CARRIER EASES PDS BURDEN

Security, especially for RED systems, generally requires that they are subject to periodic visual inspections—daily or more often—to ensure the integrity of the system. This requires that cable runs be visually accessible, not behind wall or under floors. Even above a drop ceiling is not recommended because of the difficulty of inspection. Pathways require electrical metallic tubing (EMT) or sealed metallic raceways as part of the PDS. EMT not only adds another layer of shielding to prevent emissions, it provides physical protection against intruders. The drawback is the added costs and unsightly installation that such approaches offer.

An alarmed carrier eliminates the need for visual inspections and allows optical cable to be installed in a “normal” manner, behind walls and the like. An alarmed carrier monitors the fibers within the cables being protected, essentially turning the cable into sensors that can detect any attempts at tampering. Such monitoring devices allow armored cable to replace EMT and metallic raceways.

KEYED CONNECTORS SEGREGATE NETWORKS

Not only do RED and BLACK networks have to be kept physically separate, but mixed-use facilities must also have separate systems. For example, if the National Guard and the Army Reserve share a facility, each must have its own network.

While I3A specifically mentions the SC connector, it does not rule out small-form-factor connectors like the LC. LC connectors, being roughly half the size of the SC, offer double interconnection densities in patch panels. MTP array connectors can be used for multifiber backbone applications.

LC and MTP connectors are also available in physically keyed and color-coded variations (Figure 4). Each separate network can use its own color/key. Red keyed plugs mate only with red keyed receptacles. The keying is tamperproof so that networks with different security levels or users can be confidently co-located by assigning each its own keying combination. While the number of key combinations varies with the vendor, as many as 12 different arrangements are available.

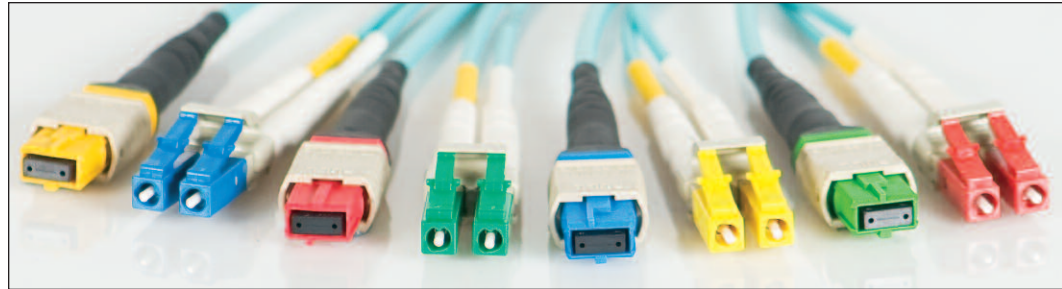


Figure 4. *Secure connectors allow networks to be segregated by functions, levels of security, or other needs.*

THE CASE FOR COPPER

Even with the advantages of optical fibers in bandwidth and security, copper cabling is still the most widely used. It is considered less expensive, better understood, and easier to work with. To achieve the best possible performance over copper cabling, it is wise to use the highest category of cable. In UTP cable, noise susceptibility is a function of the quality of the balance in the cable. A perfectly balanced cable is less sensitive to external noise. Any noise picked up is of equal magnitude but opposite polarity on each conductor of the pair. The receiver cancels the noise. Small nonuniformities in the cable's physical construction mean the balance is not perfect. Noise then affects the ability of the receiver to distinguish the desired signal. As cable design has evolved from Cat 3 through 5, 5e, 6, and 6A, high-quality cable manufacturers have ensured that each succeeding generation of cables has offered better balance and therefore better noise immunity.

As network speeds evolved to 10 Gb/s, alien crosstalk became a factor in cable and network performance. Up through Category 6, crosstalk was measured only between pairs in the same cable. Alien crosstalk is that coming from an adjacent cable and can be a significant impairment at 10 Gb/s and higher. With Category 6A, alien crosstalk specifications were added to the TIA-568C standard. Category 6A cable allows the full channel distance of 100 m at 10 Gb/s. Category 6 cable, on the other hand, was never designed to prevent alien crosstalk and therefore has a limited ability to support 10GBASE-T.

SECURITY-KEYED CONNECTORS AND CABLE ASSEMBLIES

As with fiber, copper cables are available with keyed connectors to segregate networks securely. Preterminated copper cable assemblies are also available, with benefits similar to optical assemblies such as arriving at the job site pre-tested and guaranteed by the manufacturer. In considering the choice between field termination and preterminated cable assemblies, keep in mind that the higher the category of cable and connectors, the more sensitive it is to poor application.

FOIL SHIELDING ADDS TO SECURITY

The addition of a foil shield surrounding the cable core improves alien crosstalk performance in two ways. First, the shield forms a ground plane which improves the balance of the cable. Second, it adds shielding attenuation, which is the reduction of the radiated energy caused by the shield. As shown (Figure 5) for Category 6 cables, shielding adds next to nothing to the cable's diameter.

As such, shielding can virtually eliminate external signal detection and interception. At worst case, shielded cabling emits less than one half of one percent (<0.5%) of the power radiated by UTP cabling.



Figure 5. Foil-shielded cables offer better security, adding just over one millimeter in outside cable diameter.

A best practice for shielded cable is to carry the shield to earth ground. Most often this can be accomplished through the patch panel to the rack, which is bonded to ground. A shield functions best when it provides a path to ground for the noise it picks up. Some people believe that grounding the cable at only one end is preferable to prevent ground loops. A ground loop can occur when the equipment at each end is grounded at a different ground potential. A well-designed ground system, however, should be earth grounded on at least one end to ensure proper shield performance.

Shielded cabling systems do increase the overall cost of the system, both in the component costs of the cable and connectivity and the installation labor. But the additional level of signal isolation and protection offered by shielded cabling systems makes them ideal candidates for secure networks.

CONCLUSION: SMART PLANNING FOR SMARTER COST CONTROL

Designers of secure government networks have several options when it comes to cabling systems. The level of security required by the agency being supported and the sensitivity of the information being transported will affect the design as well as the cost of the final system and the budget of the agency. The need for highly secure SIPRNET network can direct the designer toward options like keyed connectors and alarmed carrier fiber networks, while a NIPRNET network may be supported with a shielded copper cabling system. Cost can also be an influencing factor in network design.

However, costs can be controlled without compromising security in government networks. By carefully evaluating both the needs of the installation and the options available to reach those goals, contractors can create networks that offer better performance, excellent security, and lower costs.

CONTACT INFORMATION |

Corporate Headquarters

132 White Oak Road
New Holland, PA 17557
USA

TEL: 717-354-6200

TEL: 800-237-5835

FAX: 717-354-7944

www.berktek.com

In Canada, please contact:

Nexans Canada Inc.
140 Allstate Parkway
Markham, Ontario
L3R 0Z7 Canada

TEL: 905-944-4300

TEL: 800-237-5835

FAX: 905-944-4390

www.berktek.com