We Bring Security To Light™

Interceptor™ Alarmed Carrier PDS Provides Information Assurance Benefits for National Security Information on SIPRNET and JWICS Networks

A White Paper from the Interceptor™ Product Team at Network Integrity Systems

Overview

With the explosion of SIPRNet and classified information systems throughout DoD and civilian government agencies, the potential vulnerabilities and resulting need for compensating measures to protect our National Security Systems has increased exponentially. With the amplified focus on Information Assurance, the Interceptor™ Optical Network Security System is being increasingly leveraged due to its ability to reduce the cost and complexity of network deployments while also significantly enhancing network security and information assurance.

Discussion

The Committee on National Security Systems and NSTISSI 7003 provide the overarching national guidance to all DoD and civilian agencies for the protection of wireline and optical fiber Protective Distribution Systems (PDS) used to transmit unencrypted National Security Information. Per NSTISSI 7003 "…the emphasis of a PDS should be placed on 'detection' of attempted penetration in lieu of 'prevention' of penetration."

With the recent growth of secure networks, the requirement to perform PVIs places a severe strain on manpower and results in infrequent or potentially neglected visual inspections – especially during crises or periods of high operations tempo.

Because of the emphasis on detection, Hardened Carrier PDS installations constructed of rigid metallic conduit (EMT, Holocom® PDS, Wiremold Data Fence® Secure Raceway, etc.) require the owning organization to conduct daily periodic visual inspections (PVIs) as the sole means to detect unauthorized access or tampering with the PDS. The required PVIs must be conducted on the entire PDS infrastructure – with a 360-degree view – throughout the facility.

From an IA perspective, the goal of the PVI is to minimize the amount of time and exposure that takes place between the point-of-compromise (penetration, tampering, etc.) and the point-of-detection. When SIPRNet deployments were limited in number, owning agencies could easily satisfy PVI requirements. However, with the recent growth of secure networks, the requirement to perform PVIs places a severe strain on manpower and results in infrequent or potentially neglected visual inspections – especially during crises or periods of high operations tempo. With the increased focus on audits and record keeping needed to satisfy the requirements of the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), even more importance is placed on the consistent performance of PVIs and accurate logs and/or record keeping.

To conduct the required PVIs, the PDS must be installed below the ceiling and in plain view. However, this makes the PDS obvious and readily accessible to any and all building occupants and visitors and ultimately more vulnerable to overt and covert attacks.

Furthermore modular raceway PDS systems such as Holocom and Wiremold are designed to be re-enterable to allow these systems to easily allow moves, adds and changes in order to support the rapid growth in secure networks. However this feature creates an additional vulnerability since it makes it easier for unauthorized individuals to enter the systems. In response, most agencies and services have established compensating measures such as the epoxying of all seams (as specified in NSTISSI 7003 for EMT) or through a more encompassing visual inspection procedure which, in order to perform properly, requires specialized training provided through a third party.

Alarmed Carrier PDS addresses the primary intent of NSTISSI 7003 (detection) by replacing the PVIs with continuous monitoring of the raceway. This results in substantial savings in manpower – but more importantly, it eliminates the risk that an intrusion into the PDS goes unnoticed due to infrequent or neglected human inspections.

Alarmed Carrier PDS addresses the primary intent of NSTISSI 7003 (detection) by replacing the PVIs with continuous monitoring of the raceway. This results in substantial savings in manpower – but more importantly, it eliminates the risk that an intrusion into the PDS goes unnoticed due to infrequent or neglected human inspections. Attempts to penetrate the carrier system are discovered and logged immediately by the monitoring system, giving the intruder no time to do harm and thereby maximizing the potential for the intruder to be detected.

In addition, the alarm system provides a consistent and persistent log of events, which ensures compliance with DIACAP. A key advantage is that the alarm system provides persistent protection, and only notifies personnel to perform an inspection in order to investigate potential suspicious activity. This typically results in only a few inspections per month instead of conducting visual inspections each and every day whether a threat to the network exists or not.

Since alarming the PDS eliminates the requirements to perform daily visual inspections of the PDS, the resources formerly used to conduct that task can be assigned to other activities, while they stand by to respond to any alarms that might occur. The Interceptor includes features that enable it to send alarms in a variety of ways so multiple organizations (IT, security forces, NOSCs, etc.) can receive notifications and respond accordingly.

Since visual inspections are not required for an alarmed PDS, the rigid metallic carrier system can be placed in a non-visible location (i.e. below the floor or above the ceiling), which makes it much more difficult for a would-be intruder to gain access. This provides a further benefit of masking the presence of the classified network therefore making an assault even more difficult. Since the carrier is out of sight, simple EMT can be used versus more expensive modular raceway products.

Unlike traditional alarm carrier systems that monitor attacks on the raceway, the Interceptor Optical Network Security System monitors fibers *within* the cables being protected, making the entire cable sensitive to abnormal manipulation and handling.

When the threat level warrants it, some agencies and military branches deem as a compliant PDS, flexible interlocking armored cables monitored by an Interceptor, installed without a rigid metallic carrier. This allows the network cables to be distributed in existing conveyance (wire basket, ladder rack) or as suspended cabling (on D-rings, J-Hooks, etc.). The robust interlocking armor provides a high degree of physical protection, while the Interceptor performs continuous "inspections." Not only does this result in tremendous cost benefits achieved through the elimination of materials and labor to construct a metallic raceway system, it also enhances security because the classified network cables are now no longer obviously pinpointed (inside a hardened carrier PDS) and can be installed higher up in the ceiling, making access very difficult and only possible with the use of a ladder and specialized tools needed to breach the very robust armoring.

A further benefit of the Interceptor PDS and Armored Cable solution is the fact that network cabling, with its continuous protective armor, can now be run from point-to-point with no vulnerable access points at various junctions along the PDS.

Conclusion

An alarmed PDS offers significant advantages over a traditional hardened PDS by automating the inspections necessary to ensure that any penetration is detected, while still providing the robust physical protection of rigid metallic conduit capable of being placed out of sight. When conditions are acceptable, the expenses of a rigid metallic carrier system can be avoided altogether with the use of a monitoring system such as Interceptor and flexible interlocking armored cables, leading to tremendous cost savings and enhanced security.

About Network Integrity Systems, Inc.

Network Integrity Systems specializes in solutions for the protection of secure networks and critical infrastructures. Network Integrity Systems is also a founding partner of Communication Supply Corporation's Secure(it) program – focused on enhancing the security and availability of high assurance networks and facilities throughout the Department of Defense and federal government.

Network Integrity Systems
1937 Tate Blvd. SE
Hickory, NC 28602
877-NIS-4PDS
info@networkintegritysytems.com

www.networkintegritysystems.com