WESCO®

Advanced Alarmed PDS Technology

Meeting the Demand for Compliant, Secure Classified Network Deployments

Amanda Simpson, Manager, Network Integrity Systems

NetworkIntegrity SYSTEMS

Advanced Alarmed PDS Technology

Meeting the Demand for Compliant, Secure Classified Network Deployments

Summary

With the growing need for access and cost efficiencies, classified networks need to be cheaper, faster, more aesthetically and environmentally pleasing and of course more secure than what had previously been achieved with hardened PDS and Type-1 Encryption. This paper will review Advanced Alarmed PDS Technology which overcomes the shortfalls of other technologies and will discuss deployment within various applications such as Point-to-Multipoint, Encryption Replacement, and Secure-PON with case study examples for each type.

Contents

Meeting the Demand for Compliant, Secure Classified Network Deployments	3
Need: Cheaper, Faster, Aesthetically and Environmentally Pleasing and More Secure Network Connections	3
Solution: Advanced Alarmed PDS Technology (APDS)	3
Typical Advanced Alarmed Carrier PDS Applications and Actual Deployment	4
LAN Point-to-Multipoint or “SIPRNet to the Desk” Deployments	4
Example: Centrally Managed Alarmed PDS	5
Example: Passing Command Cyber Readiness Inspections (CCRI) to Obtain and Maintain Authority to Operate (ATO)	5
Building-to-Building (OSP) Deployments	5
Example: APDS in a Base-wide Building-to-Building (OSP) Deployment	6
Encryption Replacement	7
Example: Type-1 Encryption Replacement to Enable Network Full Bandwidth	7
Secure Passive Optical Networking (Secure-PON)	7
Example: Secure PON	7
The Answer	8
About Network Integrity Systems	8
About WESCO	8

ABOUT THE AUTHOR

Amanda Simpson is the Manager, Marketing Communications for Network Integrity Systems (NIS). Amanda joined NIS in 2007 and since then, has led NIS’ efforts in educating the US Government and military and most recently, the private enterprise market on the benefits of Alarmed-Carrier PDS technology and network infrastructure protection.

Advanced Alarmed PDS Technology:

Meeting the Demand for Compliant, Secure Classified Network Deployments

Need: Cheaper, Faster, Aesthetically and Environmentally Pleasing and More Secure Network Connections

U.S. Government and private enterprises performing work for the U.S. Government, where national security information is communicated via their private networks, must adhere to certain regulations to obtain and maintain an Authority to Operate (ATO) the networks. A significant component of these regulations is verification that an authorized method for assuring the confidentiality, integrity, and availability of the information transmitted over the network is in-place. A common security practice is to utilize NSA approved Type-1 encryption devices within the network. However, there are several disadvantages associated with the use of Type-1 encryption such as:

- high cost,
- network bandwidth restrictions,
- un-acceptable lead-times to acquire equipment and
- cumbersome encryption-key management processes.

When encryption is not in-place, these organizations must comply with National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Protective Distribution Systems (PDS), which provides guidance for the protection of wireline and optical fibers transmitting unencrypted national security information. In many cases however, the traditional PDS methods to protect the infrastructure cannot scale with today's demand for access to classified networks. Hardened PDS, which requires installing unencrypted cables inside of metallic raceway:

- has become cost prohibitive,
- detracts from building aesthetics, and
- requires an extensive amount of time for installation that is disruptive to personnel and operations within the facilities.

Furthermore, once the raceway is installed, it requires DAILY visual inspection along the entire PDS system to ensure the security of the network. All of this leaves information assurance managers searching for solutions that significantly reduce the time, cost and complexity of secure network deployments and provides long-term scalability and long-term flexibility to meet on-going changes in mission and organizational structure.

Solution: Advanced Alarmed PDS Technology (APDS)

Advanced Alarmed PDS technology (APDS), such as the industry leading INTERCEPTOR™ Optical Network Security System, from Network Integrity Systems (NIS), is NSTISSI 7003 compliant, and, unlike legacy PDS systems, supports the growing demand for connections to classified networks while offering cost savings, enhanced security and the situational awareness required in today's environment. APDS systems have been deployed across the globe protecting U.S. Government classified networks up to the TS/SCI level, including SIPRNet, JWICS, and in high threat level environments.

Figure 1: Advanced Alarmed PDS Technology

APDS systems monitor spare fibers contained within the cables requiring protection, making the entire cable a sensor capable of detecting any unauthorized tampering with the infrastructure. Best-of breed APDS systems use technology to eliminate false alarms by learning the normal day-to-day activity within the environment.

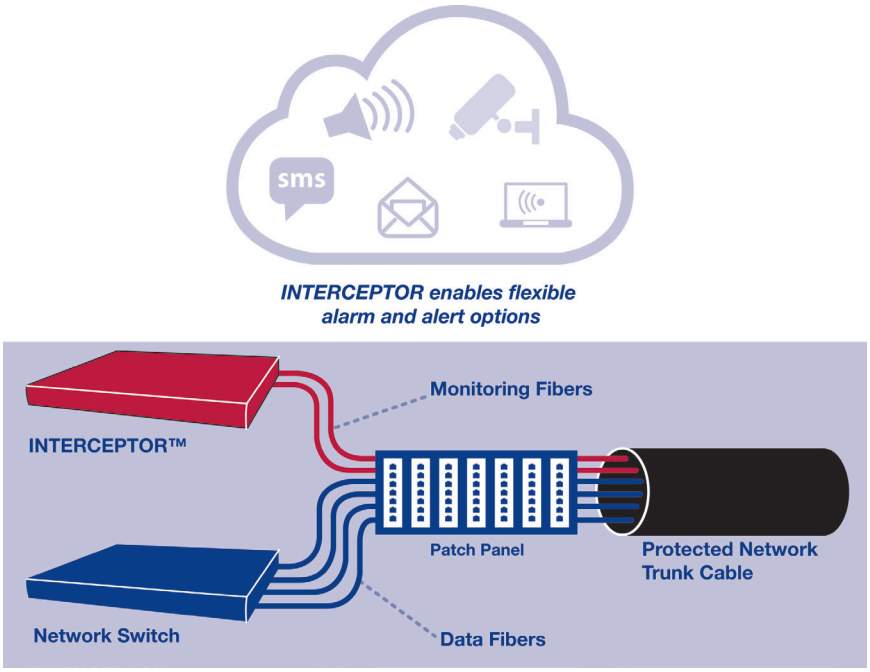


Figure 2: Advanced Alarmed PDS Technology Monitors Fibers Within the Cables Requiring Protection

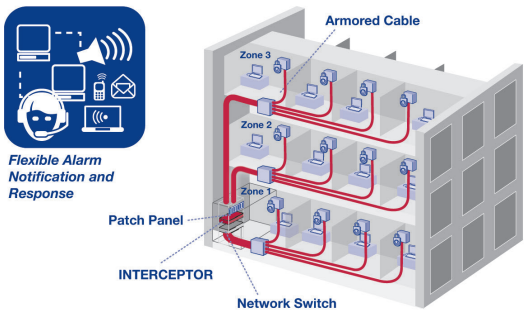
APDS technology enhances network security and lowers operational costs through the replacement of the unreliable, daily human visible inspection process required to secure traditional Hardened PDS, with automated 24/7/365 monitoring. This results in improved building aesthetics because with the elimination of inspections comes the authority to remove unsightly PDS from the wall and conceal it above the ceiling or below the floor. In some cases, APDS systems can be used along with a flexible interlocking armored cable infrastructure to eliminate all requirements for EMT or rigid metallic conduit systems, resulting in significant material cost savings. Leading APDS systems support multiple integration options for responding to alarms and managing Standard Operating Procedures (SOP) associated with an alarmed-PDS.

While encryption is an effective method for the protection of information across long-haul or metropolitan area networks, an increasing number of DoD units and other government agencies are realizing the benefits of APDS and utilizing the solution to meet the guidance of NSTISSI 7003. APDS is being used, not only in lieu of encryption, but also as a replacement of existing encryptors in many places around the world, as encryption has become A) too cost prohibitive especially for higher speed networks, B) too limiting to network performance, and C) too time consuming to manage given the Public Key Infrastructure and COMSEC issues associated with it. As a physical layer device, APDS protects the integrity and availability of network circuits transporting national security information-while offering unrestrained bandwidth and significant cost savings.

Typical Advanced Alarmed Carrier PDS Applications and Actual Deployment

LAN Point-to-Multipoint or “SIPRNet to the Desk” Deployments

Because APDS monitors the fibers within the cables carrying the classified data (intrinsic monitoring), point-to-multipoint (hub-and-spoke) monitoring architectures can be created to mimic the physical network allowing efficient utilization of the monitoring device’s ports permitting high-density, logically clustered groups of protected SIPR drops. This allows multiple offices or workstations to be protected by a single alarm system port rather than each office or workstation requiring its own port. Use of this architecture enables many dozens of end-user drops to be protected by one alarm device. This results in cost reductions of 75% or greater per drop when compared to legacy protection methods.



$

- *If using Alarmed-Armored PDS, all epoxy and conduit is eliminated*
- *Multiple drops per zone; reducing costs per secure drops*
- *Integration options include Facility IDS, Network Management Systems, and Mobile Devices*
- *No end-to-end daily inspections*
- *Concealed classified infrastructure; no conduit exposed in hallways and office spaces*
- *Scaleable and flexible infrastructure*
- *No rigid metallic conduit*
- *Highly secured by 24/7/365 real-time monitoring with Smart Filtering™ to eliminate false alarms*

Figure 3: Point-to-Multipoint Deployment with INTERCEPTOR, the leading APDS Solution

Example: Centrally Managed Alarmed PDS

When a prominent U.S. Army Europe, Command Center headquarters building was designed, the network cable infrastructure security requirements were overlooked. Specifically, the network infrastructure and cabling was installed beneath the floor, which consisted of large, heavy stone tiles cemented to a substructure, making it practically impossible to implement a traditional PDS plan with the associated daily visual inspections necessary to insure the security of the PDS. As a result, when the building went operational, personal escorts were required for all visitors without a security clearance who required access to the areas where the unsecured cabling resided. This process was time consuming, costly and most important, a security risk.

The command solved the security challenge by placing optical fibers in the cable trays under the floor and then alarming those fibers with NIS's INTERCEPTOR, the industry leader in APDS. This "extrinsic" monitoring application of INTERCEPTOR alleviated the need to perform the daily visual inspections, which were incapable of being performed in the first place, and eliminated the need for escort personnel. The INTERCEPTOR solution was integrated with a centrally managed Alarm Response Management System, which responds to alarms and manages standard operating procedures 24/7/365, as well as generates case resolution and audit trails; all of which simplifies Information Assurance Management.

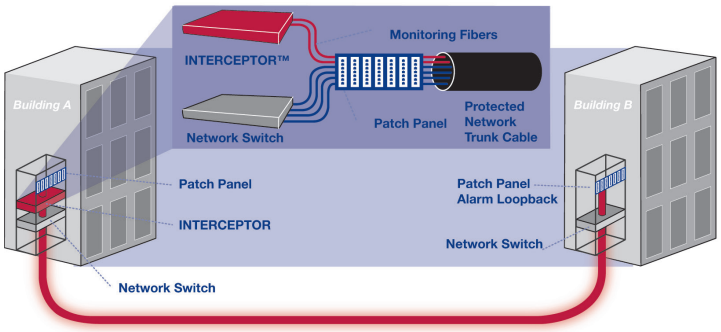
Example: Passing Command Cyber Readiness Inspections (CCRI) to Obtain and Maintain Authority to Operate (ATO)

Private enterprises performing contractual work for the U.S. Government in projects where National Security Information is communicated via the contractor's private network must undergo Command Cyber Readiness Inspections (CCRI) to obtain and maintain an Authority to Operate (ATO) the networks. Two industry leading government defense contractors, each working on mission critical projects, failed their (CCRIs) due to non-compliant PDS, leaving them unable to connect to the classified government network and exchange information necessary for the performance of their contracts. Over the years, NIS has seen this scenario on many occasions.

Both defense contractors selected NIS's INTERCEPTOR solution to rapidly and cost-effectively solve their accreditation issues. Within thirty days after making original contact with NIS, their PDS was compliant and they had gained their ATO. The INTERCEPTOR was integrated with a centrally managed Alarm Response Management System, which responds to alarms, creates site-specific standard operating procedures, and generates case resolution audit trail. The Information System Security Managers responsible for these networks now have the ability to monitor and protect the physical security of their network infrastructure. In addition, they can implement site-specific NSTISSI 7003 compliant operating procedures and generate unique case resolution audit trails, simplifying information assurance management and PDS inspection. This is possible with no bandwidth constraints on the network and a total deployment cost that was significantly less than other alternatives.

Building-to-Building (OSP) Deployments

In lieu of spending hundreds of thousands of dollars to encase conduit runs in concrete, APDS can protect those same links for a fraction of the cost. Multi-port APDS products can protect up to four separate cable runs (even more through point-to-multipoint design) or remain available for deployment to protect future SIPRNet requirements as they occur – with no additional cost or delay. APDS also alleviates the requirement of locked or alarmed manholes that are typically required even when concrete encasement is not required.



$

- *Only 1 INTERCEPTOR port to secure each Building-Building link*
- *Options for securing multiple network classifications per INTERCEPTOR port*
- *Full bandwidth utilization – INTERCEPTOR has no impact on bandwidth*
- *Easily reconfigurable to add new, relocate or reconfigure network links and classifications*
- *Integration options include Facility IDS, Network Management Systems, and Mobile Devices*
- *No end-to-end daily inspections (PVIs)*
- *Highly Secured by 24/7/365 real-time monitoring with Smart filtering™ to eliminate false alarms*
- *INTERCEPTOR Plus provides the unique capability to monitor active data fibers if no dark fiber for alarming available.*

Figure 4: Building-to-Building Deployment with INTERCEPTOR, the leading APDS Solution

Example: APDS in a Base-wide Building-to-Building (OSP) Deployment

APDS presents a major cost savings for protection of building-to-building cable links across military bases and defense industry contractor campuses. NSA Type 1 Encryption and Hardened Protected Distribution Systems (PDS), in the form of concrete encased duct banks, were the primary methods used for outside plant cable system security prior to the availability of APDS. For the sake of discussion, we will assume a large base of operations with 150 buildings.

Hardened PDS consisting of concrete encased duct banks (the NSTISSI 7003 guidance) would be very costly (labor and materials) and disruptive (excavation) to base operations. Assuming an average distance of 200 meters from the POP (point-of presence, or the facility in which information traffic first enters the base) to end-user buildings, and an installation cost of $100 or more per meter, the total cost to encase the duct banks is approximately $3 million. A single APDS unit can provide a secure uplink to a minimum of four end-user buildings. In the case of this base, using INTERCEPTOR in lieu of Hardened PDS for SIPRNet deployment to the 150 buildings would have cost approximately $675,000 or approximately 75% savings.

Hardened PDS	
Buildings	150
Meters Btwn	200
Total Meters	30,000
Cost/Meter	$100
Total Cost for Hardened PDS	**$3,000,000**

ENCRYPTION	
Buildings	150
Cost/Building	$10,000
Total Cost for Encryption	**$1,500,000**

INTERCEPTOR (ADPS)	
Buildings	150
Cost/Building	$4,500
Total Cost for INTERCEPTOR	**$675,000**

Encryptors cost approximately $10,000 each, with one unit required at each building. The total cost of the SIRPNet deployment would be $1.5 million. Since INTERCEPTOR protects the entire cable, as additional fiber pairs are utilized to transmit classified information; they are automatically protected with no further equipment needed. The cost of INTERCEPTOR is about half that of encryption when only two fibers are being secured by encryptors to each building. As encryptors are added to additional fiber pairs, the cost for INTERCEPTOR reduces again by half each time. As previously stated, in this scenario, INTERCEPTOR would have cost approximately $675,000, making it a 50% savings over encryption. In addition, as a physical layer device, INTERCEPTOR does not touch, process or verify the network data, therefore, no bandwidth bottlenecks occur as it does with encryption.

Savings using INTERCEPTOR (ADPS) vs. Hardened PDS = 78%

Savings using INTERCEPTOR (ADPS) vs. Encryptor = 55%

Encryption Replacement

Transitioning from encryption to APDS provides a quick way to upgrade performance and security, while reducing long-term costs. In fact, many units that have previously deployed encrypted connections 'tunneled' across unclassified networks are now being challenged by approval authorities to re-assess the protection being provided to both the information and the network infrastructure.

Similar to SIPRNet tunneling across campus area networks with network encryptors, APDS can be installed on existing NIPRNet cables using spare fibers to create a protected sub-unit that can then be used to tunnel SIPRNet traffic at speeds that are unconstrained (ex: 10 Gig and beyond) at a fraction of the cost. Once APDS is used to monitor an individual sub-unit of a cable, all of the fibers in that cable are protected cable and can be used for SIPRNet traffic, unlike encryption, which requires an individual encryptor for each pair of transmitting fibers. This drastically reduces the cost per port for a deployment.

Example: Type-1 Encryption Replacement to Enable Network Full Bandwidth

An operating base located in Africa, serves as the hub of a network of American drone bases in eastern Africa. Drone operations rely heavily on real-time video transmissions – demanding constant high bandwidth availability from the network. The 10GBS network installed at this base was being secured with Type-1 Encryption devices designed for gigabit network speeds, due to cost and availability constraints associated with 10G encryptors. As such, the network's bandwidth was typically degraded to 1 Gigabyte or less creating issues associated with video transmissions necessary for the completion of the base's mission. The command changed their security strategy from encryption to APDS and installed NIS's INTERCEPTOR APDS solution throughout the base. The solution provided the base with access to the full bandwidth capabilities of the network. In addition, the burdensome processes associated with encryption management were eliminated, giving base personnel time back to spend on other mission requirements.

Secure Passive Optical Networking (Secure-PON)

Passive Optical Networks (PON) provides high-speed, high-bandwidth and secure voice, video and data service delivery over a combined fiber network. Since a typical PON is a combination of the entire aforementioned APDS applications, APDS is perfectly suited for deployment within a PON to meet NSTISSI 7003 requirements. APDS is also the easiest and most cost effective solution available to secure and protect critical network infrastructure used for PON transport.

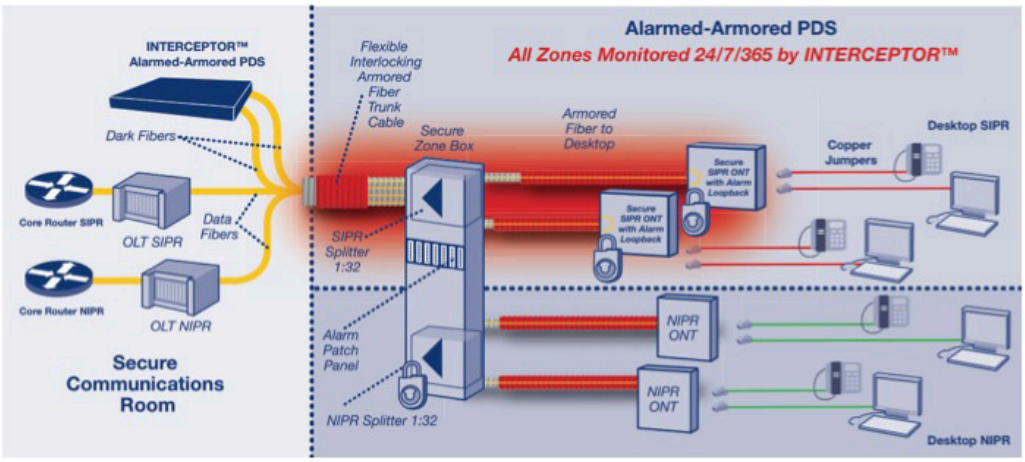


Figure 5: Secure PON with INTERCEPTOR, the leading APDS Solution

Example: Secure PON

In 2012, US Army's Network Enterprise Technologies Command (NETCOM) needed to optimize deployment of voice, video and data services to the desktop at the headquarters located at Fort Huachuca. NETCOM solicited industry for acquisition of a high-bandwidth network, which had to be secure, reliable, cost-effective and environmentally friendly. Most of the

building required classified network access – with the additional requirement that the entire building be scalable to support the classified network in the future while meeting NSTISSI 7003 requirements. The Secure PON solution, which included INTERCEPTOR, met every requirement as it delivered the immense performance and feature benefits of Gigabit Passive Optical Networking (GPON) technology, with the cost-effective and highly reliable infrastructure security enabled by APDS.

The Answer

With the increased deployment of secure networks by the U.S. Government and U.S. Military as well as private enterprise doing work for these entities, organizations deploying secure network connections today want a solution that:

- Reduces time and cost
- Simplifies secure network deployments
- Provides long-term scalability and flexibility to meet mission and organizational changes.

The answer: Advanced Alarmed PDS technology, the inherently more secure solution that is also cheaper, faster, and more aesthetically and environmentally pleasing. And when selecting the INTERCEPTOR Optical Network Security System from NIS, you are choosing the device that has been deployed across the globe and relied on to protect U.S. Government and Military networks for over a decade.

Network Integrity Systems, Inc., (NIS) is the industry leader in Advanced Alarmed PDS Technology. Our flagship product, the INTERCEPTOR Optical Network Security System is the only Alarmed Carrier PDS system developed specifically for data security. INTERCEPTOR has recorded over 80 million port hours protecting classified U.S. Government networks up to the TS/SCI level including SIPRNet, JWICS, and in high threat level environments.

About WESCO

WESCO International, Inc. (NYSE: WCC), a publicly traded Fortune 500 holding company headquartered in Pittsburgh, Pennsylvania, is a leading provider of electrical, industrial, and communications maintenance, repair and operating ("MRO") and original equipment manufacturers ("OEM") product, construction materials, and advanced supply chain management and logistic services. 2014 annual sales were approximately $7.9 billion. The Company employs approximately 9,400 people, maintains relationships with over 25,000 suppliers, and serves over 75,000 active customers worldwide. Customers include commercial and industrial businesses, contractors, government agencies, institutions, telecommunications providers and utilities. WESCO operates nine fully automated distribution centers and approximately 485 full-service branches in North America and international markets, providing a local presence for customers and a global network to serve multi-location businesses and multi-national corporations.

Additional resources developed by WESCO Government Team: www.wesco.com/government/resources.htm
For more information on APDS technology, please contact our technical team at secure-it@wesco.com or visit us online at www.wesco.com/secureit

---

HEADQUARTERS
WESCO Distribution, Inc.
225 W. Station Square Drive, Suite 700
Pittsburgh, Pennsylvania 15219

www.wesco.com/government