

*Interceptor<sup>™</sup>  
Optical Network  
Security System*

*Design Guide*



***Chapter 8:  
Tools and Resources***

**Network Integrity**  
SYSTEMS

We Bring Security To Light<sup>™</sup>

---

**Copyright © 2010 Network Integrity Systems, Inc.**

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Network Integrity Systems, Inc. The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

---

**Trademarks**

Network Integrity Systems, Inc., the Network Integrity Systems, Inc. logo, and Interceptor are trademarks of Network Integrity Systems, Inc. Other brands and product names are trademarks or registered trademarks of their respective holders.

---

**Statement of Conditions**

In the interest of improving internal design, operational function, and/or reliability, Network Integrity Systems, Inc. reserves the right to make changes to the products described in this document without notice. Network Integrity Systems, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Chapter 8 | Tools and Resources

### INTERCEPTOR Technical Specifications

<b>Electrical</b>	Power Input 100/240V, 250mA 60/50Hz IEC 3 Position Connector
<b>Environmental</b>	Operating Temperature 0°C - 45°C Storage Temperature -10°C - 50°C Operating Humidity 20% - 80% Non-Condensing
<b>Physical</b>	1U high, 19" Rack Mountable H x W x D: 45 x 432 x 368 mm H x W x D: 1.75 x 17.0 x 14.5 inches Weight 6.4 kg (14 lbs)
<b>Local Management</b>	Channel LED indicators, Channel Reset Buttons
<b>Remote Management</b>	RS232 Serial: Telnet 10/100BaseT Ethernet: SSHv2, Telnet, SNMPv3
<b>Alarm Management</b>	SNMPv3, Email, SMS and Dry Alarm Contacts
<b>Optical</b>	1, 2 or 4 Ports Singlemode, Multimode 50 µm and 62.5 µm SC Duplex Connectors Others Available On Request
<b>Power and Heat</b>	A fully loaded 4 port INTERCEPTOR draws 30VA typical, 45VA absolute maximum at a power factor of 0.6. We recommend specifying a UPS with at least a 45V rating if using a small UPS, with a larger system which only specifies watts (and therefore probably power factor corrected to 1: we recommend a rating of at least 45 Watts. Actual power dissipated (heat) will be 18 watts typical, 27 watts absolute max.

### RTU Technical Specifications

<b>Environmental</b>	Operating Temperature 0°C - 45°C Storage Temperature -10°C - 50°C Operating Humidity 20% - 80% Non-Condensing
<b>Physical</b>	<i>Rack Mount RTU</i> 1U High, 19" Rack Mountable H x W x D: 45 x 432 x 368 mm H x W x D: 1.75 x 17.0 x 14.5 inches Weight 4.5 kg (10 lbs)  <i>Micro-RTU</i> H x W x D: 25 x 50 x 100 mm H x W x D: 1 x 2 x 4 inches Weight 140 Grams 4.5 oz
<b>Optical</b>	1, 2 or 4 Ports (Rack Mount) 1 Port (Micro) Singlemode, Multimode 50 µm and 62.5 µm SC Duplex Connectors Others Available On Request

## Chapter 8 | Tools and Resources

### Frequently Asked Questions

**Q. How does INTERCEPTOR™ detect an intrusion into a fiber optic cable? A:** INTERCEPTOR launches a monitoring signal into a pair of fibers of the optical cable being protected, which turns the entire cable (up to 144 fibers) into a sensor. When any component of the cable is abnormally handled, for instance during an intrusion attempt, the monitored fibers sense the disturbance and INTERCEPTOR reports the event.

**Q. How does INTERCEPTOR distinguish between true intrusions and everyday events that may cause nuisance alarms? A:** INTERCEPTOR incorporates a patented Smart Filtering™ technology to “auto-configure” itself and learn a baseline of normal, routine, benign, non-threatening affects upon the cable system. These normal events are thereafter ignored resulting in the elimination of false alarms.

**Q. What type of fiber does INTERCEPTOR require for monitoring? A:** INTERCEPTOR uses the standard communications fibers inside the cable to perform the monitoring, and models are available for dark (unused) or active (transmitting data) fibers.

**Q. Does INTERCEPTOR protect the cable or just individual fibers? A:** For most cable designs, monitoring as few as 2 fibers within the cable can protect an entire 144-fiber cable. If ingress into the cable is attempted, the protected fibers will sense the disturbance and issue an alarm.

**Q. Is an INTERCEPTOR required at both ends of the cable run being protected? A:** In the case of dark fiber monitoring, a single INTERCEPTOR is required at one end of the cable. For monitoring active fibers, a single INTERCEPTOR Plus™ is required at one end of the cable along with a small passive device (Remote Termination Unit) at the far end.

**Q. To how many separate buildings or drops can a single INTERCEPTOR provide a secure connection? A:** A single INTERCEPTOR can provide a secure connection to a minimum of four locations and typically, based upon the network architecture, to as many as sixteen and sometimes up to thirty-two.

**Q. Does the INTERCEPTOR have an impact on the bandwidth of the network? A:** INTERCEPTOR is a physical layer device, and does not touch, process or verify the network data or the National Security Information, therefore no bandwidth bottlenecks are created allowing full utilization of the network – up to 10Gbps and beyond.

**Q. Is it necessary to perform an auto-configuration before INTERCEPTOR can start protecting a network? A:** The INTERCEPTOR is set at the factory with a default profile that enables it to be placed into service and protect the network immediately. Once installed, performing an autoconfiguration while the unit continues to monitor optimizes the protection profile.

**Q. Which organizations have approved INTERCEPTOR? A:** As an alarmed carrier hardened Protected Distribution System (PDS) compliant with the requirements of NSTISSI 7003, the instruction that governs the transmission of unencrypted National Security Information, INTERCEPTOR is a fully approved PDS option. INTERCEPTOR also complies with requirements AFI 33-201 (Air Force), AR 25-2 (Army) and NAVSO P-5239-22 (Navy). It is also listed on the US Air Force CTTA Approved Product List for PDS Alarm Systems as well as the US Navy TEMPEST PDS Approved Product list. INTERCEPTOR has been reviewed by the DISA DSAWG and confirmed as a viable tool for SIPRNet protection subject to approval by local approval authorities.

## Chapter 8 | Tools and Resources

### **Frequently Asked Questions**

---

**Q. Am I required to contain the cables being protected by INTERCEPTOR inside of a hardened carrier system (i.e. rigid metallic conduit, EMT or commercial raceway)?**

**A:** It depends on the organization. Air Force updated their PDS policy in 2009 to permit flexible interlocking armored optical cables monitored by INTERCEPTOR as a PDS (up to TS-CONUS, Secret-OCONUS). Army and Navy will consider the same solution on a project by project basis. This allows cables to be distributed in existing conveyance (wire basket, ladder rack) or suspended from D-rings, J-Hooks, etc. resulting in tremendous cost savings and construction complexity reduction. For non-armored cables INTERCEPTOR permits at a minimum, the installation of the conduit above the ceiling or below the floor since the requirement for periodic visual inspections is eliminated when an alarmed carrier PDS is used. The benefits are still significant: more reliable inspection of the PDS (performed by the INTERCEPTOR 24/7), and much better facility aesthetics.

**Q. What types of management or software tools are required to manage the INTERCEPTOR?**

**A:** The INTERCEPTOR can be locally managed by serial console, and remotely managed by Telnet or Secure Shell (SSH). The INTERCEPTOR can be accessed via terminal programs such as HyperTerminal or TeraTerm.

**Q. Doesn't the requirement to respond to alarms create an additional need for manpower?**

**A:** Since INTERCEPTOR eliminates the requirements to perform daily visual inspections of the PDS, the resources formerly used to conduct that task are no longer needed. A key thing to remember is that INTERCEPTOR prompts you when to conduct an inspection versus conducting them day-in-and-day-out whether a threat to the network exists or not. Therefore the use of INTERCEPTOR actually reduces the manpower necessary to secure a network.

**Q. Who typically monitors the INTERCEPTOR and how do they receive the alarms generated?**

**A:** Monitoring responsibility is established on an organization-by-organization basis. Typically it is performed by Security/Military Police, IT Help Desks or Network Operations & Security Centers (NOSCs). If Security/Military Police forces are used, then the INTERCEPTOR is usually integrated via dry contact interfaces into the existing building security system, which those forces routinely monitor. If monitored by IT departments or NOSCs, then the alarms are usually received via SNMP traps.

**Q. Which organizations have deployed INTERCEPTOR?**

**A:** As of this printing INTERCEPTOR has been deployed by the US Air Force, US Army, US Coast Guard, US Marine Corps, CENTCOM, Department of Homeland Security, Defense Intelligence Agency, Department of Justice, DoD Department of Inspector General, Naval Surface Weapons Center, Naval Undersea Warfare Center, National Reconnaissance Office, SPAWAR, STRATCOM, The Pentagon, numerous large and small systems integrators, major defense contractors.