

# WIREMOLD



## White Paper

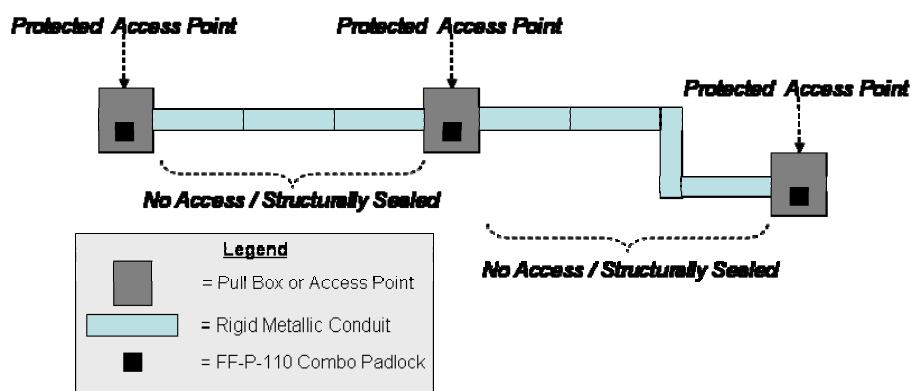
### The PDS Dilemma: Achieving Modularity & Scalability in Protected Distribution Systems without Compromising Security

Over the last 2 years, hardened carrier deployment in existing buildings have increased dramatically due to the proliferation of SIPRNET and JWICS networks by DoD and other agencies, system integrators, and contractors. As the requirement for secure network access has increased dramatically, so has the need to maximize the scalability and modularity of the associated structured cabling systems and the need to minimize the Total Cost of Ownership. Unfortunately, to date, maintaining the security of a hardened carrier system and providing modularity and scalability to the associated networks have been competing interest – with any increase in one area requiring a compromise or decreased performance in the other.

#### Traditional PDS Deployments

The national regulation that governs the deployment of hardened carriers as part of a Protected Distribution System (PDS) is NSTISSI 7003. Traditionally, hardened carrier deployments were accomplished using rigid metallic conduit or EMT. Using metallic conduit offered a great deal of security for the networks – with its seamless design and permanently attached fittings – but offered absolutely no scalability or modularity for future moves, adds, and/or changes to the network. If any structural changes were required in the building, or if the SCIF or Controlled Access Area was relocated, over 90% of the existing hardened carrier PDS would be scrapped and entirely re-constructed for the new areas. This is largely attributable to the installation required for rigid metallic conduit, which requires the PDS to be custom built into each room & hallway.

The lack of scalability & modularity was hardly a concern when SIPRNET deployments were



limited to very select groups and higher commands. But now that the deployment of the GIG and utilization of GCCS, GCSS, and JWICS have increased the war-fighters need to have access to secure networks at **ALL** levels of command, scalability and modularity are key concerns for secure network deployments and newly constructed secure facilities. In addition to its lack of modularity and scalability, rigid metallic conduit also detracted from the aesthetic environment for the areas where it was deployed. Due to the requirements out of NSTISSI 7003 for daily Periodic Visual Inspection (PVI) of hardened carrier systems, the rigid metallic conduit would be installed just below the ceiling or along the wall. For many end users, looking at what many refer to as BFUP's – or Big Fat Ugly Pipes – made a professional building or office space look more and more like an industrial factory. Along the cable pathway, several access points or pull boxes would be installed and then secured using a GSA-approved padlock. The diagram below depicts a typical rigid metallic conduit installation:

As the diagram depicts, access to the PDS IS limited to the Access Points or Pull Boxes installed – which are protected by the GSA-approved padlocks. Along the conduit sections, the PDS is structurally sealed with all fittings permanently attached (per NSTISSI 7003) - preventing any covert or surreptitious penetration of the PDS without invasive tooling. Also, by using a structurally sealed system, any loss of integrity of the PDS along the conduit sections would also require extra effort to conceal the penetration – there would be no way to easily access a section and then replace it. Any damage would have to be concealed, requiring considerable extra time for the perpetrator and leaving behind visible evidence that the PDS had been compromised (*the degree of visibility would be dependent upon the skill of the perpetrator and the amount of uninterrupted time they had for the penetration...*). Any attempts at penetrating the access points or pull boxes would require the perpetrator to defeat the security of the padlock being used for security.

**Testing & Validation of Locks used for PDS Security:**

All locks and security apparatus used to protect classified information and equipment is required to be inspected, evaluated, and certified by the DoD Lock Program. The Department of Defense directive 3224.3 entitled “Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support”, designates the Navy as the Executive Agent for the DoD Locks, Safes, Vaults, Seals and Containers Program (hereafter referred to as the DoD Lock Program). As part of the DoD Lock Program’s responsibilities, they ensure that the DoD **only** utilizes locks that have past the rigorous tests for long-term reliability and ability to withstand over, covert, and surreptitious attack. For combination padlocks used typically used on pull boxes and access points, the Federal Specification used by the DoD Lock Program for testing & validation is FF-P-110. A list of the tests required by FF-P-110 is provided below:



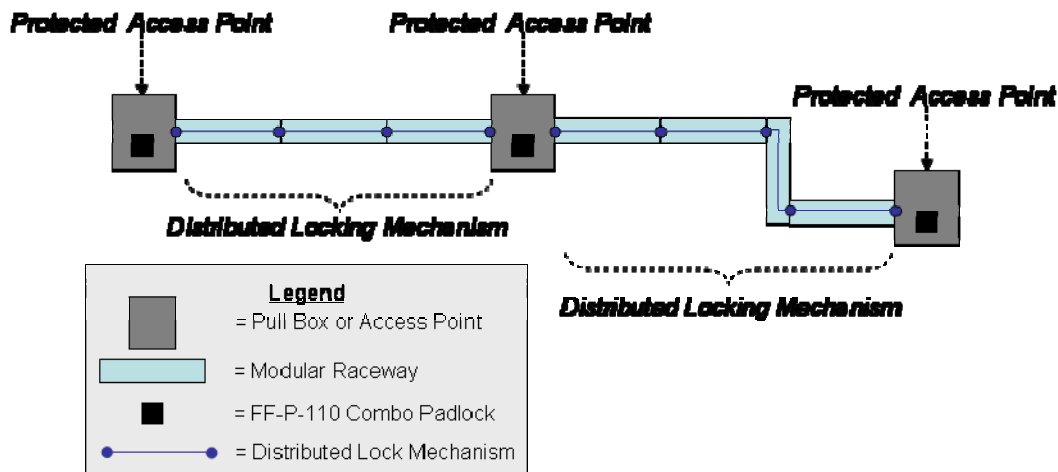
<b><u>FF-P-110 Specification</u></b>		
<i>Manipulation resistance</i>	<i>Surreptitious resistance</i>	<i>Drop resistance</i>
<i>Direct tension resistance</i>	<i>Jar with tension resistance</i>	<i>High humidity</i>
<i>Jar without tension resistance</i>	<i>Shackle and lock strength</i>	<i>High temperature operations</i>
<i>Low temperature operations</i>	<i>Cycle test for wear and lubricant</i>	<i>Heat resistance</i>
	<i>Radiographic opening resistance.</i>	

Table 1: FF-P-110 Testing Requirements

## PDS Innovation

In order to alleviate the aesthetic issues associated with rigid metallic conduit and provide increased modularity and scalability, some manufacturers have introduced modular pathway products that enable easy move, adds, and changes and claim to be “approved” or “certified” for use as a PDS. According to several of the Certified TEMPEST Technical or Approval authorities, none of the modular pathway products being proposed for use as a hardened carrier PDS have been officially approved for service-wide or agency-wide deployment; all approvals have been localized to site-specific approvals for a particular deployment.

In order to provide easy access to the raceway for modularity and scalability, some of these modular raceway product(s) incorporate a proprietary locking mechanism that is distributed throughout the pathway. The diagram below depicts a PDS installation using a pathway product with a distributed locking mechanism:



The proprietary and untested nature of locking mechanisms has created a great deal of concern as of late for many security and accreditation personnel. In fact, when the DoD Lock Program has tested product with similar distributed locking mechanisms, they have found these systems to be easily accessed and defeated – resulting in a complete Loss of Integrity for the PDS system. The gravest concern for the use of a distributed locking mechanism lies in the ability of a skilled perpetrator to (1) access, unlock, and remove a section or cover of the modular raceway; (2) corrupt the secure network; and (3) replace the section or cover of the modular raceway leaving little to no detectable evidence that the PDS had ever been compromised. The security of the PDS system will always be limited by the ‘weakest link’ - the component with the proverbial lowest common denominator. Since the FF-P-110 standard includes specific time constraints for covert and surreptitious entry, ANY PDS system installed should meet these same time constraints *at a minimum*. In fact, even filing cabinets used to store classified material or equipment has been subjected to covert, overt, and surreptitious testing for years under Federal Specification AA-F-358G (*Requires a minimum level protection of 20 man-hours against surreptitious entry and 30 man-minutes against covert entry*<sup>1</sup>.)

## PDS Buyers Beware...

Achieving increased modularity and scalability at the expense of the protection National Security Information is an unacceptable compromise. In fact, many installations and agencies have recently required modular raceway products with distributed locking mechanisms to be epoxied

<sup>1</sup> AA-F-358H – Section 3.7 Resistance to Entry Techniques

closed along the entire raceway to (1) achieve compliance with NSTISSI 7003<sup>2</sup>, and (2) provide a means of detecting any unauthorized access. By requiring that the modular raceway to be expoxied in order to be used as a hardened carrier PDS, the system has lost any intended modularity and scalability it was originally deigned to provide. In fact, the only benefit the system then provides above and beyond the traditional rigid metallic conduit PDS is the improved aesthetics in the workplace – but this is still a considerable feature & benefit and strong rationale to advocate the use above and beyond traditional EMT. Unfortunately, most modular raceway system(s) used to date as a PDS typically require costly design & engineering services and specialized installation personnel resulting in a considerable cost premium & increased complexity above and beyond a similar rigid metallic conduit PDS system.

Aside from the security concerns associated with a distributed locking mechanism, there is also a degree of uncertainty associated with its long-term reliability and performance. For decades, combination and padlocks used to secure classified information & equipment have been required to withstand the rigorous testing and validation of the DoD Lock Program. The tests required under FF-P-110 (see Table 1) ensure that any locks tested and validated do not experience a degradation of performance or protection as a result of extreme environmental conditions and/or rigorous usage over the lifecycle of the device. When a proprietary lock or locking mechanism is incorporated into a modular raceway used as a PDS system, it introduces a degree of uncertainty as to the long-term reliability and effectiveness in securing the raceway and protecting the National Security Information contained within. Even if the distributed locking mechanism was 100% effective after initial installation, there is no way to be certain that re-accessing and re-configuring the modular raceway (which is the primary objective of being modular) would cause a decrease in the long-term reliability and integrity of the locking mechanism.

Without the testing and re-assurance of the DoD Lock Program, federal agencies and installations have to weigh the potential risks associated with proprietary locks and distributed locking mechanisms *very* carefully. If there is any question or concern with a product as part of a PDS, the agency or installation should receive confirmation or direction from the applicable Designated Approval Authority (DAA) and Certified TEMPEST Approval Authority or Technical Authority (CTAA/CTTA) before any product(s) are purchased or installed.

While the intentions of most vendors and manufacturers are good, they should not be entrusted as the sole source of guidance and direction for *any* PDS systems – the entrusted source for this information is the DAA and the CTAA/CTTA. PDS approvals have always been site and facility specific, so what is approved for use as a PDS in one facility or project does NOT guarantee that the same product will be approved in another facility, installation, or project. Several agencies are establishing ‘approved product lists’ to alleviate any question or uncertainty when selecting product(s) for PDS and secure network installations, but the basic rule still applies – “*When in doubt, ASK before you ACT.*”

With the tremendous advantage in information superiority and combat effectiveness that SIPRNET and JWICS networks are providing to the warfighter, we have to be diligent now more than ever in ensuring that these networks are protected and defended against all threats – both internal & external – over the entire lifecycle of the network. We simply cannot afford to provide less than adequate protection or operate under a false sense of security - especially since

---

<sup>2</sup> NSTISSI 7003 – Annex B: “All connectors should be permanently sealed completely around all surfaces (e.g., welding (continuous or track), compression, epoxy, fusion, etc.).”

our enemies are strategizing now more than ever on ways to compromise our secure networks and prevent the warfighter from accessing and leveraging this critical resource to achieve information superiority. In the words of General Douglas MacArthur, “One of the quickest ways to fail in battle is to underestimate our enemies’ capabilities, commitment or will to succeed. Such behavior is akin to arrogance and is the doorway to success for our enemies...”<sup>3</sup>

---

<sup>3</sup>*These words were spoken by General MacArthur in a speech just two weeks prior to the attack on Pearl Harbor....*