White Paper

April 2012 • WP-16

Unified Physical Infrastructure^{SM} Solutions for Industrial Automation

Introduction to the Micro Data Center

Author: Dan McGrath, Industrial Automation Solutions Manager
Andrew Banathy, Lead Software Engineer

PANDUIT®
building a smarter,
unified business foundation
Connect. Manage. Automate.

Introduction

The industrial network is the fundamental backbone for data collection and transmission to points of use. Industrial network applications range from the ability to trace quality of production lots, improve preventive maintenance schedules, manage and monitor processes, improve safety, and identify constraints to increase productivity. These applications are supported by a reliable and secure network to keep production flowing and business communication running smoothly where downtime is measured in minutes and in thousands of dollars from missed customer commitments.

Office-grade IT equipment often is deployed in the industrial space, with additional environmental protection required. Automation vendors are integrating Ethernet connectivity at all levels of manufacturing starting at the bottom with sensors to PLCs and up to manufacturing servers and switches. Crucial to success is ensuring that the linkage between these systems is secure, environmentally protected, and optimized to speed diagnostics and problem solving; reserving the ability to isolate the networks when security threats to production arise.

The centerpiece that brings this all together is a Micro Data Center (MDC). An MDC is a partial, single, or multiple rack/cabinet that houses rack mounted servers, switches, UPS, Backup Systems, and DIN rail mounted devices (see Figure 1). The Micro Data Center is designed to provide the link between the Corporate and the Industrial Networks in order to:

- Maintain network uptime
- Provide the ability to segregate networks
- Manage network security
- Speed changes and troubleshooting
- Provide ease of installation

This White Paper reviews the elements of an MDC and investigates the benefits of deploying this technology in an Industrial Automation environment.

Figure 1. MDC Cabinet Featuring Network Zones

Micro Data Center Characteristics

The Impact of Team Cooperation on Reducing Downtime

In today's business environment, there has been a movement to centralize responsibility of all computer networks under the IT department. This move has created clashes between IT and manufacturing due to differing needs and equipment deployed. A Micro Data Center helps to separate the networks and reduce conflicts points between both networks and enterprise teams that support them.

Historically, the industrial network has been the responsibility of the manufacturing organization and all other networks have been firmly under the control of the IT organization with little connectivity between. One common complication has been the tendency to install IT equipment without full consideration for the high availability and security requirements of automation systems (see Figure 2). Another spot where problems may arise is identifying if IT or manufacturing has responsibility for deployment and maintenance of the networks.

Without close communication, coordination, and consensus building between all industrial network stakeholders, critical manufacturing resources can be at risk of outages, lost batches, and ultimately lost revenue.

Figure 2. Poor Industrial Network Installation Can Generate Unacceptable Downtime Risks

The Micro Data Center Defined

A Micro Data Center (or MDC) is a versatile combination of hardware, software and cabling that serves as an end-to-end networking hub, similar to a telecommunications room or network room but much smaller scale than the typical enterprise data center. The defining characteristic of an MDC is that it houses a complete data center infrastructure in a single space –electronic devices, patch fields, cable management, grounding/bonding, power, and copper/fiber cabling – yet is sized to serve the demands of a manufacturing environment.

The MDC is a new concept, representing the next phase in the transition from tower computing systems in a manufacturing environment to rack and cabinet-based deployments, with the ability to serve a variety of enterprise purposes. For example, the MDC can act as a standalone system that runs manufacturing applications such as:

- Process and event monitoring, process historian, production tracking, OEE reporting
- Control network, outer loop control, recipe download
- Quality control, material handling, maintenance, lot tracing, and asset management
- ERP integration (i.e. scheduling, reporting, material consumption, etc.)

The MDC also can take the form of a networking hub that has no servers, existing primarily to tie cabling and switches together. For large manufacturing complexes or remote locations, an MDC can serve as a data collection node that passes manufacturing data up to the enterprise (i.e., Store and Forward). Finally, an MDC can also house Virtual Machine (VM) systems for high reliability and efficient server utilization.

From a physical perspective, the MDC is typically located in a secure space (such as a Control Room, Production Office, or Telecommunications Closet) that is located close to the production environment but is not actually part of it. This stems from the need to separate the effects of these environments on MDC equipment (i.e., dust, moisture, vibration, corrosion, etc.). Positioning the MDC near production equipment helps reduce the number of connections, minimizes cable run length(s), and facilitates easy access in order to achieve high network reliability and performance (see Figure 3). Further benefits offered by this proximity include reducing the number of potential failure points and lowering inherent network latency while facilitating rapid troubleshooting and diagnostic capabilities.

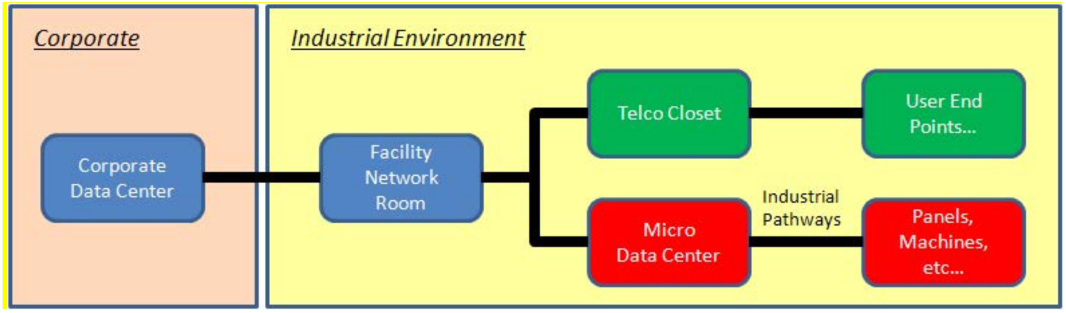

Figure 3. Block Diagram Indicating Location of Micro Data Center in Relation to the Data Center, Corp Network, Industrial Pathways, and Equipment Panels

From a logical architecture perspective, the MDC is positioned between the manufacturing floor and the enterprise data center (see Figure 3). To maintain separation, a demilitarized zone (DMZ) is used in conjunction with a firewall to prevent direct traffic between the enterprise and manufacturing network. This separation prevents viruses and other unwanted user intrusions while ensuring maximum bandwidth dedicated for manufacturing. The benefit of this structured approach is that events unfolding in one network can be addressed independently, leaving the unaffected network to function normally.

MDC Design

The starting point to the MDC design is identifying the capabilities and associated equipment required as well as a housing solution that centralizes equipment. A superior MDC design addresses the following key considerations:

- Housing – Racks and Cabinets
- Equipment Layout
- Network Cabling – Media Selection and Security
- Power and Grounding
- Cable Management

The remainder of this section describes in greater detail each of these points of consideration.

Housing – Racks and Cabinets

A rack or cabinet is typically used to house MDC elements in a centralized modular form factor. The main difference between a rack and a cabinet is one of protection: a cabinet offers greater security and environmental protection (i.e., from both dirt and workers) due to four walls and the ability of a locking door mechanism, versus the open environment provided by a rack. For harsh environments, the MDC can be housed in a NEMA-rated hardened cabinet with the proper cooling and environmental protection.

The housing (i.e., rack, see Figure 4) needs to accommodate all equipment, patch panels, and cable managers while providing a growth factor of between 30-50% to accommodate future expansion. For small MDCs, half-height racks or cabinets may be sufficient, while large installations may require full size or multiple racks/cabinets.

Figure 4. Example Panduit 4 Post Rack (half or full) with Cable Management Deployed for Micro Data Center Application

- ***Cabinets.*** In general, cabinets are designed for servers or switches. Server cabinets are deeper with cable routing in the back, whereas switch cabinets may be more shallow with cable routing in the front with the ability to utilize sides for additional cable capacity. If combining servers and switches in the same housing, a server cabinet should be selected to provide greatest design flexibility.
- ***Racks.*** Racks can be a 2 post or 4 post design. Typically, a network rack with shallow switches can fit a 2 post design. Larger and heavier equipment is best handled by a 4 post design, especially if mounting servers. If combing servers and switches together in the same rack, a 4 post design should be selected to provide greater design flexibility.

Equipment Layout

Equipment layout in a rack or cabinet depends on the number, weight, and type of components as well as segregation. Common design practice locates enterprise network equipment at the top and industrial network equipment at the bottom, with the DMZ positioned in the middle of the housing. Typically, heavy components are located at the bottom of the rack or cabinet with the patch field located at the top for best stability. In general, like equipment should be grouped with spaces for free RU.

If combining servers and switches into the same housing, several design considerations come into play. Common practice is to face the front of switches and the back of servers in the same direction, in order to keep connectivity on one side of the housing for ease of access. This layout strategy mitigates the risks involved with less organized wire management approaches, and reduces network interruptions resulting from common cabling problems (i.e., difficult to access cables, cords that snag when pulled, etc.).

Thermal loads in an industrial Micro Data Center application are quite low, typically less than 25% of that experienced in an enterprise data center environment. This reduced heat load, coupled with the extended operating capabilities of industrial-rated switches, greatly diminishes the need for active cooling solutions in many industrial applications.

There may be cases where network designers may wish to combine DIN rail mounted devices within racks (components such as PLCs, gateways, manufacturing switches, etc.) in order to save space. Placement of DIN rail mounted devices in the MDC may help achieve this benefit by eliminating separate enclosures while closely linking DIN rail mounted devices to the network (see Figure 5).

Figure 5. Manufacturing Switch Mounted on a DIN Rail Bracket

Network Cabling - Media Selection and Security

Ethernet media can be fiber optic cabling and/or copper cabling. There are many design considerations to properly select the cable media: Table 1 compares cable types when multiple criteria are considered:

- Run distances between MDC and manufacturing equipment
- Type of information transmitted (i.e., machine instruction or production monitoring data)
- Equipment connectivity (i.e., types of connectors/ports)
- Environmental conditions (i.e., electrical noise, vibration, temperature, moisture, etc.)
- Ease of installation and maintenance frequency

Table 1. MDC Cabling Options for Copper and Fiber Optic Cabling Media

Parameter	Copper Cable	Multi-mode Fiber	Single-mode Fiber
Reach (max)	100m (330ft)	500m (1,750ft)	40km (24 miles)
Noise Mitigation	Foil shielding	Noise immune	Noise immune
Bandwidth	1 Gb/s	10 Gb/s	10 Gb/s
Cable Bundles	Large	Medium	Small
POE Capable	Yes	No	No

Multiple varieties of copper cabling media are available based on data speed and volume requirements. Typically Category 6 copper cabling is used for enterprise and manufacturing network connections. Fiber is typically used for distances greater than 330 ft / 100m, in environments where electrical noise is a concern, or for high volume transmission rates. There are two common types of fiber optic cabling, Multimode and Single Mode. Primary differences between them include cable run distance and cost of installation.

Another consideration would be the environmental surroundings and the level of protection needed for the cable jacket (temperature, corrosive, vibration, etc.). Depending on conditions, armored fiber and grounding are a good alternative for outdoor applications or harsh manufacturing environments where a good level of protection is needed. If a higher level of cable protection/durability is needed, an external pathway may be used to provide added protection.

Panduit is a supplier of a wide range of network media options for copper and fiber, including cabling and connectivity designed to operate in industrial environments. These varieties include ruggedized all-dielectric fiber optic cabling that enables customers to deploy cabling in tight spaces without the need of an additional protective conduit, which eliminated the need for grounding associated with typical armored fiber deployments.

Another consideration is whether to run Power over Ethernet (PoE) to deliver power to devices such as video surveillance cameras, wireless access points, or IP phone applications. This requires the use of copper cabling where current capabilities for PoE (standard IEEE 802.3af-2003) can provide up to 15.4 W of DC power. There is a higher power version known as PoE+ based on the IEEE 802.3at-2009 standard that can deliver up to 25.5 W of power. As technology improves, the ability to transmit higher power over Ethernet continues to increase. Some vendors including Panduit can power devices with up to 51 W over a single cable by utilizing the four twisted pairs in a copper cable.

Regardless of the media selection (fiber optic or copper cable), the use of a patch panel for connections in a MDC provides for essential testing and diagnostic points between equipment and field connections. The benefit of adding a patch panel is that it provides diagnostic points directly in the MDC, providing the ability to speed network troubleshooting and accommodate future expansion as network speeds increase or equipment connectivity ports change.

Power and Grounding

To keep the factory network running smoothly without compromises in communications and equipment performance, it is essential that robust and clean power be supplied to the Micro Data Center. The incoming power feed typically includes an Uninterruptable Power Supply (UPS) and one or more Power Outlet Units (POUs) to distribute power where needed. POU voltages range from 100 to 125v or 220 to 250v depending upon region of the world, with currents ranging from 15 to 30 amp. Connectors may be straight blade or twist locks. Popular IEC configurations are C13 to C14 and C19 to C20. Additionally, POUs may include intelligent features such as power and environmental monitoring to aid in troubleshooting and diagnostics.

Grounding of the MDC is critical to optimizing performance of all equipment located within the MDC unit, reducing downtime due to equipment failures and reducing the risk of data loss. Also, Cisco and other suppliers of logic components require good grounding practices to maintain warranty support. The use of a single ground path at low potential is commonly achieved through a busbar. There are several ways to bridge the grounding connection from MDC to busbar: (1) braided grounding straps connect the Rack or Cabinet to the building ground network, (2) grounding jumpers connect equipment to the housing structure, and (3) paint piercing screws and washers ensure a direct metal-to-metal connection throughout the MDC. Unless a clear and deliberate effort to ensure proper grounding has been performed, there is the potential for ground loops to be established that result in lost communication data and compromised equipment performance.

Cable Management

Proper wire management is essential for reliable connectivity and to speed troubleshooting, diagnostics, and moves, adds, and changes. Three areas in the MDC require wire management: input to the MDC, within the MDC, and output from the MDC.

Input to the MDC

Wires are routed to the MDC through a ladder rack, wire basket, or other secure overhead cable pathway. Cable labeling and separation are key elements of successful wire management in this area of the MDC: labeling provides a consistent method of identifying network connections, and cable separation mitigates the effect of crosstalk between adjacent cables or cable bundles. Both copper and fiber optic cables commonly are deployed as MDC input cables connecting the main data center to the MDC. Copper is traditionally used as a short reach solution in this type of application; however, fiber optic cabling is gaining greater acceptance due to its longer reach, higher bandwidth, and intrinsic ability to mitigate EMI noise concerns.

Within the MDC

Within an MDC, copper patch cords commonly are used to connect enterprise network equipment to the DMZ and then again to the factory floor network. Copper is preferred due to the short length of connections within the MDC and ease of installation. The simplest management approach uses D-rings and horizontal managers above and below devices to route cables, ensuring that optimal bend radius is observed and preventing signal degradation due to cable crosstalk. Strain relief bars and/or clips often are used to add additional protection to cables and maintain communication robustness.

Output from the MDC

Deployment of the network from the MDC to the factory floor can be achieved using either copper or fiber optic cabling media, with reach typically being the deciding factor on which media to deploy. Other considerations include the level of environmental protection needed to protect cables from harsh environmental factors (heat, moisture, vibration, etc.). Table 2 is a list of recommended pathways to use when routing cables outbound from an MDC, depending on several key site-specific variables for the industrial environments.

Table 2. Cable Routing Solutions Beyond the Micro Data Center

Installation Consideration	**J-Hook** 	**Wyr-Grid®** 	**FiberRunner®** 
Cable Protection Environment	Mild	Moderate	Moderate to harsh
Cable Density	Light to medium	Medium to heavy	Light to heavy
Applicable in Constrained Spaces	Yes	No	No
Installation Complexity	Simple	Moderate	Moderate to strong
Ease of Moves, Adds, Changes	Simple	Moderate	Moderate

Visual Identification

The use of clear visual identification practices throughout the infrastructure can aid rapid problem identification, facilitating quick troubleshooting and subsequent repair. This is accomplished through the use of cable labeling to identify connections and color coding to enhance wire management (connectivity, network security blockouts/lock-ins, and patch cords).

Cables equipped with descriptive labels that have “from” and “to” end points printed on them allow technicians to quickly trace cables, thereby minimizing improper disconnects. Color coding is a quick visual reference that provides meaning to a cable; for example, red patch cords may indicate connections to a fire wall or safety specific systems. Color coding can also be used to note manufacturing process, building destination, cable media performance, network segment, VLANs, or departments.

Physical Network Security

Ensuring the network is protected from unwanted intrusion or erroneous connections is of major concern in any environment (see Figure 6). Cable security is essential to achieve a full physical “defense in depth” strategy. Unused network ports can be blocked with plastic inserts (blockouts) to prevent unauthorized or mistaken access. Critical cabling can be “locked-in” to ports to prevent accidental or malicious disconnections. A further layer of security can be achieved through the use of keyed jacks and connectors that require specific keyed patch cords for connection.

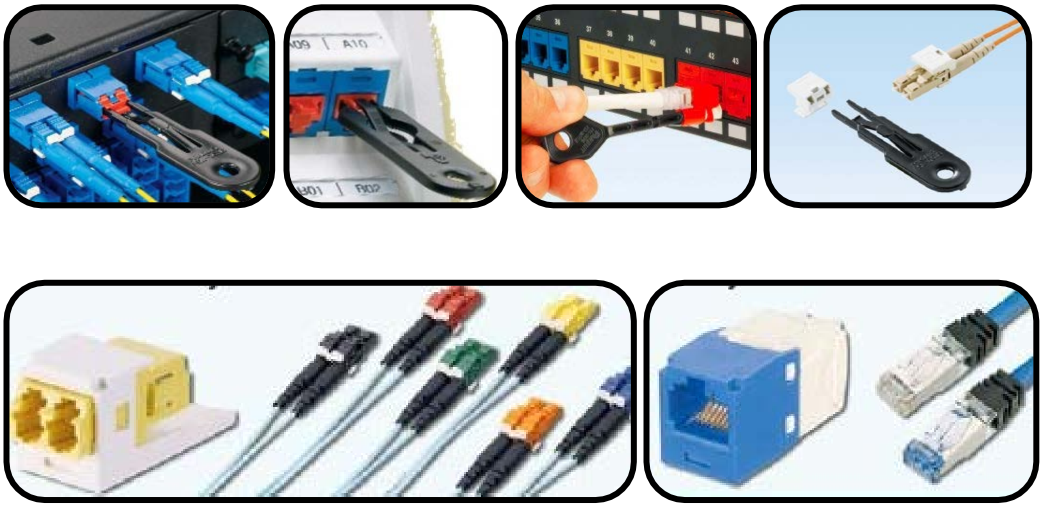

Figure 6. Panduit Lock-In, Blockout, and Keyed Connectivity Devices for Copper and Fiber Optic Cabling Deployments Help Mitigate Physical Security Risk in the MDC Infrastructure

Conclusion

A Micro Data Center is an effective solution to maintain robust, integrated, and secure networks. As networks continue to be deployed in Industrial settings, there is an essential need to capture production lot data as well as transmitting machine instructions to equipment. It bridges the gap between the Corporate and Industrial networks while maintaining flexibility to quickly disconnect the network links in the event of a problem.

Key elements of a robust Micro Data Center include:

- Housing – Rack or Cabinet
- Equipment Layout
- Network Cabling – Media Selection and Security
- Power and Grounding
- Cable Management

A well designed MDC protects the integrity, availability and confidentiality of control and information data. It facilitates the connectivity from the plant floor up to the enterprise giving greater visibility into the manufacturing processes to identify problems, optimize processes, and plan for the future. For further information, please visit www.panduit.com/microdatacenter or contact your distributor or Panduit Sales representative.

About Panduit

Panduit is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, increased agility and operational efficiency. Panduit's Unified Physical Infrastructure℠ (UPI) based solutions give enterprises the capabilities to connect, manage and automate communications, computing, power, control and security systems for a smarter, unified business foundation. Panduit provides flexible, end-to-end solutions tailored by application and industry to drive performance, operational and financial advantages. Panduit's global manufacturing, logistics, and e-commerce capabilities along with a global network of distribution partners help customers reduce supply chain risk. Strong technology relationships with industry leading systems vendors and an engaged partner ecosystem of consultants, integrators and contractors together with its global staff, and unmatched service and support, make Panduit a valuable and trusted partner.

www.panduit.com · cs@panduit.com