BELDEN
SENDING ALL THE RIGHT SIGNALS®

A Robust Industrial Ethernet Infrastructure Consisting of Environmentally Hardened Network Cabling, Connectivity, and Active Components Is Essential to Long-Term Performance and Reliability

Table of Contents

Industrial Ethernet is trending to be the principal infrastructure choice for mission-critical industrial automation and control applications. Industrial Ethernet is built on the same standards-based networking platform as enterprise Ethernet, which has long reigned as the universal network solution.

Industrial Ethernet connects the office with the plant floor by utilizing a single cabling platform with Ethernet connectivity and IP addressing. This convergence of open, standards-based Ethernet communications provides all the advantages of secure, seamless interoperability among manufacturing enterprise networks — from corporate offices to the shop floor — and enables Internet and enterprise connectivity, anytime and anywhere.

In addition to system integration and interoperability, there are a host of other benefits to be gained from implementing a complete, end-to-end Ethernet solution — from cabling and connectivity, to active components and associated hardware.

Key business benefits include lower overall Total Cost of Ownership (TCO) and higher return on investment (ROI) resulting from real-time visibility and flexibility, reduced network maintenance and administration costs and labor, and greater physical and virtual network security.

Operational benefits at both the plant and enterprise levels include:

- Faster and less costly plant upgrades, expansions and changeouts

- Access to real time data to improve overall plant operations

- Faster installation, remote troubleshooting and corrective action capabilities

- Real time inventory visibility

- Collaborative reviews of production data and virtual support groups

- Increased production capacity

- Shop floor system integration with ERP for scheduling, planning, quality tracking and delivery information

Network Infrastructure Risks in Extreme Environments

Industrial communications and control networks are expected to operate consistently and reliably under extreme conditions, such as electromagnetic interference (EMI), high operating temperatures, ambient outdoor temperatures, power/voltage fluctuations, machine vibration, mechanical hazards and more.

For example:

- In the **Oil, Gas and Petrochemical** industry, signal transmission components typically have to withstand the destructive effects of temperature extremes, humidity, moisture, dust, mud, oil and solvents, and the potentially corrosive effects of chemicals.

- In **Water and Wastewater** treatment plants, the cabling, connectivity and networking devices must endure high levels of humidity, grit and sludge, and, in some cases, are exposed to lime, as well as corrosive gases such as methane, hydrogen sulfide and chlorine.

- In the rapidly growing **Wind Power** industry, signal transmission components in wind energy sites, whether on-shore or off-shore, are routinely exposed to temperature extremes, excessive moisture and humidity from rainfall, mist, and fog. Mechanical and electrical stressors may include vigorous, prolonged vibration, torque, damage from rodents, EMI interference, and even lightning strikes.

- In the **Mining** industry, environmental conditions are extremely harsh. Dust, dirt and dampness can threaten signal transmission equipment and performance. In some mines, caustic chemicals and potentially explosive ambient conditions exacerbate the threat. While the use of conduit, aerial fiber optic cabling and wireless communications can alleviate some risk, mining remains one of the most challenging industries for industrial networking.

Oil, gas and petrochemical plants, water and wastewater facilities, wind farms and mines are just a few examples of industrial operations in which extreme environmental hazards can be detrimental to the performance and reliability of commercial-grade Ethernet cabling, connectivity and networking devices.

Untimely and costly disruptions can largely be prevented by installation of a robust network infrastructure utilizing environmentally hardened, industrial-grade components in all three OSI layers. A ruggedly designed framework enables industrial enterprises to carry out their mission-critical functions by providing the highest possible levels of:

Safety. Optimum safety is critical in all industrial operations. Full safety demands fail-save reliability and redundancy of data transmissions, as well as network components that meet and exceed industrial requirements for potentially hazardous environments.

Uptime. Prevention of signal transmission problems is a major factor in ensuring consistent and dependable network uptime and plant productivity. Whether an operation involves a discrete manufacturing facility, a processing plant or an infrastructure site, such as an airport or power generation plant, keeping operations running smoothly and reliably assures optimum uptime and peace of mind.

Control. Continuous monitoring, management and control, as well as operational efficiency, require continuity in data transmission and network availability. Any network failure, and subsequent downtime, can result in severe and extremely costly consequences.

The *Real* Costs of Network Failure

Industrial plants rely heavily on their automation, instrumentation and control data communications to relay signals between devices, machinery and the control system to activate events on an exacting and pre-determined schedule, with little or no margin for error. Many industrial facilities are sizeable and their networking products must meet or exceed stringent industrial regulations and ratings. Users also desire optimal manageability and security so that network availability attains 99.999% uptime or better.

Given these environmental risks, it is clear that the networked communications systems in extreme environments must be exceptionally rugged and durable. Any physical deterioration or electrical failure in key data transmission components can lead to unreliable network performance and/or safety issues, and may ultimately lead to loss of critical data, costly downtime, or even catastrophic failure.

Network Safety, Uptime and Control Are Paramount

'Industry' is a broad term encompassing a multitude of diverse operations — from discrete manufacturing of every kind, to processing of foods and beverages, pulp and paper, chemicals, oil/gas and petrochemicals, to commercial and government sites such as power generation plants, wind energy farms,

water and wastewater treatment facilities, airports and transportation hubs, military bases, ships and shipyards, railyards, tunnels, dams and bridges.

Networks in all of these operations must perform in extreme and often hazardous environments and every operation has its own set of environmental challenges to contend with. Analysts report that an overwhelming percentage of unplanned downtime in industrial operations can be attributed to network infrastructure failure. According to one network management report, *fully 72 percent of network faults can be attributed to failure at the OSI (Open Systems Interconnection) Layer 1 (Physical Media), Layer 2 (Data Link) and/or Layer 3 (Network).*

Maximum productivity with minimal downtime is a key goal, and 24/7 network performance and reliability are critical to achieving that goal. No matter what the industry, if a switch, connector or cabling system in the plant fails, the cost of parts replacement and repair represents only a tiny fraction of the overall costs associated with production downtime.

For example, if a cabling system component or Ethernet switch fails in a power generation facility, the repair/labor costs alone could be 15-20 times the cost of the component itself. However, disruptions in the plant's flow of information or control signals could lead to power outages — which, even today, cost the power generation industry as much as $150 billion per year. Downtime in an automotive assembly plant capable of producing one vehicle per minute would stand to lose profits of about $2,000 to $3,000 per minute for small car production, and up to $8,000 per minute for SUV and pick-up truck production!

The indirect costs of Ethernet system failure in any industry must take into account lost productivity, delayed downstream processes, cost of system shut-down and start-up, and the potentially devastating loss of service to customers relying on the plant's mission-critical output. Depending on the industry and overall operating costs, these indirect effects can send total downtime costs soaring to hundreds of thousands, even millions of dollars.

That is why investing in a high-quality, rugged Ethernet infrastructure designed specifically for use in harsh environments is a wise business decision — one that can provide tremendous peace of mind to network engineers and administrators and the organizations they serve.

Commercial-grade Components Are Not the Solution

In a typical office, the Ethernet infrastructure is installed in a relatively clean, quiet environment with cables hidden behind walls, in ceilings or under floors and network switches, hardware and connectivity components sheltered in protected areas.

Industrial facilities present a very different reality. Here, many if not most cables, connectors, switches, and active network components are integral to machine automation, instrumentation and control systems, which places them in harsh and potentially hazardous situations. Even the best Commercial-Off-The-Shelf (COTS) Ethernet systems are not made to handle such conditions over time. Rugged conditions call for ruggedized cables and only industrial-grade Ethernet system components are built tough enough to withstand the hazards and risks they are exposed to day after day.

Consider, for example, the deleterious effects the following common environmental conditions can have on network components:

- **Temperature Extremes.** Extreme cold can make COTS cables stiff and brittle, while elevated temperatures can degrade the plastic used in the cables' construction and cause an increase in attenuation. Industrial-grade cables are available that will operate in a wider temperature range (-40°C to +85°C) than commercial cables (0°C to +60°C).

   Commercial-grade hardware (switches, etc.) is designed to operate from 0°C to +40°C, while industrial Ethernet hardware can operate efficiently from 0°C to +60°C — extendable to -40°C to +85°C (conformal coating also available for humid/moist applications).

- **Chemical Exposure.** Oils, solvents, chemicals and cleaning solutions can soak into COTS cables, especially under heat, causing the cable jacket to swell and lose mechanical strength.

   On the hardware side, corrosive chemicals can damage the electronics in commercial switches, whereas ruggedized industrial switches are securely sealed to prevent ingress of these substances.

- **Humidity Levels** of up to 99 percent can be accommodated by industrial-grade switches, which can also be sealed to meet IP67 standards.

- **UV Radiation Exposure** can cause COTS cable jackets to decompose at an accelerated rate, compromising mechanical strength and electrical performance.

- **Physical Hazards.** The factory floor holds many mechanical risks, especially for machine automation cables and connectors. Excessive machine movement or vibration can result in cables being pulled or stretched with excessive force, which can create imbalance between the pairs, degrade electrical performance, and increase susceptibility to ambient EMI/RFI. Plant floor vehicles, such as forklifts and moving carts, can accidentally run over cables, causing abrasion, crushing or cut-through.

Even well-made, properly installed COTS Ethernet components are not constructed to survive these kinds of hazards. Only hardened, industrial-grade components are robust enough to withstand the environmental challenges present every day in industrial settings.

Industrial Ethernet Hardware vs. Typical Office-grade Ethernet Hardware

Characteristics (Hub / Switch / Fiber Interfaces)	Industrial Ethernet Hardware	Typical Office-grade Ethernet Hardware
Operating Temperature	0°C to +60°C standard, with extended temp of -40ºC to +85°C and conformal coating available	0°C to +40°C
Humidity	99% (non-condensing); 100% using IP67 (waterproof) switches	Typically 10-85% (non-condensing)
EMC	EN50082-2	EN50082-1
Operating Voltage	Variety of voltages, but 24 V (redundant) being the most common/standard No internal power supply	120 / 240 V Internal power supply
Redundancy	Media ring reconfig time < 30ms and as low as 10 ms.	Depending upon topology, possibly significantly more
Link Media	Multimode / Single-mode / UTP/STP	Multimode / Single-mode / UTP/STP
Communication Distances	Up to 68 miles longhaul single-mode	Up to 68 miles longhaul single-mode
Management	SNMP (Simple Networking Management Protocol) WEB-Based Management Serial (RS232) CLI (command line interface) EtherNet / IP™ and PROFINET profiles for integration of management into PLC/HMI	SNMP (Simple Networking Management Protocol) WEB-Based Management Serial (RS232) CLI (command line interface)
Diagnostics	Fault relay output(s) e.g., to PLC I/O Port LED (visual information) SNMP trap to OPC server	LED (visual information)
Chassis		
- Material	Plastic / Metal	Plastic / Metal
- Dimensions	Small (e.g. 80x140x85 mm)	Medium (e.g. 440x70x380 mm)
- Mounting	DIN rail / Rack	Desktop / Rack
Approvals	CE, cUL 1950, UL508, FCC Part 15, Germanic Lloyd, Class 1 Div 2, IEC 61850-3, IEEE 1613, NEMA TS2, EN 50121-4, EN 50155	CE, cUL
Vibration	2g (IEC 60068-2-6 FC)	Typically not rated/tested
Shock	15g+ (IEC 60068-2-27)	Typically not rated/tested
Cooling System	Fan-less operation	Fan Operation
Resistance	RFI/EMI, dust, oil (even IP67)	Dust
Data Throughput	10Mb, 100Mb, 1Gb, 10Gb	10Mb, 100Mb, 1Gb, 10Gb
Switches	Yes (DIN rail, 19" rack and hard mount)	Yes (19"rack or tabletop)
Hubs	Yes (DIN rail)	Yes (19"rack or tabletop)
Transceiver	Yes (DIN rail)	Yes (19"rack or tabletop)
Firewall	Yes (DIN rail)	Yes (19"rack or tabletop)

"Ruggedized" for High Mean Time Between Failure

In selecting physical media, data links and network hardware for the industrial Ethernet, multiple factors should be considered to ensure optimal performance, ease of maintenance, and long-term reliability.

Ruggedized industrial Ethernet products have been designed specifically to network in tough environments, to support the industrial protocols which are being transmitted across these networks, and to accommodate the environmental rigors of the location. Key considerations in specifying industrial-grade network components include:

MTBF (Mean Time Between Failure). Industrial Ethernet products are designed to provide the same lifespan as other automation components — typically 10 to 30 years or more. By comparison, typical commercial-grade products are built to achieve a 5-year average lifespan.

Mounting options. Industrial Ethernet hardware devices are usually DIN rail mounted or bolted directly onto the machines that receive transmitted data.

Small form factor. Equipment is typically designed to occupy less space to allow greater density within a control panel.

Ventilation without fans. Industrial Ethernet devices rely on passive heat dissipation.

Protection class. Devices must be available in dustproof and waterproof housings.

Conformal coating. A special coating is applied to PCBs to protect electronic components in damp or corrosive environments.

Redundancy. Redundant power, redundant media paths and even redundant devices can assure 24/7 uptime.

Bandwidth. With an ever-increasing number of Ethernet-enabled devices being added to networks, sufficient bandwidth is needed to ensure meeting future needs.

Hardened Components Protect Network Integrity

As stated previously, an overwhelming percentage of network performance problems are due to failure at OSI Layer 1, Layer 2 or Layer 3. Therefore, it is critical to ensure that components at all three layers — physical media, data links and active network devices — are designed and constructed to withstand the operational and environmental stressors to which they are subjected. For each category, multiple factors need to be considered to ensure optimal performance, ease of maintenance, and long-term reliability of the mission-critical network.

Physical Media — Cabling & Connectivity

For the physical media layer, there are a host of products in today's marketplace that fully conform to the Ethernet LAN.IEEE 802.3 standard. Selection will depend on each plant's network configuration and application requirements. Products include:

- Heavy-duty, all dielectric, indoor/ outdoor-rated optical fiber cabling in single-mode and multimode constructions. Many feature water-blocking agents for added protection in moisture-laden environments.

- Industrial grade Cat 5e (2-pair and 4-pair) and Cat 6 UTP (4-pair) cables with heavy-duty oil- and UV-resistant jackets. Some Category cables feature a Bonded-Pair inner construction in which the conductor insulation of the pairs is affixed along their longitudinal axis to ensure consistent conductor concentricity to prevent any performance-robbing gaps between the conductor pairs during installation and use.

- Upjacketed and armored cables for more extreme environments.

- Continuous flex cables designed for use with continuous motion machines and automation systems.

- Low smoke zero halogen (LSZH) cables, waterblocked and burial cables are also available.

- Cables designed for use with leading industrial automation networking and communications protocols, such as EtherNet/IP (ODVA), Modbus TCP/IP, ProfiNet and Fieldbus HSE.

- Industrial-grade connectivity components, such as: IP67- or IP20-rated UTP or FTP patch cords, connectors, modular jacks and plug kits, adaptors, faceplates and surface mount boxes.

BELDEN
SENDING ALL THE RIGHT SIGNALS

Industrial Ethernet Cable Selection

Fiber optic Ethernet cables represent the ultimate in future-proofing and are available for indoor use (riser or tray) or outdoor use (including direct burial). Typical designs use multimode fibers in a loose tube configuration, usually available in 2- to 72-fiber constructions. For plenums, tight buffered, 2- or 6-fiber single-mode or multimode construc-tions are typically available.

- To handle Gigabit Ethernet light sources and any expanded bandwidth requirements some cables use a laser-optimized fiber.

- For moisture protection, a water-blocking agent should be included in the cable's construction.

- In particularly harsh environments, a CPE outer jacket will provide addi-tional protection against chemicals or abrasion; an armor tape or aluminum/steel armoring may also be appropri-ate for the extreme environments, including some burial situations.

- Ratings include: UL Type: OFNR, cUL Type: OFN FT4, IEEE 383-2003 Flame Test.

Copper Ethernet cables are the more traditional option in industrial installations, available for either Cat-egory 5e or Category 6 applications. Category 5e cables are the dominant choice today, while Category 6 cables are finding increasing use where Giga-bit speeds and increased bandwidth are desired and/or for future-proofing purposes. Category 5e and Category 6 twisted pair cables are available using any number of conductor types, insulations, shielding and jackets. Armoring is also available for extremely harsh environments.

**Construction selection criteria:**

- **Unshielded or shielded?** Unshielded products can be used in most environments; shielded products are recommended for especially high noise environments.

- **Shields:** Typically a foil or braid is used to protect the integrity of the signal and to screen out any undesirable interference or noise. However, to provide extra durability and noise protection, a foil/braid combination can be used.

- **Solid or stranded conductors?** Solid conductors are appropriate for most installations; stranded conductors provide extra flexibility for better handling in close environments. For robotic/continuous flex applications, use of a cable with a highly stranded conductor is recommended.

- **Pair conformity/centricity:** Bonded-Pair cables provide resis-tance to the rigors of installation by utilizing a manufacturing technique that affixes the insulation of the cable pairs along their longitudinal axes so no gaps can develop between the conductor pairs; a nonbonded-pair cable construction can be susceptible to pair-gapping during installation (and impedance mismatches).

- **Insulations:** Most industrial-grade Ethernet cables utilize a polyolefin insulation. For extreme temperatures, however, an FEP insulation (and jacket) is recommended.

- **Jackets:** Oil- and sunlight-resistant cables typically have a PVC jacket. If the cables are exposed to moisture, a waterblocking agent should be part of the cable's construction, as well as inner and outer PE jackets if the cable is buried. Gas-resistance calls for an FEP-jacketed cable, while low smoke zero halogen (LSZH) PVC jackets are available for environments where smoke/flames are a risk. For extreme temperature environments, the cables should feature an FEP jacket (for an extended operating temperature of -70ºC to +150ºC). And, for continuous flexing or robotic applications (which could include the complication of weld splatter), cables with TPE inner and outer jackets are recommended.

The Proof is in the Testing

A series of rigorous tests conducted by Belden on COTS cables versus industrial-grade cables has proven that the COTS cables simply do not stand up as well as industrial-grade Ethernet cables in harsh environments. All nine tests were performed on state-of-the-art testing equipment, and all the cables used in the study initially tested as fully compliant to ANSI/TIA/EIA 568-B.2 Cat 5e standards. Following is a summary of tests performed and the results:

Abrasion. Using a fixed drum covered with sandpaper, cables were stretched across a portion of its circumference, then moved back and forth cyclically for 25 cycle counts. At that point, the conductors of the COTS cable could be seen through breaks in the jacket, which would cause it to lose mechanical and electrical integrity. **The pairs of the armored industrial cable were not compromised.**
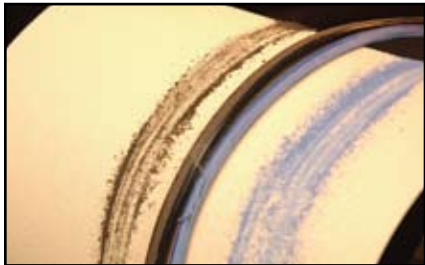
The test set-up — with the cables on a fixed drum covered with sandpaper.

Commercial cable after 25 cycles.

Industrial cable after 25 cycles.

Cold Bend. Conducted per UL 444, samples of cables were left in a controlled temperature and humidity chamber called a cold box. They remained for one hour prior to testing. They were then tested (at -80°C, -60°C, and -40°C) by being partially wound around a 3-inch diameter horizontal mandrel with one end of the cable under tension from an aluminum weight. The cables were then unrolled and visually inspected to check for cracks in the jacket. The COTS cable became brittle and showed visible cracks. **The industrial-grade high/low temp cable had no visible damage.**

In the cold bend test, the cables were first placed into a cold box.

After the cold box, the cables were partially wound around a mandrel and subjected to the tension experienced through the use of an aluminum weight.

Cold Impact. In this test, also conducted per UL 444, an aluminum weight was dropped down a hollow guide-tube to smash against a segment of cable under test. The impact force delivered 24 in-lbs or 2.7 joules of impact energy. Each length of cable had been previously cooled; and a total of ten samples were inspected at a series of increasingly lower temperatures to determine if the cables' jacket integrity was damaged, a condition which could allow ingress of chemicals and moisture and could potential lead to a conductor-to-conductor short or even catastrophic failure. The standard jacketed COTS cables failed at -20°C. **The industrial-grade cables, protected by high-low temperature jackets, did not crack until impacted at -70°C.**

In the cold impact test, after the cable is cooled an aluminum weight smashes against it.

Crushing. In this test, an Instron machine head brings a 2-inch by 2-inch plate down on a segment of cable to crush it — with failure defined as the point at which the cable would no longer reliably support Cat 5e performance. Each cable's electrical characteristics were measure throughout the testing. At 400 lbs applied force, the COTS cable with PVC jacket failed — it was smashed flat and would not spring back to its original shape. **The industrial-grade, black-jacketed armored cable had a failure value of 2,250 lbs — over a ton.**

Cut-Through. In this test, based on CSA standard #22.2, a chisel-point mandrel on an Instron machine was lowered onto a segment of cable to test the cable's susceptibility to a cut-through leaving the conductor exposed. Several kinds of cable were sliced by the chisel to the point where a short circuit was sensed across the conductors, creating a potentially hazardous situation. The COTS cable shorted out at 92 lbs of applied force. Two unarmored industrial-grade cables took 205 lbs and 346 lbs of applied force to short. **The armored industrial cable took 346 lbs applied force to pierce the armor; however, the conductors did not short until a force of 1,048 lbs was applied.**

High Temperature. In this test, three spools of cable were suspended from a mandrel in a high-temperature oven. The blue cable in the middle is a COTS Cat 5e cable with standard PVC jacket. The two are black industrial-grade Cat 5e cables, one with a PVC jacket, the other jacketed in FEP. All cables were first tested at an ambient temperature of 20°C and were then tested again after being exposed to a high temperature of 60°C over time. The COTS cable functioned acceptably at 20°C but, over time, at 60°C, attenuation increased to where the cable would not support a run distance of 100 meters. **The industrial-grade cables, even after exposure to 60°C over time, continued to support the maximum run distance.**

The Instron crushing device.

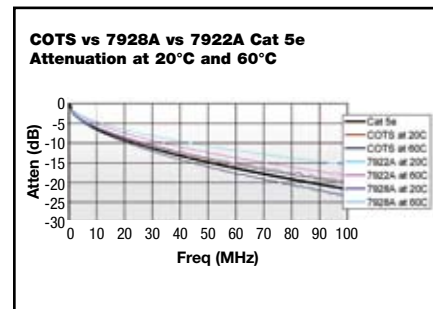A chisel-point mandrel on an Instron machine performs the cut-through procedure.

The cables were tested, as suspended, in a high temp oven.

The COTS cable is smashed flat and fails at 400 lbs.

The industrial-grade armored cable fails only after a ton of crush pressure.

COTS vs 7928A vs 7922A Cat 5e Attenuation at 20°C and 60°C

The industrial-grade cable showed little attenuation — even at 60°C.

Oil Resistance. In this test, conducted per UL 1277, lengths of cable were immersed in containers of oil, which in turn were immersed in a water bath that was placed in a chamber held at 125°C for 60 days. After the test period, cable segments were removed and their jackets evaluated for tensile and elongation properties. Exposure to oil and lubricants can make jacketing brittle and fragile, even at room temperature, resulting in loss of mechanical properties and reduced service life. The blue COTS cable showed signs of this type of deterioration. **The industrial cable's jacket did not, because the materials and jacket thickness are rated for exposure to oil and other substances, even at elevated temperatures.**

UV Exposure. In this procedure-based ASTM G 154 test (Standard Practices for Operating Fluorescent Light Apparatus for UV Exposure of Non-Metallic Materials), segments of various cables were affixed to panels that were mounted so that the cables directly faced a fluorescent light source whose output range was adjusted to match that of solar radiation levels. The cables were exposed to light for 720 hours (30 days), then their jackets were visually checked for discoloration, as well as for signs of degradation in tensile strength and elongation. The COTS cable was not sunlight-resistant and their jackets showed discoloration, a precursor to degradation of the jacket material. **The industrial–grade cables were rated to resist the effects of sunlight and other UV sources and showed no jacket damage.**

Water Immersion. In this test, the electrical properties of the cables (primarily attenuation) were measured initially. Then the cables were coiled into a dry container, and water was added to submerge them. The cables were tested intermittently over a six-month period. The COTS cable showed increased attenuation as soon as the cable was immersed in water and this continued to degrade over the half-year immersion. **After six months of immersion, the industrial–grade cable showed only a slight increase in attenuation — and the cable still exceeded the Cat 5e requirements.**

The oil bath test, conducted as specified in UL 1277.

The UV exposure test is based upon ASTM procedures.

The water bath test is a six-month long test, with the cables fully submerged in water.

Ethernet Switch Selection Options

Wireless or Wired?

While wireless has its advantages in industrial applications, it is poorly suited for transmitting time-sensitive control data that could adversely affect productivity or safety.

Wireless

Pros: Provides mobility and network flexibility. Limited cabling costs. Overall convenience.

Cons: Not as reliable or as secure as a cabled solution. Larger and more complex networks require a site survey. Achieving long distance communications reliably can be very difficult.

Wired

Pros: Significantly more reliable and secure. Far higher data speeds are possible — up to 10 Gigabit with some wired switches.

Cons: Lower flexibility. High initial cost of cabling and the cost of relocating an Ethernet device (if it will not be close to a network connection/port).

DIN Rail, 19" Rack or Panel Mounted?

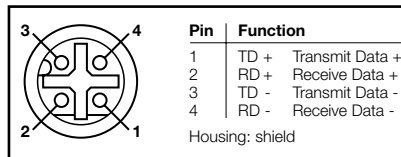The mounting choice/preference will dictate which products are applicable.

DIN Rail Mount: Managed and unmanaged open rail switches, unmanaged switches, and wireless Ethernet devices.

Rack Mount: Some suppliers offer a DIN rail adapter for 19" racks, permitting multiple DIN rail mount devices to be mounted inside a 19" rack.

Panel Mount: A variety of switches and wireless Ethernet devices are available, some with adapters for panel mounting. Some companies offer ultra-rugged switch options for use in extreme environments.

IP67 Ethernet Connectors?

IP67-rated connectors are ideal for use in extremely damp/wet environments and applications where significant vibration could result in intermittent communication from connector contact deterioration. The connector, approved by the ODVA (Open Device Vendor Association), is the M12 D-code Ethernet connector — a 4-pin connector that uses CAT 5e or better (2-pair).

Pin	Function	
1	TD +	Transmit Data +
2	RD +	Receive Data +
3	TD -	Transmit Data -
4	RD -	Receive Data -
Housing: shield		

The IP67/waterproof connector solution is typically available as field-installable connectors or pre-terminated and overmolded patch cords (single M12 or RJ45 or double ended M12-M12, M12-RJ45 and RJ45-RJ45). A bulkhead M12 is an excellent solution for migrating the Ethernet cable from the inside of the control panel to the outside.

Keep in mind that the IP67 rating is not always used in wet environments or applications where vibration is an issue: Some users choose instead to deploy all M12 D-code connectors so that they can eliminate control panels.

This Hirschmann OCTOPUS switch is ideal for installation in vibration-prone environments. Here, the Ethernet IP67 switch is used to provide passenger compartment video surveillance, as well as travel updates and entertainment.

Managed or Unmanaged Switches?

A classic analogy for management has always been the dashboard and electronics of a car:

A **managed switch** is akin to a car with a dashboard and an unmanaged switch is one without. A managed switch can, through web browser access (secured by password), control certain internal switch functionality that may be critical to the flow of data and the function of the network. A managed switch also has the ability to inform and react to certain conditions and provide a level of security, making it an ideal solution for an application with a higher need for uptime (where control data, rather than measurement data is transmitted).

An **unmanaged switch** has none of this functionality and is typically a plug-and-play switch and is best used on smaller stand-alone applications or as an edge-switch in a larger network.

Hardware: Switches, Active Network Devices and Accessories

A wide range of hardware is available to enable management of industrial Ethernet networks at the information, control and device levels. There are products to support both copper and optical fiber media, as well as switches capable of data speeds as high as 10 Gigabits per second. At a minimum, all of these network components — switches, connectors, and other hardware — should offer robust construction and resistance to high temperatures, vibration and EMI.

The Importance of Redundancy

Another Ethernet factor considered to be an industry best practice for mission-critical applications is redundancy, which is extremely important but sometimes overlooked in selecting industrial Ethernet switches. Two specific kinds of redundancy are key to maintaining uninterrupted signal transmission and maximum uptime.

Power source redundancy. Having an uninterruptible power source (UPS) is absolutely critical to consistent and reliable switch performance. Specifying switches that have dual power input capabilities means that if one power source fails, the other immediately takes over.

Data path redundancy. The daisy-chain network topologies used by many industrial plants to connect automated machinery and devices have one inherent flaw: if any link between the two switches fails, the entire system could potentially go down, as the devices on one network segment can no longer communicate with devices in other segments. The solution is to build in a redundant data path which can take the form of either a ring or mesh topology.

- **Ring Topology.** In a ring configuration, the easier and simpler of the two types, a series of managed switches are daisy-chained and the first and last switch of the chain are then linked to form a ring. In the event of a failure in the media or any of the switches, data is automatically re-routed, achieving network resiliency in milliseconds.

- **Mesh Topology.** Mesh topologies require that all switches in the mesh support STP (Spanning Tree Protocol) or RSTP (Rapid Spanning Tree Protocol). While supported by most managed switches, this feature can be difficult to configure and network recovery can be several seconds — depending on the number of switches in the mesh and how the fail-over is configured.

Industrial Ethernet Hardware Standards and Specifications

Temperature and Humidity/Moisture

Typical industrial temperature range is 0° to +60°C

Extended temperature range components are available from -40° up to +85°C

IP20/IP30/IP67 (95% relative humidity, non-condensing — not applicable to IP67

IP classifications are governed by the IEC 429 standard

Mechanical Stability

Shock and vibration tests should be in accordance with PLC standards IEC 1131-2, EC 60068

Electric Requirements

EMI: EN 50022-2, FCC part15 (class B)

IEC 1000-4-2, IEC 1000-4-6, IEC 1000-4-4, EN 61000

Certifications

cUL 508 — the basic and most common safety standard for industrial control equipment

cUL 1604 — the standard for Class 1, Division 2, hazardous locations

IEC 61850-3 — the standard for electrical substation automation networks

IEEE 1613 — the standard for communications networking devices in electrical substations

EN50155 — European specification for onboard rolling stock/train applications

EN50121-4 — European specification for track-side rail applications

NEMA TS-2 — US-based standard for traffic signaling and communications

ATEX100A, ZONE 2 — a standard required in Europe for hazardous/explosive environments (similar to, but not compatible with cUL 1604 Class 1, Div 2)

GL (Germanischer Lloyd) — a German standard that has gained global acceptance for marine (ship, offshore oil, etc.), some petroleum and wind industries

Belden logo: BELDEN — SENDING ALL THE RIGHT SIGNALS

Be Sure Hardware Components Match the Application

As with selection of the network's cabling, it is critical to ensure that the specifications of the active hardware are suited to the application. Some factors to keep in mind when making buying decisions include:

- **Temperature.** Standard PLC requirements are 0-60°C (a standard met by most industrial switches), but some applications can present an ambient temperature as high as 85°C and as low as -40°C. Note: Although most switches will run at extremely low temperatures, many will not start up after having been idle.
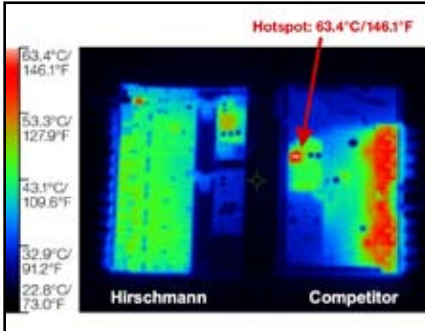
Typical industrial Ethernet hardware is rated for temperature ranges of 0° to +60°C. Most Hirschmann switches offer an extended range of -40° to +70° C, or up to +85° C and beyond. This thermal photograph demonstrates the superior heat-resistant performance of Hirschmann industrial Ethernet switches over a typical industrial-grade switch.

- **Moisture**. Conformal coating or IP67 housing solutions can negate these issues. The IP67 connectivity of choice is the ODVA-approved M12 D-code Ethernet connectors (a 4-pin circular connector that is available as a field-installable IP67/waterproof connector or as pre-terminated patchcords using Cat 5e with an industry-appropriate jacket material).

- **Shock and vibration.** Even the minutest vibration on a plant floor can wear on the RJ45 connections over time, causing intermittent data communication. For application such as this, look for switches that utilize the M12 D-code connector.

- **Industry Approvals.** While UL508, the requirement for all automation equipment, is a must-have, some often negate to take into consideration the other approvals that are common to the various automation markets.

  - cUL1604 — The standard for Class I, Division 2, hazardous locations

  - IEC 61850-3 and IEEE 1613 — The standard for electrical substation automation networks

    EN50155 and EN50121-4 A — Railway networking/communication specifications

An Industrial Ethernet Infrastructure Built to Last

Field-proven Solutions Deliver Proven Reliability. The most effective — and cost-effective — path to ensuring long-term performance and reliability of the industrial Ethernet is to find and invest in network infrastructure components designed and rated specifically for use in harsh and demanding environments. End-to-end industrial-grade products are more ruggedly engineered and constructed in every way, incorporating design features and materials capable of withstanding the severe environmental and physical stressors to which they are subjected every day.

End-to-End Integration Ensures Optimum Interoperability. During the selection process, it is important to take the time to evaluate the marketplace and select a qualified supplier capable of providing a top-quality, end-to-end Ethernet framework tailored to

Belden's matched, end-to-end "Complete Industrial Solution" for Ethernet includes Hirschmann™-branded switches/active network devices and networking software, Lumberg Automation™ -branded connectivity and Belden® cable.

the application and environmental conditions. As many adopters of industrial Ethernet have already discovered, taking a "total system" approach will result in a more integrated system with all products seamlessly matched to deliver interoperability and consistently reliable performance day after day, and year after year.

Conclusion

Most industrial organizations invest significantly to protect the safety and security of their production processes, and to provide workers with safety and protective gear, such as hard hats, safety glasses, gloves and footwear. Doesn't it make good business sense to invest wisely to preserve, protect and defend the data network infrastructure that supports all of the facility's mission-critical information, automation and control functions?