BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

WP00022

The Case for Specifying Industrial Ethernet Cable for Harsh Environments

Brian Shuman
Senior Product Engineering
Project Manager
Industrial Cable Belden

Table of Contents

Be certain.
Belden.

Executive Summary

Network uptime is the single most critical concern of industrial automation and control applications. Each second of downtime equals money lost – through lower production, costly repairs, or maintenance and worker safety expenses. To maintain high reliability and availability of systems and data communication, networks must be built on a robust and dependable infrastructure.

Today, industrial Ethernet is the principal network infrastructure choice for mission-critical operations. 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 through a single platform.

This convergence of open, standards-based Ethernet communications enables secure, seamless interoperability among manufacturing enterprise networks – from corporate offices to the shop floor to remote locations – and offers Internet and enterprise connectivity, anytime and anywhere.

And as more smart devices connect to the Internet and produce rapidly growing amounts of data through a movement known as the Industrial Internet of Things (IIoT) – networks built on industrial Ethernet technology ensure flexibility for future expansion and change.

It is also critical to note that while the base technology is the same, enterprise-grade products are not appropriate for use in industrial networks. The industrial applications previously mentioned operate in drastically different environments. Products designed for use in a simple, clean and stable office setting will not be able to withstand the harsh, extreme and relentless conditions found in an industrial setting. Industrial-grade solutions are built with these extremes in mind and feature unique protections to enable long-standing, reliable operation, no matter the environment.

This white paper will address the risks and priorities of industrial networking, as well as key considerations when selecting physical layer products and solutions to support an industrial Ethernet infrastructure.

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Realizing Key Business Benefits

In addition to system integration and interoperability, there are many other key business benefits to a complete, end-to-end Ethernet solution – from cabling and connectivity, to active components and associated hardware. These benefits include lower overall total cost of ownership (TCO) and higher return on investment (ROI) through 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 industrial facility and enterprise levels include:

- Faster and less costly plant upgrades, expansions and change-outs
- Access to real-time data to improve overall operations
- Faster installation and remote troubleshooting
- Real-time inventory visibility and increased production capacity
- Integration with enterprise resource planning (ERP) for scheduling, planning, quality tracking and delivery information

The plant or shop floor is just one example of an industrial setting. The term 'industry' is broad and encompasses many diverse operations – from discrete manufacturing of every kind; to the 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. Industrial-grade products are also relevant for other uses, such as sensors in the pavement at a stoplight, intelligent parking meter systems, or campus security measures, like pan-tilt-zoom cameras and call boxes. While each industry is unique, they all share common factors, such as environmental risks and business priorities.

Addressing Network Priorities: Uptime, Safety and Control

Untimely and costly disruptions can largely be prevented through a well-planned and executed network infrastructure that incorporates environmentally hardened, industrial-grade components in the physical, data link and network layers[1]. A ruggedly designed framework enables industrial enterprises to carry out their mission-critical functions by providing the highest possible levels of:

1. **Uptime.** Preventing signal transmission problems is a major factor in ensuring consistent and dependable network uptime and productivity. Whether an operation involves a discrete manufacturing facility, a processing plant or an airport, keeping operations running smoothly and reliably assures maximum uptime and peace of mind for network managers – who want to attain 99.999 percent uptime or better. Any network failure, and subsequent downtime, also results in severe and extremely costly consequences.
2. **Safety.** Optimum safety is critical to protect people and processes in all industrial operations. These applications demand fail-safe reliability and redundancy of data transmissions, as well as network components that meet and exceed the requirements for hazardous environments.
3. **Control.** Industrial facilities rely heavily on their automation, instrumentation and control data communications to relay signals between devices, machinery and the control system. This communication triggers events and functions on a very specific and pre-determined schedule, with little or no margin for error. Continuous monitoring, management and control drives operational efficiencies and potential cost savings.

Identifying Risks: Top Environmental Factors Facing Industrial Applications

Networks in all industrial operations must perform in extreme and often hazardous environments and every operation has its own set of environmental challenges. But no matter the conditions, industrial communications and control networks are expected to operate consistently and reliably by withstanding high operating temperatures, power or voltage fluctuations, UV exposure, machine vibration, electromagnetic interference (EMI), mechanical hazards, and other special industrial criteria.

Food and Beverage

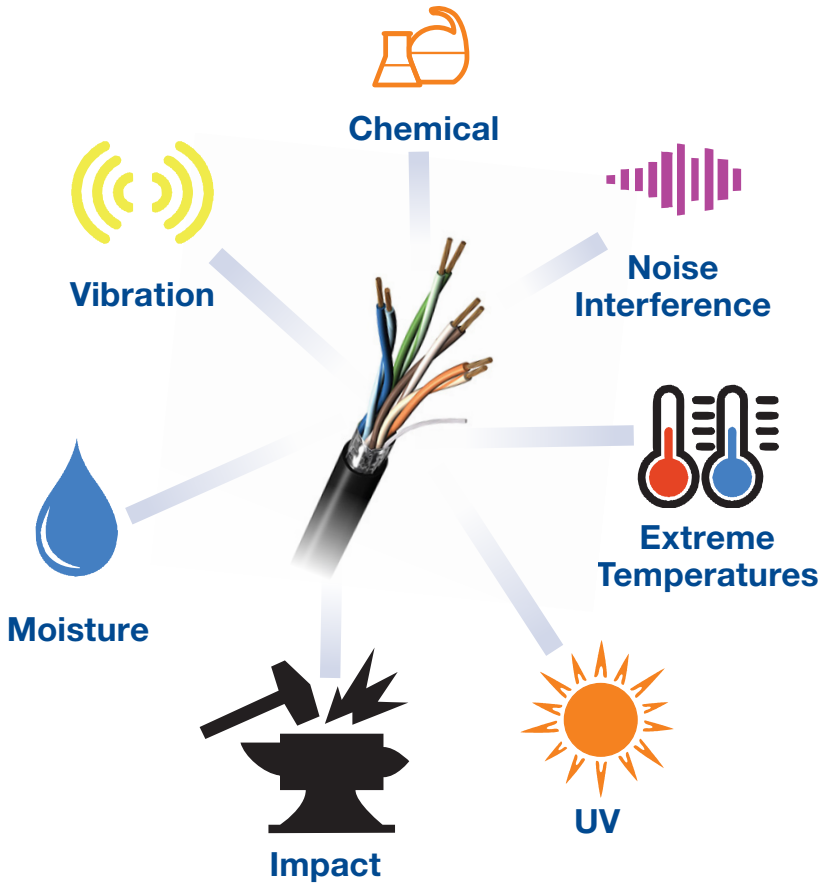
To meet stringent hygiene requirements, communications network components face regular, high-intensity cleanings, commonly referred to as "wash-downs" or "splash zones," and must be able to withstand the caustic cleaning chemicals and high-pressure water. Systems in the food and beverage industry must also deal with motion during packaging, extreme temperature and moisture/humidity from freezers and ovens during processes, like pasteurization, as well as high noise sensitivity in order to fill precise measurements.

Machine Building

To handle the constant, and often extreme, motion of packaging lines, assembly cells and transport belts, this highly automated equipment must deal with tight spaces, elevated levels of electrical noise, changing electrical currents, prolonged vibration and vigorous torque. Several environmental factors are also at play, such as resistance to oils and solvents, chemicals, welding spatter, and dust.

Chemical Processing

In the chemical processing industry, any communications network components used must be able to withstand many outdoor environmental conditions, including sunlight, extreme temperatures,



In the traditional office environment, you don't have to be concerned about cable exposure to abrasive chemicals, extreme temperatures, heavy vibration or water and other fluids. That's not true in the unforgiving settings where machines, automation and manufacturing equipment live.

damage from rodents, excessive moisture from rainfall, mist or fog, and have the ability to operate when buried underground.

Drive-Thru Restaurant

Even non-traditional applications require robust solutions. For example, outdoor ordering boards at drive-thru restaurants are exposed to temperature extremes, humidity, sunlight, corrosive cleaning chemicals, dust, extreme moisture and humidity, rainfall, grit, and sludge. The cars that drive by may also expose the equipment to oil, gas and caustic fumes. This application is very similar to the connectivity needs at gas station pumps or parking meters on city streets.

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 safety issues, and may ultimately lead to loss of critical data, costly downtime, or even catastrophic failure.

Assessing the Impact: The Real Costs of Network Failure

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 fails, the cost of replacement parts and repair represents only a tiny fraction of the overall costs associated with production downtime.

Many instances of unplanned downtime in industrial operations can be attributed to network infrastructure failure, and that downtime is costly. According to one survey of manufacturing executives in the automotive industry, downtime can cost companies an average of $22,000 per minute[2].

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 facility's mission-critical output. If a cabling system component or Ethernet switch fails, the repair and labor costs alone could be 15-20 times the cost of the component itself. 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 the obvious business choice – one that can provide tremendous peace-of-mind to network engineers and administrators and the organizations they serve.

Identifying a Solution: Key Considerations

Given many network performance problems are due to failure at the physical media layer[3] – it is critical to ensure that components 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.

Comparing Commercial vs. Industrial-Grade Components

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 with network switches, hardware and connectivity components sheltered in protected areas.

Industrial facilities present a very different reality. Here, many, if not most, cables and connectors 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 these conditions over time. Extreme conditions call for ruggedized cables.

Consider, for example, the harmful effects these 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 construction of the cables and cause an increase in attenuation. Industrial-grade cables can operate in a far wider temperature range (-40° C to +85° C) than COTS cables (0° C to +60° C).
- **Chemical Exposure.** Oils, solvents, chemicals and cleaning solutions can soak into COTS cables, especially under the stress of heat, causing the cable jacket to swell and lose mechanical strength.
- **UV Radiation.** Exposure to sunlight can cause COTS cable jackets to decompose at an accelerated rate, compromising mechanical strength and electrical performance.
- **Physical Hazards.** Industrial settings present 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 degrade electrical performance and increase susceptibility to ambient electromagnetic interference (EMI) or radio-frequency interference (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 in every day industrial settings.

The Proof is in the Testing[4]

An office and an industrial setting couldn't be more different – especially when you consider the level of stress placed on Ethernet cabling systems or adverse effects environmental conditions can have on active devices. Belden has done extensive testing to compare both the physical and electrical performance of COTS cables versus industrial cables. The results of each test clearly indicate why a commercial-grade cable is never suitable for the wide variety of extreme conditions commonly seen in an industrial environment.

Abrasion. Cables were stretched across a fixed drum covered with rough sandpaper and moved back and forth 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 armored industrial cables were not compromised.

Cold Bend. Cables were left in a cold box for one hour then wound around a mandrel with one end of the cable placed under tension from an aluminum weight. When unrolled and inspected, the COTS cable became brittle and showed visible cracks. The industrial-grade high/low temp cable had no visible damage.

Cold Impact. An aluminum weight was dropped to smash against a segment of cooled cable. Ten samples were inspected at a series of increasingly lower temperatures. 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.

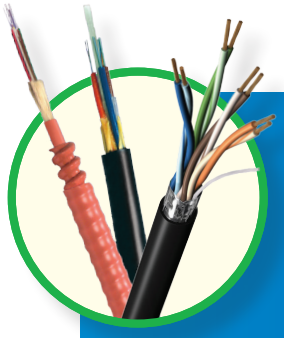
Crushing. An Instron crushing device was used to determine the point at which a cable could no longer reliably support Cat 5e applications. The COTS cable with a PVC jacket failed at 400 pounds applied force. The industrial-grade, black-jacketed armored cable failed only after 2,250 pounds – more than a ton of applied force.

Cut-Through. A chisel-point mandrel on an Instron machine was lowered onto a segment of cable to test the cable's susceptibility to being cut-through, leaving the conductor exposed. The COTS cable shorted out at 92 pounds of applied force. The armored industrial cable took 346 pounds applied force to pierce the armor; however, the conductors did not short until a force of 1,048 pounds was applied.

High Temperature. Three types of cables were placed in a high-temperature oven – a COTS Cat 5e cable with standard PVC jacket, an industrial-grade Cat 5e cable with a PVC jacket, and an industrial-grade Cat 5e cable with an FEP jacket. 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. Both of the industrial-grade cables, even after exposure to +60° C over time, continued to support the maximum run distance.

Oil Resistance. Cables were immersed in containers of oil, then in water, and finally held in a +125° C chamber for 60 days. The COTS cable showed signs 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. Cables were exposed to fluorescent light that mimicked solar radiation levels for 720 hours (30 days). The COTS cable was not sunlight-resistant and their jackets showed discoloration,



Selecting an Industrial Ethernet Cable: Fiber or Copper?

Fiber optic Ethernet cables represent the ultimate in future-proofing and are available for indoor or outdoor use, including burying underground. Typical designs use multimode fibers in a loose tube configuration, usually available in 2- to 72-fiber constructions.

Other fiber cable considerations include the following:

- 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 chlorinated polyethylene (CPE) outer jacket will provide additional protection against chemicals or abrasion. An armor tape or aluminum/steel armoring may also be appropriate for extreme environments, including some burial situations.
- A basic, COTS fiber optic cable will likely not withstand industrial conditions – a fiber optic Ethernet cable, designed with ruggedized features to operate in industrial settings, is needed.
- Ratings include:
  - UL Type: Optical fiber, nonconductive riser (OFNR)
  - cUL Type: OFN FT4
  - IEEE 383-2003 Flame Test

Copper Ethernet cables are the more traditional option in industrial installations, available for Cat 5e, Cat 6 or Cat 6a applications.

Other copper cable considerations include:

- Cat 5e cables are still widely used today, however new installations favor the use of Cat 6 cables to meet Gigabit speeds and increased bandwidth. Cat 6a cables are also an option for extreme future-proofing.
- Cat 5e, Cat 6 and Cat 6a twisted pair cables are available using any number of conductor types, insulations, shielding and jackets.
- Armoring is also available for extremely harsh environments.

Additional Selection Criteria Include:

- Unshielded or shielded? Unshielded products can be used in most environments, while shielded products are recommended for environments with high noise.
- Shields. Typically, a foil 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, while stranded conductors provide extra flexibility for better handling in small spaces. For robotic/continuous flex applications, use of a cable with a highly stranded conductor is recommended.
- Pair conformity/centricity. Bonded-pair cables provide resistance 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 (resulting in impedance mismatches).
- Insulation. Most industrial-grade Ethernet cables utilize a polyolefin insulation. For extreme temperatures, however, a fluorinated ethylene propylene (FEP) insulation and jacket is recommended.
- Jackets. Oil- and sunlight-resistant cables typically have a polyvinyl chloride (PVC) jacket. If the cables are exposed to moisture, a water-blocking agent should be part of the cable's construction, as well as inner and outer polyethylene (PE) jackets if the cable is buried. Gas-resistance calls for an FEP-jacketed cable, while LSZH jackets are available for environments where smoke/flames are a risk, in order to avoid smoke toxicity for safety reasons. For extreme temperature environments, the cables should feature an FEP jacket (for an extended operating temperature of -70° C to +150° C). And, for continuous flexing or robotic applications, which could include the complication of welding spatter, cables with thermoplastic elastomer (TPE) inner and outer jackets are recommended.

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. Cables were coiled and submerged in water, and then tested intermittently over a six-month period. The COTS cable showed increased attenuation as soon as it was immersed in water and 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.

Physical Media – Cabling and Connectivity
For the physical media layer, there are many solutions available that fully conform to the IEEE 802.3 Local Area Network (LAN) standard. Selection will depend on each facility's network configuration and application requirements. These physical media products may 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), Cat 6 (4-pair) and Cat 6a (4-pair) cables with heavy-duty, oil- and UV-resistant jackets. Some category cables feature a bonded-pair technology, which delivers superior electrical stability in the harshest of environments.
- 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), water-blocked and/or burial cables.
- 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.

Extreme Conditions?
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 Open Device Vendor Association (ODVA), is the M12 D-code Ethernet connector — a 4-pin connector that uses Cat 5e or better (2-pair).

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.

Meeting Industrial Ethernet Standards and Approvals

Industrial facilities' networking products must meet or exceed stringent industrial regulations and ratings. When designing a network infrastructure, consider these common certifications and ensure any selected products meet the requirements necessary for the network's vertical market or application.

- UL CMR-CMX Outdoor – the basic and most common safety standard for communication cable
- C(UL) CMG FT-4 – the basic and most common safety standard for Canada
- UL Verification Cat 5e/6/6a – third-party testing of electrical performance
- UL Power Limited Tray Cable (PLTC) – the basic rating for installation in 300V power trays
- UL Tray Cable (TC) – the basic rating for installation in 600V power trays

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 where needed. Doesn't it make good business sense to invest wisely to preserve, protect and defend the network infrastructure that supports all of the facility's mission-critical information, automation and control functions?

The most effective – and cost-effective – way to ensure long-term network performance and reliability is to invest in an industrial Ethernet infrastructure with networking components designed and rated specifically for use in harsh and demanding environments. Components in the physical layer are especially vulnerable and costly to replace. It's also important to keep in mind that Enterprise-grade products are neither designed for, nor intended for use in, industrial markets or applications; do not risk your network uptime by using COTS cables, which cannot stand up to harsh environments. Industrial-grade products are far more ruggedly engineered and constructed, and they incorporate design features and materials capable of withstanding the severe environmental and physical stressors to which they are subjected every day.

During the product 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 the specific 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.

References

1. OSI Reference Model (Open Systems Interconnection) definition. TechTarget.com. http://searchnetworking.techtarget.com/definition/OSI
2. Downtime Costs Auto Industry $22k/Minute. http://news.thomasnet.com/companystory/downtime-costs-auto-industry-22k-minute-survey-481017 (March 27, 2006)
3. Source: Datacom Mag, Network Management Special
4. Nine tests published in the Industrial Ethernet User Guide, IEUG002 2008

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.belden.com and follow us on Twitter @BeldenIND.