How to avoid a USB meltdown in harsh environments

USB is useful, but can be dangerous as well

On a rainy day in 1937 the German airship Hindenburg arrived in Lakehurst, NJ, after a trans-oceanic flight. The ship dropped its mooring ropes, and a few minutes later it went up in flames. Theories about the fire include exotic tales of sabotage, but most scientists agree that the true culprit was an electrostatic discharge (ESD). And they agree that the potential for disaster was designed into the Hindenburg right from the very beginning.

The problem was a matter of simple physics. Hindenburg’s fabric outer cover was connected to the duralumin frame with non-conductive ramie cords. The cords were coated with a light metal covering that was intended to improve conductivity, but it wasn’t very effective. As a result, the outer skin and the duralumin frame were able to develop very large differences in electrical potential. And on its approach to Lakehurst the Hindenburg passed through a weather front with a high electrical charge.

Upon its arrival, still in the rain, the airship dropped its mooring ropes. Within minutes the ropes were wet enough to ground the airship. When they did, an electrostatic discharge jumped between the Hindenburg’s cover and its duralumin frame. Theorists have argued about the ensuing fire, and whether it was initially fueled by a leaking hydrogen cell or flammable paint on the fabric cover. But they don’t disagree about the end result. The Hindenburg was consumed in less than one minute.

Like the Hindenburg, USB has potential trouble designed in. This article will discuss the problem, and what can be done to remedy it.

The USB Specification

Indiana Jones and the Last Crusade is set in 1938. Had it been real life, Jones could never have his zeppelin adventure. (Commercial airship service had come to its abrupt end the year before.) But he might easily have lived long enough to see the introduction of electronic data communications and factory automation. He might even have lived long enough to see the introduction of USB.

Developed to be a universal serial bus, hence the name, USB was intended to simplify and standardize the connection of computer peripherals and to eliminate much of the need for specialized expansion cards, which were installed by opening the computer case and physically adding new parts to the machine. And it has proven to be a great improvement upon earlier data communications standards. USB not only simplifies installation; it allows you to connect up to 127 devices to a single port, devices are hot swappable, and it will supply 5 VDC power downstream. We’ve come a long way since the days of airships and singing telegrams. But the laws of physics have remained the same, and USB can’t get around them.

The Hindenburg Revisited.

USB was designed for safe office and IT environments. When it moves off the desktop into industrial applications it’s subject to serious electrical problems. They’re a function of its basic design.

Note that a standard USB cable contains four wires. Two are meant to carry the data, and two carry 5 VDC power for downstream devices. (See Fig. 1) Whereas other types of industrial communication, like RS-485, can use differential signal transmission with no ground connection, the ground connection in a USB cable is unavoidable. And it means that USB can easily transfer spikes, surges and ESD strikes to connected devices and computers.

Electrostatic discharges, for example, happen all the time. We’ve all experienced them -- just walking on some carpet and touching the family dog’s nose is enough to give both of you a sudden surprise. Like the Hindenburg’s outer cover, we’re all changing our electrical potentials every time we move around. But USB is deliberately designed to be hot swappable. We’re expected to connect and disconnect USB cables over and over again, and there’s a chance of an ESD strike every time we do. Your trip across the carpet can generate ESD levels higher than 15 kV, and the typical level of ESD protection in an IC chip is usually going to be closer to 2 kV.
And because USB carries power, and has a connecting ground wire, there is an ever-present risk for ground loops. That’s rarely an issue in consumer applications, where distances are short and connected devices normally share a common ground via a nearby wall outlet. But industrial applications are likely to be much more complex. Various pieces of equipment will be powered from entirely different building ground references. A process control system and the front panel may be separated by hundreds of meters. They may not even be in the same building. When you connect a PC to the panel via USB you may also be creating a ground loop path for a remote device with a very different building ground reference.

USB cables aren’t helplessly vulnerable to electromagnetic interference (EMI). They do use twisted pair wire on the data lines and there should be some copper braid and aluminum shielding. (See Fig. 1) In desktop applications any EMI issues will be insignificant. But it’s a different story when a length of USB cable is exposed to the strong magnetic fields associated with industrial motors. Powerful currents will be induced on the USB cable. The results may include anything from data loss and downtime to burned circuitry in connected devices.

Arcing
One of USB’s great advantages is simultaneously one of its weaknesses. USB hubs provide 5 VDC power to downstream devices at up to 500 mA. Current is allocated in units of 100 mA, and devices may draw up to 500 mA per port. If the hub is bus powered it can’t provide more than four 100 mA units of current to downstream devices, as it needs one unit for itself. And it can’t have more than four downstream ports. But if a hub has its own power supply it can provide the full 500 mA to every port. (Computers normally have a powered USB hub built in.)

This ability to power gadgetry like cameras and external hard drives via a USB port is quite convenient. But conditions can get rough in the industrial world. Shock and vibration are common occurrences and USB cables can work themselves loose. They can also be dislodged accidentally, when workers are moving things about. When that happens, the same 5 VDC that is so useful in benign environments becomes a serious fire hazard. If it arcs, and flammable gases or materials are present, you’ve got trouble.

Solutions: Range Extension
USB doesn’t have great range. Even with hubs, the best you can do is 30 meters. As cable is normally laid above, below and around working spaces, and as industrial working spaces can be very large indeed, 30 meters isn’t much. Your network will most likely involve various kinds of extension and conversion, and some of them automatically resolve USB’s electrical issues while they’re extending its range.

Fiber optics, for example, not only give data communications incredible range, they eliminate the risk for grounds loops, power surges and EMI. As data travels on a beam of light, rather than a copper core, fiber optic cable is immune to electrical issues of any kind. Single-mode fiber has the greatest bandwidth, but is also more expensive than multi-mode. And in both cases the cabling, transceivers and receivers are more expensive than the materials used in a copper cable installation. But a large part of any installation, fiber or copper, is actually going to be labor cost. Fiber’s immunity to damaging electrical currents, and the protection it provides to connected devices, can more than make up the difference.

Solutions: Wireless
Wi-Fi is rapidly becoming another viable option for industrial installations. Wireless networking used to be plagued by issues like multipath propagation, the phenomenon that occurs when transmitted signals bounce off intervening objects. Different parts of the signal would arrive at the receiver at different times and out of sequence. If multipath propagation got bad enough, early Wi-Fi devices couldn’t distinguish between the signal and the noise floor. But the current 802.11n Wi-Fi standard provides for the use of multiple input multiple output (MIMO) technology. MIMO devices anticipate multipath propagation and turn it into an advantage. They deploy multiple antennas at both the transmitting and receiving sides of the wireless connection, and they split the data into numerous spatial streams. The streams are transmitted through separate antennas and collected by corresponding antennas in the receiving devices, where onboard software uses signal processing algorithms to correct and interpret the incoming data. The new Wi-Fi devices also use precoding and postcoding techniques like spatial beamforming, and the 802.11n standard adds frame aggregation to the MAC layer. These new techniques give Wi-Fi the range and bandwidth it needed to become a reliable option for M2M data communications and industrial networking. And, as is the case with a fiber optic link, a radio link creates a barrier that damaging electrical events cannot cross.

Solutions: Isolation
There will be many situations in which fiber optic cable and Wi-Fi connections will be impractical. But manufacturers have found numerous ways to interpose isolation in data communications streams. Isolation works by altering the signal on USB D- and D+
lines and transforming the 5 VDC power on the other pair. The isolator converts the data signal, either to pulses of light that work like a very short fiber optic connection, or to an electrical field. It then converts it back to an electrical signal again. Data can pass through, but the isolator stops power surges and ESDs at the isolation zone. The isolator controls surges and ESD on the power line by transforming the 5 VDC USB power to AC, then back to DC.

Isolation has a minor disadvantage. USB devices default to Full-Speed (12 Mbps) until they are able to negotiate a Hi-Speed (Up to 480 Mbps) connection rate with the USB hub. The USB device initiates the negotiation by driving 17.78mA into the D- data line for at least a millisecond. The connected hub responds by alternately injecting 17.78 mA into the D- and the D+ lines. If the USB device detects at least three of these “chirp pairs” it will decide that the hub is Hi-Speed capable, and it will establish a Hi-Speed connection. But isolators interfere with this negotiation when they convert the DC signal to AC at the isolation zone. That makes the negotiation fail, and the USB devices will default to Full Speed. That’s fast enough for most industrial applications, of course. And leaving your devices unprotected is unwise. But, until things go wrong, unprotected devices can establish some very fast connections.

You can add isolation to your network many different ways, and in many different places. You can use in line isolators that protect just a single piece of equipment. You can use isolated USB hubs that protect many devices at the same time. You can install isolated Ethernet servers, isolated repeaters, isolated expansion cards, and heavy duty isolators for DIN rail mounting. You can even get USB “key” isolators that you can tuck into your laptop bag.

**Solutions: Hi Retention USB Ports**

Manufacturers have strengthened USB’s physical connections by introducing high retention USB ports. High retention ports look much like the USB ports installed in office-grade equipment, and they’ll work with any USB cable. Connecting and disconnecting cables feels pretty much the same. But they grip cables much more firmly than a standard port. A typical high retention port can resist 3.4 lbs of force. You won’t dislodge the cable with vibration, or by brushing up against it.

Some of USB’s features may seem to be design flaws when USB is used in harsh environments. But they’re all easily addressed via conversion, isolation and the use of high retention USB ports. Just remember the laws of physics, think about electrical potentials and plan ahead. There’s no reason that your expensive equipment should ever have to share the costly, untimely and unnecessary fate of the Hindenburg.