Protecting mission critical electronics in the industrial environment

Today's engineers are designing more and more sophisticated control systems that bring higher productivity to meet ever increasing expectations of performance—all while keeping system costs under control. In order to achieve these results, they are employing more electronic equipment, much of it adopted from non-industrial applications, and almost all of it more sensitive to electrical disturbances than the equipment being replaced.

These new realities are then mixed with the inherently poor power environment of an industrial facility and aging power generation and distribution facilities—both inside and outside of the plant - to produce a wide variety of power and electrical noise problems.

Understanding these problems, along with some of their causes and solutions, can help ensure the design of mission critical electronic systems that are both reliable and cost-effective.

Introduction

Mission critical elements

The first task in protecting mission critical elements is to identify them. While each system is unique, the mission critical components are usually easily recognized. They include items that, if they fail, will cause customer displeasure, increased labor, or increased material cost.

Typically, programmable logic controllers (PLCs), industrial computers, and electronic motor speed controls serving in the control loop of a manufacturing process are the first components that are put on the "mission critical" list. But, this list is far from complete.

Sensors, data communication equipment, actuators, and even production planning systems must be included to achieve a high level of customer satisfaction and minimize costs due to downtime. As each component is evaluated for inclusion on the critical component list, remember it's "mission critical" if its downtime causes lost profits.

Levels of protection

Once the list of mission critical components and systems is identified, the next step is to determine the necessary level of protection. When making this decision, it is valuable to look at achieving three distinct levels of protection.

The first level of protection provides a defense against the instantaneous destruction of critical equipment. This is often the level of protection desired for a home computer or entertainment center—just enough protection to keep things from catastrophically failing.

The second level provides additional protection against long term degradation of equipment, a condition often seen in semiconductor devices.

The third, and most important level for most industrial systems, adds defense against disruption—those unexplained soft failures, system lock-ups and resets for which no specific cause can be identified.

As more devices containing volatile memory find their way onto the production floor, guarding against such disruptive events becomes even more critical to ensure that these costly interruptions do not occur.

Total Protection Solution

If satisfied customers and controlled costs are of primary importance, there is little question that systems must be protected to the third, and highest level. To accomplish this, it is critical to use a *Total Protection Solution* for your mission critical systems. This approach requires that each and every input and output line, whether power or data, be examined and appropriately protected against likely hazards. Achievement of this level of protection usually requires the use of industrial grade components, along with a combination of devices such as surge protectors, power conditioners, power conditioned uninterruptible power supplies (UPSs), as well as appropriate grounding techniques.

Power Line Issues

"Outside" events

Power line problems that can cause the destruction, degradation, or disruption of mission critical equipment can originate either "inside" or "outside" the industrial facility. Outside problems include inclement weather that produces lightning induced transients or power line outages due to high winds or ice. Power problems may also come from routine utility operations such as capacitor switching to effect power factor correction, or from the clearing of line faults.

"Inside" events

While "outside" events are the most obvious and spectacular, it is estimated that in industrial facilities, up to 80 percent of power related problems originate on the customer's side of the meter.

"Inside" problems are caused by a wide variety of factors including stopping and starting of motors, welding equipment, electronic motor speed controls, poor grounding, and some of the same problems facing the utility company—fault clearing, and capacitor switching. The result of these events show themselves in many ways including voltage interruptions, sags and the less obvious, but more disruptive voltage transients.

Power Interruption

Among the most noticeable power quality problems is a power interruption. While power interruptions are relatively infrequent in most locations, their effect can be dramatic and obvious, as everything grinds to a halt.

Solutions to combat power interruptions include alternate power feeds to the facility, local back up generating capability (diesel or gas powered generators) and the addition of UPSs on selected equipment. While alternate power feeds and local power generation may not be practical for every facility, the addition of UPSs, particularly to software controlled devices, is an important component in a total protection strategy.

When properly selected, the UPS will ensure that the attached devices are kept active during an outage. With proper communications interface software, these devices can also smoothly and automatically shut down all running software applications and the operating system, to ensure a clean restart of the process—a factor particularly important in batch processing applications.

Voltage sags

Voltage sags, and to a lesser extent voltage swells, are reported to be the most measured power line problem. A study of one site estimated that up to 62 voltage sags down to a limit of 80 percent of nominal voltage, and an additional 17 sags down to a limit of 50 percent of nominal voltage occurred yearly at that site. In another study of a large industrial facility, more than 500 sags of various levels were recorded at the input to key control equipment over a 3½ month period. In the same study, only about 100 such sags were recorded during that period on the input power line to the facility. Both of these studies also report that individual pieces of control equipment were effected quite differently by the recorded voltage sags.

Protecting against voltage sags

As with power interruption, solutions can be applied both locally and plant wide. Plant-wide solutions include layout of power distribution to minimize the number of sags induced on critical equipment from internal causes such as starting motors and fault clearing. Since studies show that up to 80 percent of sags are caused within the plant, such solutions, while expensive, can greatly aid in protecting critical control components from unwanted sags.

Typically, however, a more practical approach for protecting controllers is the application of a voltage control device in the power path supplying the control system. Because these local devices can compensate for sags generated both inside and outside of the facility, using them is usually more reliable and less expensive than attempting a plant-wide solution.

At least three basic types of devices that provide local sag protection are available. These include devices that store energy in a transformer (Constant Voltage Transformer), devices that use boost windings to raise voltages during sags (tap switching transformer), and devices that supply energy from batteries during sags (Uninterruptible Power Supplies). There are also devices that use some combination of these three technologies to combat sags.

While each of these solutions has its advantages and disadvantages, some are better suited than others to today's electronic control systems. In the past, the most common device applied to control sags was the Constant Voltage Transformer (CVT). This device, which also typically provided the step down voltage function, was an excellent choice when most control devices used linear power supplies, most sags were not too severe, the attached control system "crashed" well, and the CVT was presented with a relatively constant load.

A new environment

Today, however, control systems have changed. Loads are more typically Switch Mode Power Supplies (SMPS), and sags (particularly with deregulation) are likely to become more severe. In addition, control systems are often no longer based on proprietary software that "crashes" well, but on commercially available operating systems that need to be properly shut down in order to start up smoothly. Power system load requirements also change more often as control schemes are frequently updated with the latest technology in order to gain additional performance from existing tooling and equipment.

While changes have been made in many CVT's to adapt to this new technology, the best solution is one that was specifically designed to support SMPS and has more energy to ride through severe sags than a typical CVT. Such a device is a USP with integral isolation transformer that provides highly robust regulation, isolation, and backup. If an isolation transformer already exists in the power path near the load, a UPS with double conversion topology can also serve quite effectively.

Transients

By their very nature, transient voltages on power lines, below the level of those that cause massive destruction, are difficult to measure directly. Among the most difficult transients to measure are the high speed transients that are the most likely to cause disruption of electronic equipment. To further complicate the situation, transients often occur randomly; and special power quality monitoring equipment is usually required to capture the high speed impulse and oscillatory events that can cause sensitive electronic equipment to be disrupted. While often not discussed or considered, this "least measured" power quality event can be a major contributor to those random errors and "lock-ups" that occur in a control system.

As with many industrial power quality issues, most of the high speed transients that cause system disruptions are not supplied through the power utility, but are generated "inside", or within the facility. This conclusion can be reached not only by observation, but through examination of the typical transient's high frequency content and its interaction with the intrinsic impedance of power distribution lines. The one obvious exception is lightning, which is clearly a natural, and external or "outside" event. Typical "inside" causes of transient events include switching devices such as contactors, motor starters, compressors, variable speed drives, and the switching of capacitor banks for power factor correction.

Reducing or eliminating transients

Before progressing, it is important to note that while these transients are clearly a threat to a mission critical system's overall reliability, not every transient will cause a system disruption. The transient's, frequency, edge speed, the mode in which it appears to the equipment, and where it occurs in the effected equipments' clock or processing cycle will all determine its immediate effect.

Clearly, almost all transient events are ignored by electronic equipment. If they were not, it would be almost impossible to keep a computer running. However, in mission critical applications the goal is to push disruptions as close to zero as is possible, and the reduction or elimination of these transients is critical in achieving this result. Thus, in mission critical applications, reducing the amplitude and edge speed of all transients becomes paramount in achieving the desired system reliability.

In order to better understand the specific methods that may be used to control the amplitude and edge speed of transient voltages, it is useful to review how transient noise appears to electronic equipment.

Normal mode noise

Transients are said to be Normal Mode (NM) noise when they appear between the Line (hot or phase) and Neutral conductors supplying the equipment. While somewhat troublesome, noise appearing in this mode can often be controlled by a combination of Transient Voltage Surge Suppressor (TVSS) devices and filters. Typically, individual pieces of equipment often make some provision for controlling this noise mode within the control equipment itself.

Common mode noise

The far more difficult noise mode to control is Common Mode (CM). In this situation, there is noise between the neutral line and the ground line connected to the equipment. While the neutral and common are bonded either at the service entrance or at an intermediate transformer, noise in this mode is quite common, and very disruptive. Common mode noise typically occurs when current is "dumped" into the ground lead by other equipment—input and output filters to suppress high frequency line noise are a typical cause, as are protective devices such as TVSSs.

Power conditioning

Control of common mode noise usually requires a transformer based power conditioning device that provides a "separately derived" source of power in which the neutral and ground wire are locally rebonded.

Almost all such commercial power conditioning devices also include appropriate components to control any normal mode noise that is present. These devices, which are typically available as traditional power conditioners or as power conditioners with battery backup, accomplish the necessary reduction in amplitude and edge speed of transient noise sources to help ensure that equipment in mission critical systems is not unnecessarily effected by transient events.

Additional considerations

In addition to installing an appropriate power conditioning device, proper care must be taken in system layout and wiring. In particular, it is critical that the wiring to the power conditioner not be run with the power from the output of the power conditioner. Running these wires in the same conduit or wiring tray will significantly reduce the benefits provided by installing the power conditioner.

It is also important that, whenever possible, all critical devices, including sensors, be powered from the same power conditioner as the controller and that sensor and peripheral equipment grounds be connected at a common point. Finally, data communication cables should be run in conduit or wiring trays that do not contain power, or at a minimum, do not contain unconditioned power.

Communication line issues

Today's typical control system uses communication lines for several purposes. Control busses such as DeviceNet, or Profibus; data lines to peripheral devices such as Human Machine Interfaces (HMIs) and connections to plant-wide production information systems are typical. While not subject to all of the problems of power lines, communication lines are often more likely to cause system disruption due to transients. In addition, grounded (non-isolated) communication schemes such as RS232 and RS485, provide an opportunity for an additional path of disruption known as ground skew.

Communication line protectors

As in power lines, a user must be concerned about destruction, degradation, and disruption when addressing communication line protection. In communication lines, minimizing the chance of destruction or degradation is best addressed by the use of a Communication Line Protector (CLP).

Typically, the semiconductor devices associated with communication lines are not designed to withstand the high voltages or currents that can be induced from power lines or other noise sources, and thus need to be protected with a CLP.

System considerations

Selection of CLPs should be done with care to ensure that the clamping voltage is lower than the point at which damage will occur, but higher than the maximum voltage that can be applied to the line for normal communication. In addition, when using systems with the higher transmission speeds now available, care must be taken to ensure that the insertion loss due to the added capacitance and inductance of the CLP will not cause unacceptable signal level reductions.

Use of external CLPs is often suggested to improve system reliability, even if a communication port is internally protected by a TVSS against over voltage. This approach can lead to improved reliability since a typical CLP will have a grounding lead which can be wired to direct transient noise away from the chassis ground of the control device. Redirecting this transient noise current will avoid introducing potentially disruptive common mode noise into the equipment, a situation that can occur if the internal TVSS is triggered.

For this scheme to have value, however, the external CLP will be required to activate at a lower voltage level than the internal protective devices. While proper selection of an external CLP will provide this result, the selection requires investigation into the internal protection levels for each piece of equipment in order to ensure proper coordination.

Grounding

While CLPs can provide protection against system destruction and degradation, they do little to assist in reducing disruptions from transient voltages that are below the level of component destruction, but above the disruptive level that interferes with routine communication. Protection against such disruption can be addressed in several ways.

First, it is critical that system grounding follows good practice, and meets the equipment manufacturers' guidelines. With grounded communication schemes in particular, a small grounding problem can lead to very inconsistent communication.

A second key factor is cable routing, which should be done in a manner to avoid inducing any noise into communication cables from other sources. In particular, to maximize system reliability, do not run communication cables with power cables, and when crossing power cables, if at all possible, do so at right angles.

Ground skew issues

Addressing ground skew is the next step in improving communication reliability. Ground skew problems occur when noise currents flow in a ground path between two pieces of equipment connected by more than one ground lead.

In grounded communication systems, the primary connection is the power ground, while the second ground lead is the shield and or common lead in the communication cable. When ground currents flow in the power ground, they cause a voltage difference (ground voltage skew) between the two locations, thus causing a voltage differential to be reflected in the communication cable. This voltage differential, and the resultant current flow in the communication cable can cause serious disruption of the communication path, and can even destroy devices not protected by a CLP.

Solutions to the ground skew problem

There are two solutions to eliminate or reduce ground skew related problems. The first, most expensive, and often most difficult to implement is full isolation on the communication port. Such isolation typically requires separate power supplies be added at each end of the line, in addition to adding the appropriate isolation device. While commercially available, such devices are relatively expensive and take time to install. To avoid such costs, an alternative solution is desirable.

One alternative solution to ground skew induced problems is a ground skew protective device in the power path. Such a device is available from multiple sources; each with slightly different, and patented, implementations. The device works on the principle of creating a high impedance in the ground path at high frequencies while maintaining a "zero" (Chloride implementation) or low (other implementations) impedance at power line frequencies.

By increasing the high frequency impedance in the ground line, the resultant voltage produced by high frequency ground currents is substantially reduced, thereby reducing the opportunity for disruption or destruction of the communication line. In order to ensure proper protection, one ground skew device should be placed in the power path of each device containing a grounded communication port. Commercially, ground skew devices are typically sold as an internal option to power conditioners and power conditioned UPSs.

Conclusion

In order to provide the highest level of confidence in the reliability of a mission critical industrial system two steps are required. First, robust equipment designed to be used in an industrial environment must be selected. While this paper discusses techniques to minimize the effect of electrical anomalies on the system, items such as working temperature range, and mechanical ruggedness are also important to ensure long term system reliability. Once the proper equipment is selected, installing it with the proper "Total Protection Solution" on power and communication ports becomes of paramount importance to provide a system that is as failure free as possible.

When installing equipment with the goal of achieving a "Total Protection" it is important to protect each and every power and communication port into the system and provide a grounding scheme that is in accordance with the NEC and the manufacturers' guidelines. In a well protected system, each power port should be protected with a low impedance transformer based power conditioner to control both common and normal mode noise. On some power ports a low impedance transformer based power conditioner with batteries (UPS) may be the proper choice to provide protection against extended sags and outages when sensitive controllers need to be shut down in an orderly fashion.

In addition, each communication line should have a CLP installed that has the appropriate voltage breakdown level and controlled insertion loss for the type of communication port being protected.

When grounded communication lines are involved, either ground skew protection devices, or full isolation of the ports should be considered.

Finally, remember that once a system is properly installed and protected, vigilance is required to maintain the level of integrity that was originally designed in. One single "on the fly" addition or change can leave a system with an unprotected path, and subject to the disruptive effects of power and communication line anomalies.

Bibliography

(1) *Power Quality and Factory Automation* IEEE Transactions on Industry Application, Vol. 26 No. 4, Wagner, Anreshak, & Staniak, July/August 1990.

(2) *Volage Sag Analysis Case Studies,* IEEE Transactions on Industry Application, Vol. 30 No. 4, Lamoree, Mueller, Vinett & Jones, July/August 1994.

(3) *EPRI Journal,* JohnDouglas, May/June 1996.

(4) *Instrumentation, measurement Techniques, and Analytical Tools in Power Quality Studies*, IEEE Transactions on Industry Applications, Vol. 34, Ronald Simpson, May/Jun 1998.

(5) *A Study of Common Mode Sensitivity of Electronic Equipment*, PowerCET Corporation, Tom Shaughnessy, 1992.

About the author

Paul Haake

Paul Haake is Vice President of Engineering for Chloride North America with responsibilities for all aspects of design and engineering of UPSs, power conditioning and communication line protection devices. He has over twenty-five years experience in design and design management for power conditioning products, and equipment and instrumentation used in the process, utility, nuclear, HVAC, safety and assembly industries. Mr. Haake holds a BSEE degree from Purdue University and an MBA from the University of Chicago.

Paul Haake
Chloride Engineering
paul.haake@chloridepower.com