Preventing Electrical Interference Problems in Industrial Barcode Data Collection and Printing Systems

Dr. Peter Green

Introduction

Industrial barcode data collection systems typically have some or all of the components shown above for a BellHawk data collection system. Systems such as this will work properly when being tested in an office environment but then can display what appear to be bizarre behaviors when installed in factories, warehouses or other industrial environments.

Often users blame the software or the equipment as being intermittently defective when, in fact, the real cause is often electrical interference.

In this paper, we identify possible causes of interference, their symptoms, and remedies to prevent the problems.

Ground Loops

In most industrial environments, equipment is grounded so that if there is a short or other malfunction, users are protected from electrical shock. In an ideal world, electrical power flows into the three phases of the electrical supply and returns through the neutral wire to the utility. But imbalances between the current drawn by the equipment on the different phases, especially
when electric motors start up, can result in significant current flowing through the ground wire, with the result that there can be a significant voltage spikes appearing across the ground wire.

In an ideal building layout all the ground wires from all the pieces of equipment are connected to a single ground point. This is so that current flowing in one grounding wire does not result in a voltage being fed back to other equipment grounded through a common grounding wire. Unfortunately this does not happen in practice in many industrial buildings, especially older ones that have had their electrical systems expanded and modified over the years.

Equipment can be inadvertently connected to ground through multiple paths that have significant voltage spikes across their grounding cables. This can happen when a PC is plugged into one power socket and a peripheral, such as a printer, is plugged into another power socket, with a different ground path. Then their grounds also become connected through any data cable that connects them, such as USB, RS232, or Ethernet LAN cables. These multiple grounding paths results in what we call a ground loop, which can result in data transfer problems or worse.

If a PC is plugged into an electrical socket that shares a common ground with some piece of equipment which has an electrical motor, the PC may well experience spikes of several volts on its ground wire whenever the motor is started up. If a peripheral device is plugged into a power circuit with a different ground, the data cable between them may experience these voltage spikes.

This can cause the PC or its peripheral devices to behave strangely whenever the motor, which may be located in another room, is started up. It can even damage the PC or its peripherals. In one case recently we had a barcode scanner plugged into the USB port of a PC generating random output because the weighing scale interface was grounded to a different electrical circuit.

The cure for this problem is to use a small uninterruptable power supply (UPS) for each PC. Then plug the PC and all the peripherals (including devices such as weighing scale controllers) into this same UPS. This will provide a common ground point for all peripherals attached to the PC. This will eliminate ground loops between the PC and its peripherals and also ensure isolation from ground loop spikes on the common incoming power cable to the UPS.

**Unshielded Ethernet Cables**

In an industrial plant there are many sources of electrical splash noise that can interfere with barcode data collection equipment. These include:

1. Big electric motors when starting and stopping
2. Electrical arc welding
3. Industrial heating units
4. Battery chargers for electrical fork-lift trucks
5. Electric cranes and hoists

This radiated energy can easily be picked up by unshielded Ethernet cables running in the vicinity of these sources of interference. Long cables act as very effective antennas and so can pick up a high level of interference. While the use of twisted pair cables and balanced feeds can
help mitigate this issue, the signal voltages on the Ethernet cables are relatively low. As a result, it is easy for a data packet from a PC to the server to be corrupted.

The transport layer in the Ethernet protocol stack can detect damaged packets and perform retries. But, if the interference is too bad, the data will not get through and communications between the PC and the server can be severely impacted.

The cure for this is to use shielded cable with the outer shield grounded. This will stop the electrical interference from reaching the signal wire inside the cable.

But this also brings with it the issue of ground loops. If you take a standard shielded Ethernet cable and plug it between a PC on one electrical circuit and a server on another, you have immediately created a ground loop that can inject ground power spikes into the PC or the server.

The answer to this is to only ground the cable at the server end and then to use an optical data-isolator between the Ethernet cable and the PC. This device has two RJ45 ports that are connected by a short length of fiber optic cable. One port is plugged into the CAT5 cable that goes to the server and the other is plugged into the PC through a short network patch-panel cable. In this way the Ethernet signals can get through but the ground for the PC (through its UPS) is isolated from the ground for the server, thus avoiding ground-loop signal injection problems.

**Wireless Communications**

This same radiated energy that is picked up by cables may also cause electrical interference with wireless communications between a mobile computer and its wireless access point. There are also other sources of possible interference. These include:

1. Microwave ovens and similar heating equipment
2. Handheld radios used for communications between plant personnel
3. Remote controls for equipment

These, and similar devices, are all licensed to use the same frequency bands as the wireless mobile computers used for barcode data collection.

These mobile computers also use very high frequencies for their wireless communications. At these frequencies radio waves are blocked, deflected and absorbed by any conducting materials. This can result in blind-spots where you have no wireless local area network (LAN) communications. Examples of things that can block communications are:

1. Warehouse racks
2. Metal partitions or concrete walls with rebar
3. Metal machinery and equipment
4. Containers of liquid
5. Metal or carbon filled materials

Also the human body is an excellent conductor of electricity. As a result, wireless LAN communications can be blocked when the user gets his body between the mobile computer and the wireless access point.

Fortunately, these days, wireless access points are relatively inexpensive so that, in many cases, good wireless LAN coverage can be achieved by simply using enough wireless LAN access points. But this cannot overcome the problems of electrical interference.

Many older mobile barcode data collection systems use a program inside the mobile computer that acts as a direct terminal interface to a computer program running on the server computer. More modern systems use web-browser interfaces, with a web-browser running on the mobile computer communicating with a website running on the server computer.

If communications are blocked, then data communications from the mobile computer to the server computer cannot get through. If there are bursts of electrical interference then data transfers can be garbled and rejected. As a result the terminal interface or web-browser on the mobile computer stops responding because data cannot get through to the server computer. This problem can prevent the collection of barcode data in certain locations or, if intermittent, can severely impact the productivity of users.

The solution to this problem is to use store and forward communications from the mobile computer to the server computer, as shown below for BSAF (pronounced be-safe), which is the BellHawk Store and Forward technology.

In this technology, each mobile computer has a local database, which is kept in non-volatile memory. All data collection is performed through a user interface, which interacts with this database. Data captured by barcode scanning is recorded in this database. Also data captured is compared locally with the contents of this database to generate point-of-action warnings before and not after mistakes are made.

All this takes place whether the mobile computer can communicate with the server or not. When the mobile computer comes within reliable communications range of a wireless access point data is exchanged with the server computer. As a result of this, data collected by the mobile computer
is stored in the main tracking database and other information, needed for point-of-action warnings, are relayed from the server to the local database.

Data captured by the mobile computer, such as receiving or moving containers of material, is then relayed to other mobile computers when they come within reliable communications range.

The BSAF software works automatically and detects when it is within communications range or not and automatically initiates the data transfers. In this way users do not have to do anything except use the device for data capture. They do, however, have to remember to come within range of a wireless access point in order to synchronize data with the server computer.

The BSAF communications software has extensive error detection capabilities and is able to quickly detect when a data transfer packet has been damaged by electrical interference. The communications protocol then automatically retries sending the data packets until it can successfully transfer the data.

Conclusions

When installing industrial barcode data collection systems it is very important to take account of sources of electrical interference if the system is to operate reliably. It most cases it is not possible to eliminate those sources of interference as they are inherent to the industrial processes being used. But, as we have shown, it is possible to mitigate the effects of this interference through use of the correct technology.

Author

Dr. Peter Green is the President and Chief Technology Officer of BellHawk Systems Corporation. BellHawk Systems is a technology plus professional services organization that provides affordable technology solutions to operational problems for mid-size manufacturers, food processors, distributors, laboratories, engineering and other industrial organizations, primarily in the North Eastern USA.

Dr. Green received his BSEE and Ph.D. in Electronics and Computer Science from Leeds University in England. He was a member of the technical research staff at MIT and was a Professor at WPI. Dr. Green is a member of APICS (American Production and Inventory Control Society) and is a speaker at their professional development meetings. Over the past two decades Dr. Green and his team have implemented over 100 systems that provide technology solutions to operational problems for clients ranging from small manufacturing companies to the US Air Force and Navy.

If you have comments or suggestions, or would like to discuss a specific problem you are trying to solve, please contact Dr. Peter Green by Email at Peter.Green@BellHawk.com. Also please see www.BellHawk.com for details of our BellHawk® and Bell-Connector™ technologies that we use to solve issues such as those discussed in this paper.

Publication Rights

This document may not be republished without permission from the Author.