

THE TEN COMMANDMENTS OF INDUSTRIAL ETHERNET

10 RULES OF SMART NETWORKING
PRACTICE, THAT IT MAY BE WELL
WITH YOU AND THAT YOUR YEARS
OF HAPPY EMPLOYMENT AND
PROSPERITY MAY BE PROLONGED

BY
B&B ELECTRONICS,
OTTAWA IL



B&B electronics
MANUFACTURING COMPANY

The Ten Commandments of Industrial Ethernet

1 Thou shalt place high priority on security, knowing that the hacker constantly lurketh and thieves break in and steal.

The first thing to remember is this: The most probable cause of problems is not the environmental extremist who sees your smokestack on his way to work and decides to launch a virtual terrorist attack on your factory.

It's more likely to be related to the ubiquity of PCs with Ethernet cards, the ease with which your own employees can "hang stuff on the network," and careless or nonexistent internal security measures. Accidental problems are more common than deliberate ones.

But you should be prepared for both, because nothing would give a hacker more pleasure than a giant plume of smoke where your factory used to be.

The following guidelines will help you guard against the most common problems:

- At the control level, prioritization and security can be easily overlooked. The most common instances of industrial sites being "hacked" are the result of well-intentioned employees, not outsiders.

- Another hazard is connecting consumer "plug and play" devices to your factory LAN. A printer, for example, might flood the network with traffic with a "broadcast storm" as it tries to self-configure or advertise its presence to all nodes on the network.
- Faulty devices, for example defective NIC cards, can vomit zillions of bad packets (i.e., runts, which are abnormally short Ethernet frames) into your network. Using switches instead of hubs limits the effect of such problems. Diagnostic tools can locate the source of bad traffic.
- Duplicate IP addresses can deactivate devices that otherwise appear to be perfectly functional. This is especially common when replacing devices, and is a very perplexing problem to trace.
- Passwords often stay the same for years, and are often easy to guess.
- It's unwise to assume that your industrial Ethernet products themselves have any security features at all. You should minimally use inspection-type firewalls (such as packet filters) to control access that is based on a combination of IP source address, destination address, and port number. This is by no means completely hacker-proof, but it should keep the well-meaning employees out.

2 Thou shalt document thine installation, so that even Homer Simpson mayest discern the system whither thou goest; for to write the IP address on your hand or your forehead shall not be deemed sufficient.

Perhaps this point doesn't need lengthy treatment, but it's always worth repeating. Industrial installations require good documentation in particular, because when devices need to be replaced, it needs to happen fast. Things you need to know and document for every device:

- Replacement part numbers
- IP addresses
- Subnet masks
- Gateway addresses
- Menu settings of devices like Serial Servers, data collectors, and also routers and configurable switches
- Functions like DHCP enabled/disabled; static vs. dynamic IP addresses

Be sure that if a device fails and needs replacement, that all of this documentation can be quickly and easily located by a panicked, uneducated Homer Simpson who's counting the seconds as they tick by!

3 Thou shalt execute a definite plan for assigning and re-assigning IP addresses, from the very opening of the box to the inheritance of future generations.

There is no standardized way to set IP addresses in automation. Users must have a plan in place. It's dangerous to just "wing it" when putting a system together. The following recommendations apply to Industrial Ethernet systems today:

- Whether you have a specific plan for setting IP addresses manually or if you intend to use DHCP, your IP address assignments should be semi-permanent.
- Understand the Client software IP address requirements as they relate to the hardware devices in a Client/Server application. Note that in a PLC-style control system, the PLC is a client and all of the I/O devices are servers, which is the exact opposite of the arrangement in an office LAN.
- Devices in offices are usually designated by name, but industrial devices are normally just assigned IP addresses.
- The IP Address of each device must be documented and quickly available.
- Documentation should clearly indicate the mechanism by which the IP address of a replacement device should be set.
- You should cooperate with your IT department in choosing IP addresses so that conflicts do not arise in the future.

- Great care should be taken to not have duplicate IP addresses, because Ethernet doesn't provide a common standard for duplicate IP address detection or defense.

Don't "wing it" – have a plan for assigning IP addresses and replacing failed devices. As standards and product availabilities mature, it is hoped that IP address assignment will cease to be an obstacle for designers and maintenance professionals.

(From Bennet Levine, *IP Addresses in Automation*, from The Industrial Ethernet Book, One/2004)

4 Thou shalt employ hardware which endureth the cold of winter, yea, and the withering heat of the broken air conditioner in July.

It's tempting to run down to Office Max and buy a \$29 Ethernet hub, plug the DC adapter into an outlet strip, and Velcro it into your panel.

But of course you get what you pay for. And considering that your Ethernet components are the nerve center of your communication center, the downside risk is much bigger than the upside of a good deal on equipment.

Considerations for industrial equipment – and features of good industrial grade hardware:

- DIN Rail solid mounting to panels, instead of Velcro
- Low voltage AC/DC connections instead of AC adapters

- Below-zero to 70 or 85 degrees C, instead of 40 degrees C
- Fault interrupt relays
- Sturdier physical construction
- Advanced functions like port management; features that facilitate trouble-shooting, like Port Mirroring
- Provisions which guard against broadcast storms and "runt" packets
- Live technical support and advice from real people

5 Thou shalt maintain a healthy separation between office and factory, with routers, bridges and firewalls.

- Never mix your office LAN with your industrial-control LAN. They should be separated by a firewall, or at minimum, a bridge or router. That firewall also serves as a convenient boundary between the loyal, dedicated, competent automation engineer, and the egotistical control freak from the IT department whose mission in life is to discredit the engineering department and take over the planet. A control network and a business LAN have two entirely different purposes and their interaction should be closely controlled.
- Industrial Ethernet needs to be viewed in at least two categories: a control-level industrial Ethernet and an I/O-level industrial Ethernet. This means each manufacturing cell will have its own Ethernet network, possibly more than one. Ideally those networks will be isolated as well.

6 Thou shalt empower legacy equipment by extension of its lowly serial port; thou shalt not abandon it to destruction.

Most older control devices have serial ports, and still much of today's high-tech equipment ships with a serial port for programming, monitoring or diagnostics.

But these ports are rarely used for their intended purposes. You can put those ports to work, saving you time and trips to the factory floor.

- Communicate with every piece of equipment from any networked PC
- Reduce service calls
- Increase productivity by knowing what your equipment is doing before you get a trouble report
- Spend more time doing your work, not chasing down problems at remotely located equipment

Serial Servers solve this problem with Virtual COM drivers, which make the PC software think it is talking to a serial device connected to a COM port on the PC when in reality the device is on the LAN or WAN.

B&B offers a more detailed application guide for this subject. You can get it free at www.bb-elec.com/serialserver

7 Thou shalt observe lawful wiring practices and exercise sound judgment in the laying down of cable.

When You Install Cable

- If you are unable to plan the exact cable locations, add a measure of protection with armored shield or conduit.
- If physical protection or local codes necessitate using conduit, use STP wire.
- Isolate the STP shield from the conduit, since high voltages may be present on the conduit.
- Attach the STP shield to ground at only one end of the cable. Connecting at both ends creates ground loops with substantial current flow and induces noise.
- If for some reason you are required to terminate the shield at both ends, wire a Metal Oxide Varistor (MOV) shunt in parallel with a 1-Mohm resistor and 0.01- to 0.1-mF capacitor. This severely limits ground current except when extreme voltages are present.
- Check cables with a cable tester, not just with an ohmmeter. A tester quickly identifies continuity problems such as shorts, open wires, reversed pairs, crossed pairs, shield integrity, and miswiring of cables.
- If your cable trays are metal, they should be conductive from end to end.
- Avoid proximity to power lines and sources of electrical transients. High-voltage lines should intersect the cable at a 90° angle.

- Maintain at least a 10-cm distance from 120 VAC, 15 cm from 220 VAC, and 20 cm from 440 VAC if you use conduit. If you don't use conduit, double those distances.
- Educate unsupervised electricians about the practices described here: Purchase a copy of this book for each of them.

8 Thou shalt use connectors which moth and rust do not destroy, and water and oil do not corrode.

You don't have to spend much time investigating industrial Ethernet to discover that RJ-45 "telephone connectors" aren't viewed with a great deal of respect. Nor should they. The design lacks even the most minimal environmental protection and can be easily damaged with a good yank on the cable. The surface area of the contacts is quite small and if the thin layer of gold over nickel is worn away by vibration, it becomes susceptible to corrosion and oxidation. Not a great choice for your robotic welder, especially if downtime costs \$15,000 per minute.

Fortunately there are alternatives, three in particular from the industrial world. They have been designed to keep out liquids (e.g., IP65 or IP67), maximize contact surface area, and improve the sturdiness of the design. All of them facilitate feeding Ethernet cables through panels, simply by choosing appropriate receptacles.

Thou shalt take advantage of such connectors whenever appropriate, as the cost of these items is small in relation to the weeping and gnashing of teeth you can experience if you neglect them.

9 Thou shalt recognize industrial automation protocols and compatibility concerns before thou issueth purchase orders.

There are several different open standards for representing industrial data on Ethernet—Modbus/TCP, EtherNet/IP, Foundation Fieldbus and PROFINet. There are also other proprietary standards used by some vendors. Here are some things to keep in mind:

- These protocols are not interoperable, though it is possible to define structures that make them interoperate.
- All of these protocols can theoretically exist on the same network, even though they don't interoperate.
- Yes, this is another version of the fieldbus wars, though not nearly as competitive as the last round was.
- Even within a single protocol, there are variations in the features supported.
- You should do your homework on all industrial Ethernet products you purchase, especially in terms of these protocols.

10 Of the mixing of wires and wireless there is no end; but thou shalt deploy wireless with care, knowing that the mixing of Wi-Fi, Hi-Fi and Process Control openeth a can of worms.

PC's weren't designed for the factory floor. Neither was Windows. Neither was Ethernet. Nor Wireless.

But they're all going to show up there anyway, at least fairly often. So given that this is to some degree inevitable, let's talk about the precautions you must take.

Wi-Fi Antennas figure strongly into the equation: they have everything to do with who is, and who is not, able to access your network.

The first priority is making sure that those who need to access the network can. If you're going to use wireless, you need to make sure that there's enough signal strength margin to cover all of the space, not some of it. That means walking through the space with a signal meter and making sure that the signal is strong everywhere.

Second priority is restricting transmission to desired areas. The problem with wireless is that it's hard to restrict the transmission to only areas under your control.

But there's no rule that says Wi-Fi transmissions have to be omnidirectional. You can use directional antennas to restrict radiation in undesirable directions. It's a crude but nevertheless sensible first line of defense for security.

Data collection vs. Control: It's one thing to do data acquisition with a wireless, but quite another to run I/O from your PLC. These days it IS actually possible to do the latter, but we don't recommend it. Keep the control stuff on physical cables if at all possible. Do the less 'mission critical' tasks with wireless.

Wi-Fi Security: This is a big, big topic. We can't cover it exhaustively here, but here are some tips:

- It's very easy to tap into most wireless networks, literally just by sitting in a car outside on the street. Two thirds of all wireless networks don't have any encryption whatsoever. This is very, very bad. You need to make sure that this is not possible in your facility, especially near your manufacturing equipment.
- Just because an ordinary antenna can't pick up the signal doesn't mean a high-gain directional antenna can't. Check this out too.
- If your notebook computer has a wireless connection built in, you may be unaware that this makes it possible for you to be on multiple networks simultaneously, without you knowing it. You're on a wired or wireless network but you also share a link with a hacker, who then shares your access to sensitive data. Note that other users can facilitate this problem, not just you.
- Most wireless systems employ industry-standard WEP ("Wired Equivalent Privacy") protocol which is infinitely better than unsecured connections, but can still be hacked within a few hours. There are other forms of protection, like Extensible Authentication Protocol and Tunneled Extensible Authentication Protocol, which you should investigate. These protocols are much more difficult to crack than WEP.
- You can have all kinds of security policies, but people must understand the need for them or they won't comply.

Consult the B&B website for more information and tools for wireless systems.

**B&B Electronics invites you to call and discuss your wireless application.
What makes sense for you? Bluetooth? A wireless RS-232 serial link?
Wireless Ethernet? Ember's new Zigbee mesh technology?
It's an exciting time to be going wireless, and we're here to help.
Email support@bb-elec.com or call (815) 433-5100.
And check out all our Industrial Ethernet and
Wireless products at www.bb-elec.com.**



Data Communication Tools

U.S. Headquarters:
707 Dayton Road • P.O. Box 1040
Ottawa, IL 61350
Phone: 815-433-5100 • Fax: 815-433-5109
info@bb-elec.com

European Headquarters:
Westlink Commercial Park,
Oranmore, County Galway, Ireland
Phone: +353 91 792444 • Fax: +353 91 792445
info@bb-europe.com