The Ten Commandments of Industrial Ethernet

I. Thou shalt place high priority on security, for hackers lurketh, thieves stealeth and employees bungleth
A Wi-Fi-enabled computer can connect to multiple networks at the same time. Your employees can give a hacker a pathway into your internal network simply by powering up a laptop. Imagine the mess an eco-terrorist could make if he didn't like the look of your smokestack.

Even your well-intentioned employees can bring a network down, simply by blundering around in areas they shouldn't. Don't take chances with network security.

Most wireless systems employ industry-standard WEP (Wired Equivalent Privacy). A hacker can get around it within a few hours. Look into more powerful standards like Extensible Authentication Protocol and Tunneled Extensible Authentication Protocol.

Never assume that your industrial Ethernet products have built-in security features. At the very least, you should use inspection-type firewalls (such as packet filters) to control any access that is based on IP source address, destination address, and port number.

Don't just talk about changing your passwords a regular basis. Do it. And don't make them easy to guess.

Consumer plug and play devices can flood your network with traffic in a "broadcast storm" as they try to self-configure or advertise their presence to every other node on the network. Faulty devices can vomit zillions of "runts", or abnormally short Ethernet frames. Using switches instead of hubs will take care of those problems.

Duplicate IP addresses can deactivate devices that otherwise appear to be perfectly functional.

II. 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
Document your installation. When devices need to be replaced it needs to happen quickly. 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, routers and configurable switches.
- Functions like DHCP enabled/disabled, static vs. dynamic IP addresses.

III. 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, but don't just wing it. Have a plan in place.
- Whether you use DHCP or set IP addresses manually, IP 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.
- 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.

IV. Thou shalt not be the little piggy who buildeth his house with straw
You get what you pay for in this world. If you've duct-taped a $20 office store Ethernet hub into your panel and plugged the DC adapter into an outlet strip you're going to pay for it when your network goes down. Ruggedize your communications with industrial-grade hardware and let the doom-beasties go eat somebody else.
- Use DIN Rail mounting, not duct-tape.
- Use low-voltage AC/DC connections instead of AC.
- Look for industrial-grade temperature specs and industrial grade physical construction.
- Deploy fault interrupt relays.

- Look for advanced functions like port management and features that facilitate trouble-shooting, like port mirroring.
- Back yourself up with live technical support and sound advice from real people.

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

A business LAN and a control network have very different roles, and so it only makes sense to increase your system-wide level of security by limiting their interaction. Separate them with a firewall or, at minimum, a bridge or router. Additionally, your industrial Ethernet can be looked at as two separate entities: a control-level industrial Ethernet and an I/O-level industrial Ethernet. These can be protected with additional security boundaries. Ideally, each manufacturing cell would be isolated and protected.

VI. Thou shalt empower legacy equipment by extension of the lowly serial port

It is far too soon to consider abandoning your legacy serial equipment. In fact, the serial communications protocol remains so useful that the number of deployed serial devices is expected to keep growing. Connect your legacy serial devices to Ethernet with serial servers and let them keep doing their jobs.

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

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

Install shielded twisted pair (STP) wire anywhere physical protection or local codes require the use of conduit. Attach the STP shield to ground at only one end of the cable. (Connecting at both ends creates ground loops.) If you are required to terminate the shield at both ends, wire a metal oxide varistor (MOV) shunt in parallel with a one megohm resistor and 0.01- to 0.1-mF capacitor. 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 and shield integrity. Metal cable trays 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 90º angle. Your conduit should maintain at least a 10 cm distance from 120 VAC, 15 cm from 220 VAC, and 20 cm from 440 VAC. If you don't use conduit, double those distances.

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

RJ-45 "telephone connectors" don't stand up to industrial applications. Their contacts have a small surface area and vibration can wear away the thin layer of gold that covers the underlying nickel, making the connection susceptible to corrosion and oxidation. A simple yank on the cable can also damage a connection. They're not a great choice for your robotic welder when downtime costs $15,000 per minute.

Fortunately there are alternatives. IP65 or IP67 cables keep out liquids, maximize contact surface area, and improve the sturdiness of the design. All of them facilitate feeding Ethernet cables through panels.

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

There are numerous open standards for representing industrial data on Ethernet, like Modbus/TCP, Ethernet/IP, Foundation Fieldbus and PROFINet. And some vendors use proprietary standards. The fieldbus wars are not over yet. But it's possible to define structures that make them interoperable. Don't commit to anything until you've done your homework.

X. Thou shalt deploy wireless with care, knowing that the mixing of Wi-Fi, Hi-Fi and Process Control openeth a can of worms

Position your Wi-Fi antennas so that they cover all of the required space. Walk around with a signal meter and make sure that they do. At the same time, do your best to restrict transmission to desired areas only. You can use directional antennas to restrict radiation in undesirable directions.

It's one thing to do data acquisition with wireless, but quite another to run I/O from your PLC. Keep the control stuff on physical cables wherever possible.