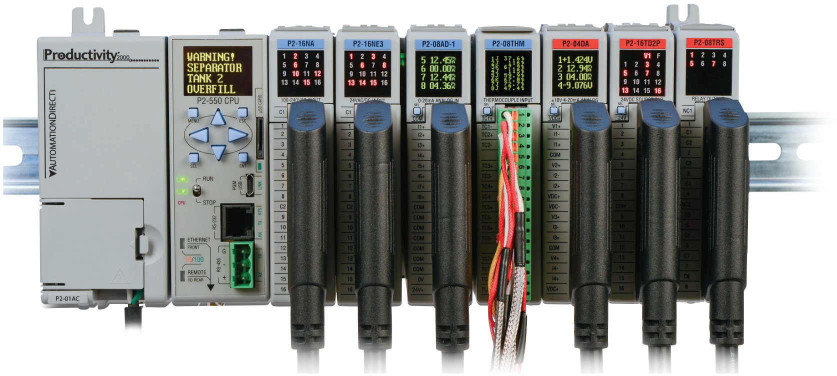
JEFF KERNS | Technology Editor
jeff.kerns@penton.com

Starting Small in the Growing IoT

A network is only as strong as its foundation, and industry experts give their take on the basic—and essential—building blocks.

When starting up a company, one basic tenet is crucial: Build a solid foundation. This is especially true when diving into the Industrial Internet of Things (IIoT) to create a connected network. Otherwise, expect to see a litany of problems arise down the road.

To build a strong foundation with a connected network, basic engineering practices are necessary: define the problem, protect your investment, and design with the future in mind. Even though these may not sound like first steps, they're necessary when planning your network's foundation.



To start out small with future IoT expansion in mind, the specified control system must have the required protocol support and communication capabilities, along with built-in data logging and web-server functionality. For example, this Productivity 2000 controller offers "controls and required IoT-related network connection and data capabilities for future expansion," said Jeff Payne, automation controls group product manager at AutomationDirect.

DEFINE THE PROBLEM

An analysis needs to document the root cause of the problem. Understanding how this affects the rest of the process is important, as it may show that connecting a device up or downstream may solve multiple problems in one location with a less complex system. After that, the key step involves finding the minimum information necessary in order to detect the problem.

"You have to find the pain point and what is needed to alleviate it. If there is no problem, there may be no reason to invest money into what could end up being bells and whistles," said Joel Young, CTO of Digi International.

"There must be a need; whether it's for safety, cost reduction, or to improve efficiency, a need is the first step," said April Ankrum, senior product manager at TURCK.

For example, if there's a problem with shutdowns due to emergency stops, maintenance, or line changes, connected devices can offer solutions. Find the information that will allow the user to correct problems, or make changes before the occurrence of a shutdown or full stop.

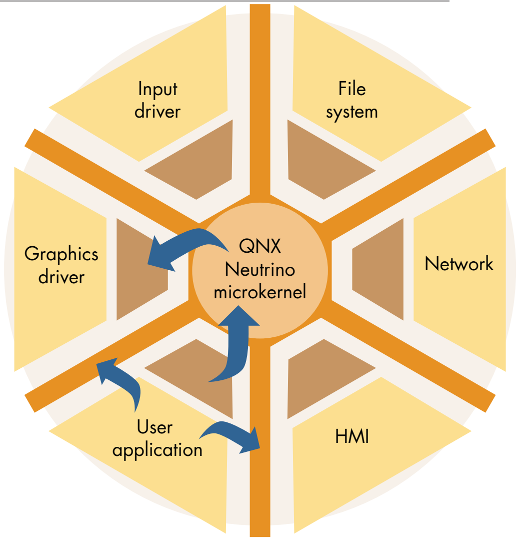
Know whom and where that user is, and what resources are currently available (power, Ethernet, Wi-Fi, etc.) that might be useful to transfer that information. Keep in mind a user might be on-site, off-site, human, or machine. The basics behind all industrial connected networks are to understand the problem or what you're improving, define the information that communicates this, and map out where that information needs to go.

"Don't integrate and collect everything," said Digi International's Young. "Too much information tends to lead people to lose sight of what they want to accomplish, and spend more money than necessary. Follow proper engineering design practices, and solve the important problem first."

A network divided against itself will not stand. "For IIoT to work properly, plant data and enterprise data need to converge," said Mike Hannah, manager of market development for Rockwell Automation. Develop a business plan that connects information technology with operating technology to find out if and where different networking technologies add value to the company.

As with any business plan, the financials will be important for managers. If the system costs more than it can return, it will be difficult to adopt. One must consider direct and indirect financial information. Indirect financials involve any new revenue streams generated from connecting a product or process. For example, collecting data can improve a customer's experience, or offer better warranties.

In addition, security can become a large expense for connected networks, thus dictating how much integration a company is able to start with. Even basic information must be secure. Rather than steal information, a person can introduce excessive data into a system to cause lag, or overload the system to trigger a shutdown.



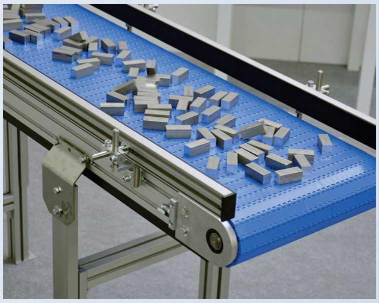
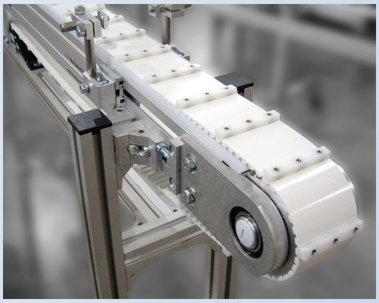
In one example of partitioning, the QNX Neutrino RTOS includes only the most fundamental services, such as signals, timers, and schedulers, in its processing center (typically referred to as the kernel). All other components—file systems, drivers, protocol stacks, and applications—run outside the kernel in the safety of memory-protected user space.

PROTECTING YOUR INVESTMENT

There are internal (people with access) and external (people without access) security threats. Internal threats may not have meant to be malicious. A culprit may have no clue he or she is causing a problem. This unawareness can make internal exploits difficult to combat and fix. An example of an internal security problem could be an engineer installing a camera to have a live feed of the shop floor. The camera consumes bandwidth and can potentially slow the network, causing errors and lag time that could stop manufacturing lines.

Another internal security threat could be contractors with access that might find a company's information to be valuable, or add access points to make their job easier. Different techniques can protect against internal and external security problems. Here's a short list of what's available:

- *Encryption:* If someone gains access to a company's network, they will only see gibberish and symbols. Encryption can give contractors access to work on a network, but not be able to see any information that might jeopardize security. Also known as cryptography, encryption is a serious method with strict U.S. government-published standards, namely the Federal Information Processing Standard (FIPS) 140-2.
- *Multiple networks:* "You need to have a seamless flow of information," according to Rockwell's Hannah. "Splitting up a network into multiple networks, such as NFC, intranet, and cloud technologies, can create more open access points that require protection. In addition, changes, upgrades, and other operations become more difficult and less streamlined. As you add more technology, you add more complexity, and modes of failure. One network is why some companies are going to fully integrated, cloud-based networks."
- *Partitioning:* Segmenting a network into sections helps prevent the occurrence of larger problems. By monitoring the sections and pinpointing where the problem started, troubleshoot-

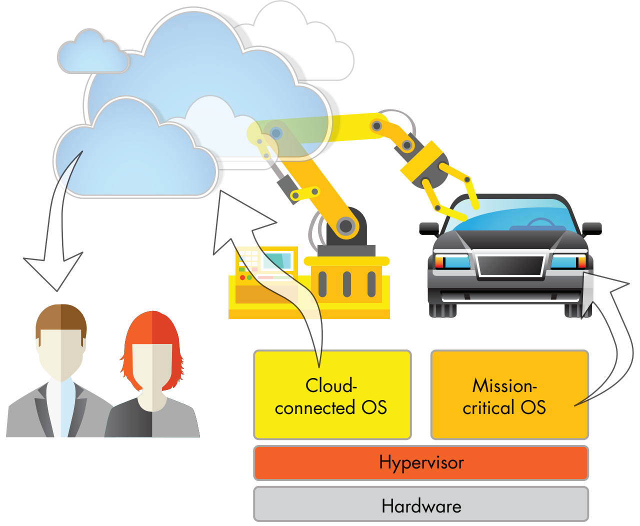



ing times can be reduced. You can also use time partitioning, which lets you assign a guaranteed minimum of CPU time to each set of processes or threads. This approach will work to prevent malicious software from starving critical threads of CPU cycles. In addition, it allows an algorithm to reassign CPU cycles from partitions not using them to those that can benefit from extra processing time.

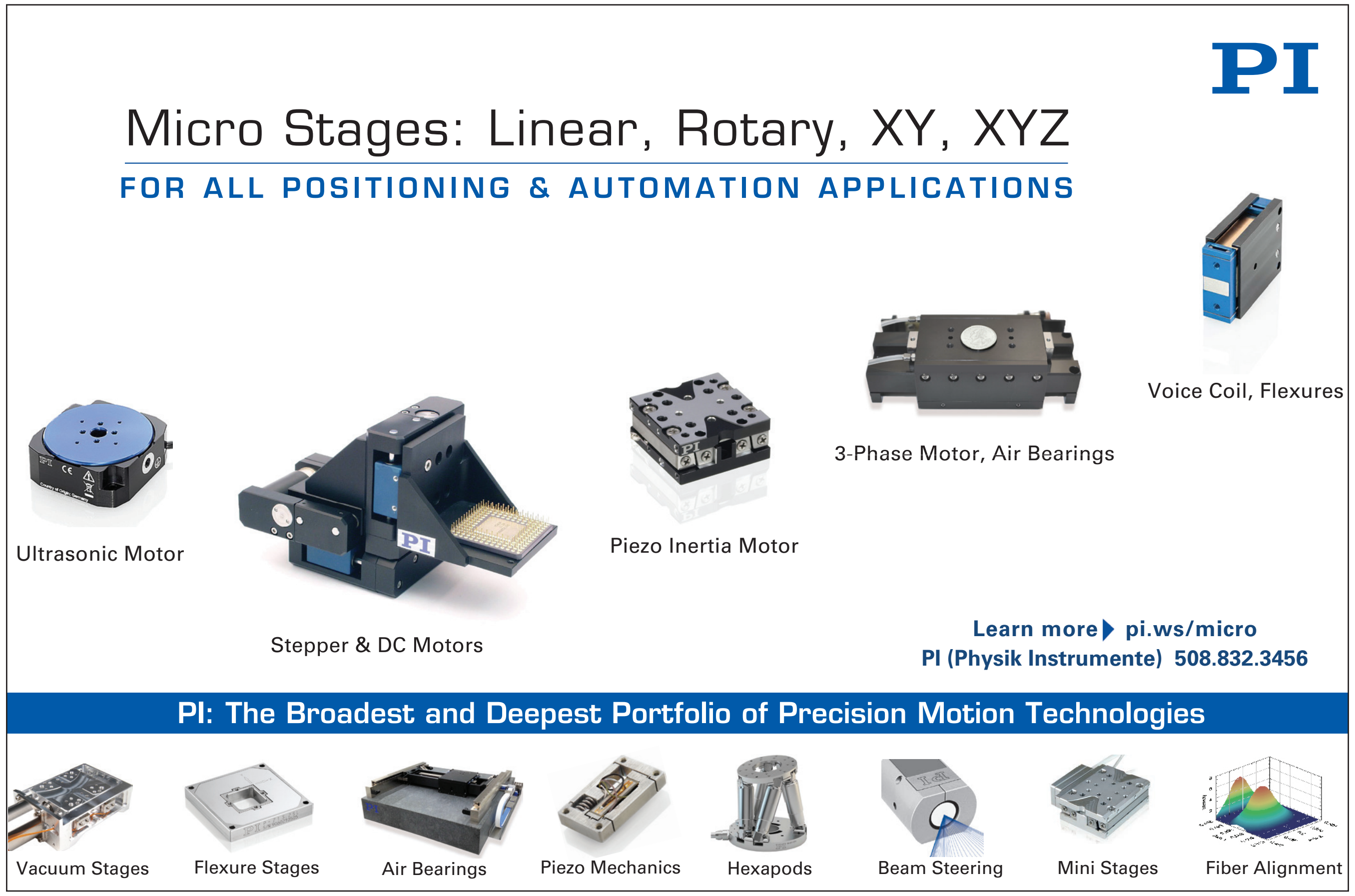
- *Prioritizing data:* It's possible to partition data by giving different priority to different threads. For example, if an undocumented camera were to enter the network, it would process important operational data first before non-priority data. Handling data by priority helps reduce security problems associated with bandwidth or processing speeds.

Protecting against security problems can never be 100%, but, as Hannah explained, "It's like a house. You can lock the door, but there are windows. If you lock the windows, you can break one, or even break down a wall. This depends on the value of what is in the house, but there is always a way in. Most problems can be reduced by following basic security practices, such as locking the network's openings, because it will not be worth the trouble of "breaking a window.""

Key management, a popular security method, uses passwords and keys to access different sections of the network.



Embedded developers can consolidate multiple operating systems ("guests") onto a single compute platform or system-on-chip (SoC) to reduce the cost, size, weight, and power of their system designs while maintaining clean separation and isolation of critical and non-critical applications. The QNX Hypervisor gives customers another means of protecting applications, in addition to a software system's existing safety-centric capabilities.



Sometimes a hacker might be persistent, though, and locking of openings may not be enough to protect trade secrets, customer credit cards, or national security.

When developing a company's business plan for a network, it's important to include two documents. One will lay out how valuable the connected information is worth. The second reveals how much damage and cost could be associated if someone was able to obtain that information and use it maliciously. Information associated with security, compared to the available budget, can change how much networking a company is able to start with.

On another front, a network business plan must answer the question: Is there any way that connecting a device could jeopardize worker security? A company may not want autonomous devices, such as a robot working in close proximity to workers, to have their programming changed with a simple remote push of a button—both for internal mistakes or external threats.

Once the problem and security are defined, a design of the network can be laid out. Often times, an Ethernet design is quick and easy, but you must be knowledgeable about standards.

"Many new standards are being formed around IIoT devices, so understanding standards becomes imperative," said Ankrum. "For example, when running an Ethernet cable through a power tray, the National Electric Coding (NEC) standards for power are different than the ones for communications."

DESIGN WITH THE FUTURE IN MIND

Standards will dictate how new devices or systems communicate and require unanticipated upgrades and cost. A system

TIPS TO SEEKING OUTSIDE IoT HELP

- Watch out for consultants that want to tell you how to solve your problem before they even listen to you or see the business plan.
- If a consultant uses lots of buzzwords without explaining them, or just doesn't communicate to you authentically, a third-party opinion or mediator can be beneficial.
- Remember to start small. Be careful of anyone who wants to start with a large, expensive system right off the bat. This can leads to bells and whistles, but not value.
- A red flag should go up if a contractor wants to integrate IoT, without clear explanation, into systems that aren't having any problems.
- The entire process must be economically viable. Otherwise, no connected device in the industry will be able to keep the company afloat.

must be designed with current standards and be aware of any that might be implemented down the road.

"A contractor or consultant may not know what standards organizations are working on, and project managers are often busy with other concerns," said Ankrum. "To find information on current standards and those that may be in the pipeline, going directly to the manufacturer of the device might be the best option."

To begin an industrial network, start small and build up. However, build with longevity in mind. Look beyond the current problem to what may happen after solving it. For example, a network might not need electrical shielding today, but a building strategy might bring upgrades, renovations, or equipment relocation that can cause network interference later on. If building plans indicate any future interference, shielding will be important.

System speed and bandwidth tend to increase over time. Looking ahead to determine potential network speed requirements will help reduce future lag time and unplanned upgrades. Ethernet is popular, but it's important to understand the different types.

"I always stress that for 10/100-Mb/s base Ethernet CAT 5E is still the cable of choice in designing a network for the future," said Ankrum. "CAT 5E supports both traditional Ethernet and Fast Ethernet. We run into scenarios where customers are tying in CAT 6 or even CAT 7 cameras into their existing network structure, and questions arise as to what type of cable will support this higher speed. If tied into an existing traditional or Fast Ethernet topology, the camera's max speed will be overall network speed. So, if your network is CAT 5E, the camera will not operate faster than this."

Investing in the fastest system is not always necessary. It's important to identify current and future high-consumption devices, such as high-resolution or high-speed cameras, and determine where and when they fit into a network. Selecting a network communication method with future speeds in mind will help add longevity to a network.

With so much to consider, collaboration is a good way to gain industry information. But don't be taken advantage of, either—you may wind up with a buzzword-happy consultant simply seeking profits in this burgeoning billion-dollar industry, rather than get the best system for your company. To reduce headaches with a subpar system, make sure you have answered some questions through development of a network business plan before talking to outside sources.