Aggregating Disparate Data Protocols on the Internet of Things

News stories about the Internet of Things tend to concentrate on consumer products like wearable tech and smart home appliances. In the consumer world, the focus is on the human experience and human interactions with machines. But the industrial Internet of Things will have different goals. Rather than creating new human experiences, it will focus on making machines more autonomous, increasing efficiency and productivity by reducing or even eliminating the need for human supervision.

You could call the Internet of Things a new device category layer that will link the formerly non-connected world with the connected world of PCs, tablets and smartphones. For consumers, that will often mean replacing older equipment with newer, smarter devices. But replacing existing equipment won't be as easy in the industrial world. Much of the infrastructure that is currently in place is far too valuable and far too complex to be discarded.

Rather than eliminating our existing M2M data networks and connected devices, the industrial Internet of Things will coexist with them for a long time. It will incorporate the older technologies, provide them with dramatic new capabilities, and increase their value.

To do this, industrial Internet of Things technology will need to accommodate disparate technologies, some of which are decades old. It will have to aggregate, convert and transmit multiple data networking protocols, from Modbus to TCP/IP. It will need to move data across fiber, copper, cellular and wireless connections. While adding smaller, smarter, more capable nodes to networks, the Industrial Internet of Things will also have to keep older equipment connected.

The Internet of Things Will Include the Internet of the Past

This isn't a complete break with the past. No single technology has ever been the best for every application, so industrial networks have always needed to connect multiple protocols and devices. Manufacturers have responded by developing a wide variety of protocol converters, making it easy to connect anything from Modbus to fiber.

But as the Internet of Things unfolds, protocol conversion will become more complex. More and more devices will be wireless. As was the case with wired connections, no single wireless technology is yet the best for every application. Cellular data networking, for example, can provide virtually infinite range, and the build-out of the 4G LTE networks will give it low latency and bandwidth that rivals fiber. But cellular data networking also uses data plans, which can make it less attractive when wireless data only needs to travel short distances, especially if that data is of low value. Wi-Fi, of course, requires no data plans. But even if connections are line of sight, its maximum range can be measured in kilometers. Low energy Bluetooth (Bluetooth LE) will be an important connection option for tablets and smartphones, but Bluetooth LE has even less range than Wi-Fi. Every wireless option has its own advantages.

Early Adoption of the Internet of Things

The ability to connect disparate data protocols will remain as important as ever, but the sheer numbers of connected devices is expected to explode. Simple protocol converters will continue to be very important, but the industrial Internet of Things will also call for single-box solutions that can aggregate multiple data streams and multiple protocols and move all of that data up to the cloud. These devices will require robust security, as wireless connections are inherently more vulnerable. And they'll need to be robust, resilient and increasingly autonomous, as they'll be tasked to function in increasingly remote locations and increasingly harsh environments.

I've been addressing many of these issues at my test site out in the Arizona Desert. It's a tank monitoring system for the Pinal County, AZ well owners co-op. Among other things, the system predicts system failures by measuring and aggregating pump current, and making decisions based on changes detected over time. It can SMS a technician to schedule preemptive maintenance before a catastrophic failure.

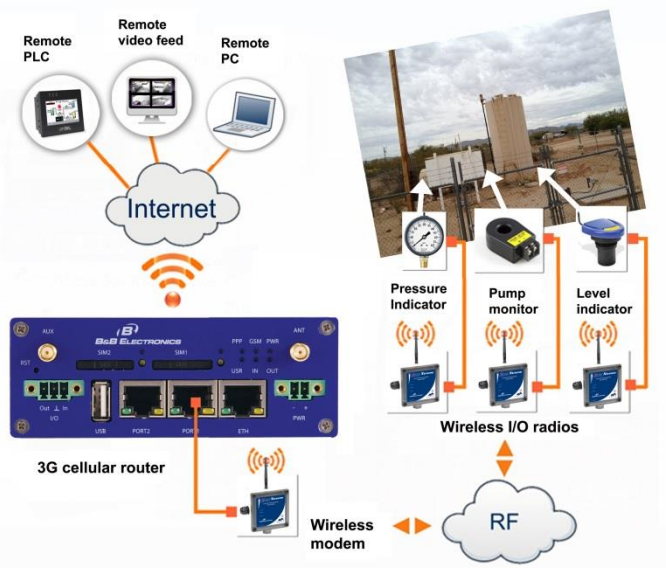

Figure 1

In an earlier incarnation, it used I/O radios to transmit data from pressure sensors, current sensors and level sensors to a radio modem. The radio modem then connected to a 3G cellular router, which provided Internet backhaul via the cellular telephone network. The router had built-in firewalls and powerful security protocols, and when combined with Virtual Private Networking (VPN) I was able to use the cellular system as securely as if it were proprietary infrastructure. (Fig. 1)

Since then I've been steadily adding new features and functionality. I've attached an IP security camera to the router's Ethernet port, for example. I'm currently adding some remote Wi-Fi sensors to the system, which bypass the I/O radios and connect directly to the cellular router.

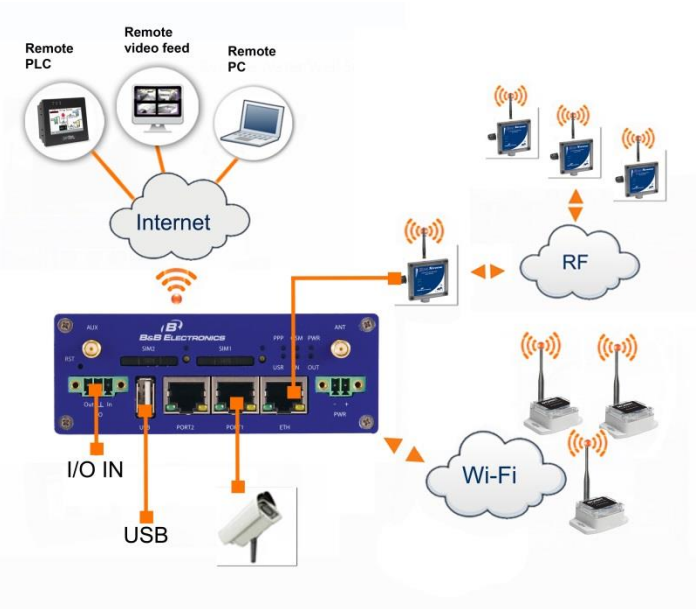

Figure 2

When the project began, with my I/O radios reporting their data to the cellular router, I think it would be fair to say that I was simply using the cellular router as a protocol converter with cellular backhaul. But as I add additional

devices and additional protocols to the system, I'm taking better advantage of the router's ability to function as a data aggregator with multiple backhaul options. (Fig 2.) I've migrated away from the old Internet model, and I've begun to apply the techniques of the Internet of Things.

But you'll note that there was no need to discard my old remote sensors. They're still connected, and they're still doing their jobs.