Line Down? No Problem.

Digi-Key Industrial Automation
Keeps You Running with Same-Day Shipping

1.800.344.4539
DIGIKEY.COM/IA
... with Interconnect Components & Hardware

Battery Clips, Contacts & Holders
Fuse Clips & Holders
Terminals and Test Points

Spacers & Standoffs
Plugs & Jacks
Multi-Purpose Hardware

IT’S WHAT’S ON THE INSIDE THAT COUNTS

KEystone ELECTRONICS CORP

www.keyelco.com  •  (516) 328-7500  •  (800) 221-5510

THiNK DESIGN SOLUTIONS
Listen to the advice being given for securing IoT devices and you are likely to be told that the level of security should be scaled to meet the probable threats. Internet-connected home thermostats, for example, should be designed to prevent compromise by hobbyists and serious hackers. But the usual recommendation is that there’s no reason to worry about a nation-state prying into your home thermostat. After all, wouldn’t North Korea have better things to do than screw around with the temperature in your house?

This philosophy about IoT security sounds completely reasonable. And it is completely wrong.

The reason emerged from a presentation by Princeton University researchers at last year’s USENIX Security Symposium. They found that it would be possible for attackers to grab control of high-wattage consumer devices – such as A/C units and heaters – to mount a large-scale coordinated attack on the power grid. The idea is to infiltrate numerous high-wattage IoT loads for the purpose of turning them all on or off simultaneously. Simulation results show these shenanigans could cause everything from local power outages to large-scale blackouts.

There is a precedent for the style of attack the Princeton researchers envision. In 2016, the Mirai botnet virus took down several major websites via a denial-of-service attack. (The botnet moniker arises from Mirai’s control of infected devices from a central set of servers.) Attacks took place via seemingly innocuous IoT devices that included home routers, air-quality monitors, and personal surveillance cameras. Researchers estimate that at its peak, Mirai infected over 600,000 vulnerable IoT devices.

Mirai proved how simple it can be to compromise large numbers of IoT devices. The initial version simply tried a fixed set of 64 well-known default login/password combinations in common use. Mirai found the vulnerable devices by randomly scanning the internet for targets and attacking. Once it got control of an IoT device, Mirai software reported to the attacking servers which then infected the device.

The Princeton researchers found that a sudden 30% rise in demand caused grid generators to trip. They figured an adversary would need access to about 90,000 A/C units or 18,000 water heaters in a target area to pull off this stunt.

Turning on loads in one area and turning them off in another could also cause further havoc. Power flows through the grid according to Kirchhoff’s laws, so the grid operator has almost no control of how power flows once generators kick in. Rising demand in one area can create line overloads and failures which, in turn, may cause further cascading line failures. Particularly at risk, say researchers, are tie lines connecting between neighboring power systems.

Even if hackers don’t succeed in shutting down the grid, they can dramatically drive up the costs of operating it. When demand exceeds planned capacity, the grid operator must purchase additional electric power from reserve generators. Power from these generators usually costs significantly more than that from the usual sources. Researchers ran simulations showing that boosting power demand during peak hours by just 5% can bring a 20% rise in the power generation costs.

All of which should give you pause the next time you hear a security expert smugly claim consumer IoT devices don’t need protection from well-organized cyberwarfare agencies.
FOR YOUR NEXT EGGCELLENT IDEA

BATTERYHOLDERS.COM
A major goal behind all of the IoT and IIoT efforts is to create smart factories that will autonomously optimize manufacturing processes. One of the keys to achieving this goal will be time sensitive networking.

It is easy for developers to get tripped up when cramming multiple antennas into the small spaces that characterize IoT applications. Automated onboarding and security features now help speed the integration of embedded devices into IoT systems.

Battery chemistries each have special qualities that can make certain cells impractical for varying kinds of internet-of-things applications. It is easy for developers to get tripped up when cramming multiple antennas into the small spaces that characterize IoT applications.
Time Sensitive Networking for industrial systems: Why an ecosystem approach is needed

With TSN’s intelligence in the network, a system can become more automated and less dependent on human intervention and subsequent error.

ANIL KUMAR • DENZIL ROBERTS, PH.D. | INTEL
STEVE ZUPONCIC | ROCKWELL AUTOMATION
AVNU ALLIANCE INDUSTRIAL SEGMENT MEMBERS

The Industrial Internet of Things (IIoT) represents massive opportunity for the factory automation and industrial markets. IIoT growth is increasing the amount of data harvested through distributed networks, requiring new methods for managing and transferring critical and non-critical information and mechanisms for streamlined operational and manufacturing models.

Key stakeholders and decision-makers increasingly look for new ways to optimize systems and operational management models, while helping to bring their company to the forefront of this growth. Demand for higher levels of reliability and security are increasing and engineers are looking to alternative solutions to today’s many specialized and segregated industrial communication standards. The latest set of IEEE 802.1 Time Sensitive Networking (TSN) standards represents the next evolution of standard Ethernet technologies, targeted to meet these new market demands.

HISTORICAL NETWORK CONFIGURATION

Traditionally, industrial network configuration has been managed on a component-by-component, switch-by-switch, and node-by-node basis. The software used for such configuration has been similar to DOS in its presentation, using such interfaces as CLI (command line interface) where hierarchical precepts are often inferred and knowing where one is in the command hierarchy is often not intuitive or clear. Furthermore, if the configuration of one switch or router requires a complementing configuration in an adjacent router or switch, any configuration error in either of the adjoining components would cause problems in the network. Essentially, there is no system-level knowledge at the component level for configuration.

If you were to look at the command lines in a CLI interface or PuTTY (terminal emulator) interface, which are both cryptic and difficult to navigate, you would be asking yourself the following questions: “What set of skills must I hire to manage my networks?” and “Is this really necessary in the year 2019?”

WHAT DOES NETWORK CONFIGURATION LOOK LIKE WITH TSN?

Time Sensitive Networking (TSN) is a collection of Ethernet standards introduced by IEEE, which defines a new set of mechanisms for managing traffic. TSN standards define new functions for Ethernet networking such as traffic shaping, frame pre-emption, traffic scheduling, ingress policing, and seamless redundancy. When all parts of a network are running with the same sense of time, traffic can be coordinated based on a schedule, one method that allows for better control of critical traffic. These features provide a whole new layer of control for managing Ethernet traffic; but from a business perspective, is it worth the investment? And if TSN represents yet another layer of new standards added to an already complex system, how can TSN create a simpler system for the end user?

TSN standards were specifically designed to facilitate system-level configuration and were created with a system view in mind, rather than from a component perspective. TSN enables end-stations to publish their requirements on the network and allows bridges and switches in the system to announce their capabilities to the wider network. As an example, the “P802.1Qcc – Stream Reservation Protocol (SRP) Enhancements and Performance Improvements” specification is one of the mechanisms that allows the network infrastructure to be more intelligent at a system level and to convey the information necessary to move the control plane from a manual configuration workflow to an automated process.
Consider the following architecture:

In the future architecture pictured above, the user has a view of the system that allows for the configuration of the I/O and control devices as well as for the layout of the topology and the infrastructure devices. A core principle of TSN is that all network communications are managed so that performance and data delivery are guaranteed.

This future architecture gives users a view of a system that allows for the configuration of the I/O and control devices as well as for the layout of the topology and the infrastructure devices. A core principle of TSN is that all network communications are managed so that performance and data delivery are guaranteed.

TSN IN INDUSTRIAL IOT APPLICATIONS – WHAT IS THE BUSINESS VALUE?

The industrial market currently requires two types of networking professionals: informational technology (IT) and operational technology (OT). The current industrial control and associated enterprise-wide systems require many IT and OT personnel to manage and configure network infrastructure and control system parameters. Now, with TSN and its potential for smart software, the smart system could handle configuring the network infrastructure. With TSN’s intelligence in the network, it becomes more automated and less dependent on human intervention and subsequent error.

Investment in intelligent systems and devices capable of participating in a wider, self-configuring ecosystem can potentially reduce costs. Software Defined Networking (SDN) type tools can enable system-level configuration software, as well as diagnostic and monitoring tools. These new mechanisms would allow the end user to finally manage the network from the manufacturing floor to the business systems.

THE BENEFITS OF COMMON TIME

Digitization and its benefits require a time-stamped data collection to provide a chronology of events, time-based analysis, time-series analytics, and finally, a model for predictable outcomes. The analysis of time-stamped data can help system managers see exactly what went wrong, as well as where and when.

TSN provides a common reference of time in which to do this. The same clocks required for traffic scheduling on the network can be synchronized with other time domains for a wider view of system events or faults. Essentially, “TSN time” can be correlated with time in the enterprise systems so that events and conditions on the plant floor are chronologically comparable to events within the company’s business systems. Consider a case where more precise understanding of when a product was completed is needed in manufacturing, with respect to the distribution systems that will move such product to the consumer. In the supply chain, there could be a tighter understanding of when products are completed against when the material to produce such products needs to be reordered. What if the cause and effect of faults on the plant floor could be more easily viewed at a system level through a sequence of events capability, where time is common across the entire manufacturing facility? Such capabilities present an opportunity for higher efficiencies that, ultimately, are reflected in a company’s financial success.
Time Sensitive Networking (TSN) is a collection of Ethernet standards introduced by IEEE, which defines a new set of mechanisms for managing traffic. TSN standards define new functions for Ethernet networking such as traffic shaping, frame pre-emption, traffic scheduling, ingress policing, and seamless redundancy. When all parts of a network are running with the same sense of time, traffic can be coordinated based on a schedule.

In summary, TSN enables the convergence of networks and systems that were previously kept separate for reasons of operational integrity, real-time performance, safety or security. Breaking down communication barriers between critical and noncritical systems is a foundational concept of the IIoT and Industry 4.0. With TSN and time synchronization, insights from real-time data at the edge arrives on time from anywhere, no matter how demanding the environment. Choosing TSN changes the industrial model and workflow with fewer workers for a more converged and deterministic network built on platforms to protect investments long-term.

However, today, many of the underlying systems for Industry 4.0 applications are based on proprietary standards and could present integration challenges. A lack of a broader industrial networks ecosystem perspective in terms of business systems, platforms and standards as well as interoperability could present a significant challenge for the adoption of Industry 4.0 into modern workflows. To take full advantage of these systems, an ecosystem perspective to standards, profiles and tests is what will make these systems interoperable and able to coexist to allow business to derive the maximum value from Industry 4.0 applications.

**HOW IS THE ECOSYSTEM BEING NURTURED?**

Many consortia, industry and government bodies as well as standards associations are working to establish standards, associated profiles and tests.

Avnu Alliance is one such body that facilitates a common TSN platform through various services, including open-source software, testing tools, and test plans to develop and verify the correct operation and implementation of TSN-enabled products.

Test plans can be used by test houses, protocol organizations and test equipment manufacturers to ensure the industrial market is testing to the same TSN specifications and guarantee an interoperable network layer for proper system interoperability.

Various industry consortia and standards organizations, such as IEEE and Industrial Internet Consortium, as well as organizations who provide conformance testing for application layers, collaborate to create a set of unified standards and an interoperable ecosystem for the industrial market. Due to the broad set of use cases addressed by IIoT, the market continues to require multiple upper-layer protocols for networked industrial systems. These upper level protocols can share a common TSN foundation.

Since TSN provides a standards-based foundation, system designers and engineers would be able to architect a network that will stay current with evolving use cases.

**Avnu Alliance**

www.avnu.org

Authors contributed to this article in their personal capacity. The views expressed are their own and do not necessarily represent the views of Intel Corporation or Rockwell Automation.
You probably already use Tadiran batteries, but just don’t know it!

If you have a smart automatic water, gas, electricity, or heat meter in your home.

If you have an electronic toll collection transponder, tire inflation sensor, or emergency E-CALL system in your car.

If you have a GPS tracking device on your trailer, container, or cargo.

If you have wireless sensors, controls, or monitors in your factories and plants.

If you use electronics with real-time clock or memory back-up in your office.

If you have never heard of Tadiran Batteries, it is only because you have never had a problem with our products powering your products.

Take no chances. Take Tadiran batteries that last a lifetime.

*Tadiran LiSOCL2 batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.
Basics of wireless power transmission design

Most consumer devices that transfer power over wireless links follow the Qi standard. The construction of these power transfer systems is simpler thanks to the availability of new reference designs.

Examine the wireless charging setup used in the passenger compartment of most vehicles and you are likely to find a system that follows the Qi standard. Promoted by the Wireless Power Consortium, Qi applies to power transfer over distances of up to 40 mm (1.6 in). Charging takes place via magnetic induction between a charging pad and a compatible wireless receiver.

Qi divides charging into low and medium-power categories. Low-power covers up to 5-W chargers as are typical of smartphones, Bluetooth earpieces, and so forth. Charging takes place via a signal in the 110 to 205 kHz range. Medium-power chargers deliver up to 120 W via signals ranging between 80 and 800 kHz.

A limited data transmission takes place between the charger and the mobile device being charged. Transmitted data provides information about the state of charge and similar parameters so the charger can shut down when the battery is charged.

The charger first begins charging when it detects a change in capacitance or resonance in its transmitter coil. When the charger detects an object, it sends an 8-bit data string on the charging carrier. The mobile device then must respond with information about the signal strength it detects. The charger in turn sends multiple pings back indicating the optimum positioning for the mobile device. Charging commences when the mobile device has been validated and positioned correctly.

During the charge process, the mobile device sends data packets (at about 2 kbps) that adjust the power level and finally end charging.

Qi chargers also can sense the presence of foreign objects in the charging field. When this happens, the charger cuts out.

The Wireless Power Consortium spells out a number of mechanical and electrical parameters for Qi wireless charging, including the make-up and configuration of the charging coils.
WPC transmitter reference design parameter examples

TRANSMITTER DESIGN

All wireless transmitters have four common building blocks: transmitter coils and resonance capacitors, a full or half-bridge inverter, a modulator/demodulator handling communication packets, and circuits that sense power transfer and protect against conditions arising from factors such as foreign objects in the resonance field.

Several factors drive decisions about the design of specific Qi chargers. The desired maximum output power determines charger circuit working voltages. A 5-W output can employ circuits on a 5-V supply; 10-W outputs demand 9-V supplies; 15-W outputs generally use 12-V power rails. The Qi specification spells out that transmitter and resonance capacitance.

The Wireless Power Consortium publishes transmitter reference designs that make recommendations for various transmitter qualities. For example, the WPC library of coil types defines coil mechanical details that include the dimensions, thickness, and the make-up of the coil layers; the ferrite shielding material and its thickness; and electrical details such as the circuit configuration, inductance, capacitance, input voltage range, and range of operating frequencies.

The reference design employs Litz wire – multistrand wire designed to reduce skin and proximity losses for frequencies up to about 1 MHz – and specifies the number of turns and inductance necessary for gain and coupling. Also specified are resonance capacitors that are a COG ceramic type (for high dielectric stability) and carry a 50-V rating for 5-W chargers, 100-V for those handling 15 W. The design as well dictates that FETs used for driving the charge coils have a low, guaranteed $R_{\text{DSon}}$ at a $V_{\text{GS}} = 4.5$ V, as well as a low $C_{\text{iss}}$ (total input capacitance) to minimize switching losses and time delays and a current rating above 8 A.

The reference design specifies several ancillary components for the transmitter bridge. They include ceramic decoupling capacitors placed near the switching FETs. These are designed to keep switching energy out of the rectifier stage. And a low-pass filter sits between the FET coil drivers and the resonant tank, used to meet CISPR25 EMI standards.

The reference design controls transmitter power by varying the frequency, duty cycle, or bridge voltage. Duty cycle variance takes place once the resonant frequency is fixed.

Communication between the transmitter and receiver takes place via ASK (amplitude shifted keying) and FSK (frequency shifted keying) with charging profiles for Qi specify dimensions and configuration details to ensure charging transmitters and receivers from different vendors will interoperate.
ASK used for sending data from the receiver to the transmitter, FSK for transmitter data going to the receiver. ASK communication is inherently slow. It is used to establish the power-transfer contract and may serve as a means of authorizing specific receivers to get charged. The receiver implements ASK modulation by switching a transistor on and off which changes the gain of its resonant tank slightly. The transmitter can detect this change to decode the ASK messages.

The capacitors used for generating the ASK modulation are generally 22-nF or 47-nF MLCC devices. One potential difficulty is that these MLCC caps can generate audible noise during communications because of the ac voltage across them. Substitution of a tantalum capacitor for some of the MLCC capacitance may help eliminate the noise. However, a point to note is that it’s generally best to apply a voltage derating to tantalum caps to avoid high failure rates.

The transmitter controller IC reads the ASK signal and may apply filtering to minimize the chance of data errors. That’s because the coupling process, any nearby permanent magnets, or transient loads can corrupt the ASK signal. The WPC spec. defines the ASK bit encoding scheme with each data packet including a preamble, header, message, and checksum. Each byte includes a start bit, eight-bit data, parity, and a stop bit.

To implement FSK, the transmitter shifts its frequency over a limited range. Its typical use is to send acknowledgements to the receiver though it may also send proprietary data packets. The modulation depth and polarity are established in the negotiation phase of the connection. The receiver IC demodulates the FSK data.

Qi systems use a control error packet (CEP) as a feedback mechanism to control transmitter power. The fastest CEP rate is about 50 msec/packet, and each CEP packet spans about 20 msec. The receiver calculates a value for the CEP by comparing actual battery voltage with a target. A positive CEP tells the transmitter to send more power by boosting the duty cycle or reducing the operating frequency. A negative CEP packet causes the opposite effect. If the transmitter doesn’t respond to the CEP, the receiver must shut down and send an End of Power Transfer signal.

Several protection mechanisms for the charging process include:

- **Temperature Detection:** Uses thermistor at the receiver to monitor temperature and shut down the transmitter if overheating is detected.
- **Overload Protection:** Limits current to prevent damage.
- **Short-Circuit Protection:** Cuts off power if a short circuit is detected.
- **Under-Voltage Protection:** shuts down if the voltage falls too low.
- **Over-Voltage Protection:** shuts down if the voltage exceeds a safe limit.
- **Over-Frequency Protection:** shuts down if the frequency exceeds a safe limit.

One way Qi systems detect foreign objects in the charging path is to calculate the power lost between the transmitter and receiver. When it exceeds a threshold, the system shuts down.
power transfer interface and limit the generation of heat. Over-voltage and over-current protection avoid short circuits and over-loads, low voltage (currents too high) and high voltage (too much energy transferred) conditions.

Facilities for foreign object detection (FOD) involve a continual calculation of power lost between the transmitter and receiver. The receiver periodically sends a received power packet (RPP) back to the transmitter. The RPP value is computed by first calculating the received power (rectified $V \times I$), then multiplying by a gain and adding an offset. The gain and offset values are programmed in the receiver IC and depend on loading and the receiver modes. A difference in the power received vs. power transmitted triggers a shut down.

Wireless chargers of different power levels use different power-difference thresholds to shut down. For Qi BPP designs the power difference threshold is 350 mW. For the higher-power EPP designs there is a 350-mW threshold for 5 W, 500 mW for 10 W, and 750 mW for 15 W.

A further point to note is that it takes accurate sensing to distinguish between differing power levels caused by offset of misaligned receiving devices and those caused by foreign objects. That is one reason why EPP designs also do FOD based on a change in quality factor, Q. The operating principle is that a foreign object reduces the transmitting coil inductance and the series impedance, reducing the Q of the resonant circuit.

FOD based on a change in Q closely resembles that based on a change in received power. The receiver sends a reference Q to the transmitter, which then sets an appropriate threshold. Power transfer terminates if the measured Q is below the threshold. To realize this behavior, the procedure is to first sweep the frequency through resonance while recording the peak voltage and the two frequencies (one on either side of resonance) at which voltage is below the peak by $1/\sqrt{2}$. Then Q is the resonant frequency divided by the difference between the upper and lower frequencies. A rise in the impedance facing the transmitting coil indicates the presence of a foreign object.

Finally, it is worth mentioning the energy efficiency involved in Qi wireless power transfer. An example comes from the IDT P9261 reference design, a 15-W wireless charging transmitter aimed at vehicle passenger compartments. This circuit provides an energy efficiency exceeding 70% when output power exceeds 8 W and more than 60% efficiency for outputs between 8 and 5 W. Examining the sources of transmitter loss reveals that coil losses make up 57% of the total losses, and MOSFET $R_{ds-on}$ accounts for another 14%. Single-digit losses come from factors such as MOSFET switching, capacitor series resistance, PCB loss, and the current-sense resistor.

REFERENCES:

Manufacturers in the medical industry face unique challenges in terms of product mix, throughput requirements, quality standards, and regulatory guidelines. Whether a company is producing diagnostic equipment for cancer screening, disposable devices such as syringes, or implantable devices such as stents for cardiac procedures, the manufacturing process must be absolutely error-free while delivering high throughput. To achieve these seemingly competing goals, companies are investing more in factory automation. And with the rise of Industry 4.0 and the Internet of Things (IoT), medical device and equipment manufacturers are finding that implementing automation in their operations not only improves throughput and quality but provides other benefits as well.

Tips on how you can reduce costs and time in all project phases - from machine design to building and testing of equipment, from shipping to installation and throughout the life of the production equipment.

RICH HANSEN • SENIOR AUTOMATION ENGINEER
BOSCH REXROTH CORPORATION
INTEGRATING AUTOMATION AND INFORMATION TECHNOLOGY

Medical device and equipment manufacturers demand more automation not only of individual processes, but also of entire factories to help them meet strict quality requirements mandated by the U.S. FDA (Food and Drug Administration) and other government agencies. This means automation of the complete manufacturing and handling value chain, including product testing, inspection, packaging, and storage and retrieval.

Just mentioning automation typically triggers visions of manufacturing plant floors filled with robots and machinery. However, the future of automation also applies to the "behind the scenes" functions of data collection and manipulation. For example, when the FDA requires documentation of machine parameters and deviations on a part-by-part basis, automated data collection allows the manufacturing parameters to be collected and stored automatically, as well as written to files tied to individual serial numbers, providing the required part-by-part verification.

The key to achieving these goals, however, is not simply a matter of adopting more automation. It lies with the core principle of Industry 4.0, which is to combine automation and IT (information technology).

INDUSTRY 4.0 INITIATIVES DRIVE OPENNESS AND EASE OF USE

One example of a solution that makes this connection between automation and IT is the Open Core Engineering platform, which combines software tools, functional toolkits, open standards, and Open Core Interface technology.

The Open Core Interface allows programmers and operators to use a familiar software platform – such as National Instruments’ LabVIEW, Java, or CATIA – to control the machine, eliminating the need to learn ladder logic or other programming language. The platform includes Software Development Kits (SDKs) that can be
The definition of Industry 4.0 was first introduced in 2011. Although there are varying explanations of what exactly Industry 4.0 entails, Germany Trade and Invest (GTIA) – the economic development agency of the Federal Republic of Germany – defines Industry 4.0 as:

“A paradigm shift... made possible by technological advances which constitute a reversal of conventional production process logic. Simply put, this means that industrial production machinery no longer simply “processes” the product, but that the product communicates with the machinery to tell it exactly what to do.”

The consulting group McKinsey & Company defines Industry 4.0 in more specific terms, as: “The next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business-intelligence capabilities; new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing.”

**Key Insights & Considerations:**
Medical device and equipment manufacturers are demanding more automation of the complete manufacturing and handling value chain.

Automation applies not only to manufacturing processes, but also to data collection and manipulation.

The key to achieving error-free, high-throughput manufacturing lies with the core principle of Industry 4.0, which is to combine automation and IT.

Industry 4.0 enables the collection and use of manufacturing data to improve quality, reduce turnaround times, and meet regulatory requirements.

To fully capitalize on the benefits of Industry 4.0, choose vendors who have designed products and systems with the integration of automation and IT as a core principle.

used, for example, in Excel’s VBA to create a user interface for controlling a motion axis. Then the axis can be run directly from Excel, or the program can be pushed from Excel to a PLC.

In smaller medical laboratories, where technicians work directly with the automation systems, it's often necessary for them to make changes to programs, test points, and other machine parameters specific to the sample being tested. The Open Core Interface allows the machine builder or end user to create an interface that provides technicians with access to certain levels of machine control to customize or change the operation. Once the interface is created, a simple handheld tablet with Excel can transfer the interface to a PLC. This is an alternative to machine-grade HMI. In addition, the interface offers portability, wi-fi connectivity, and Bluetooth already built-in.

Machine interfaces are also the root of data collection, but the true benefit of Industry 4.0 is found in how that data are used – for part tracking, error reduction, or process stability – all of which play a critical role in the manufacture of medical devices and equipment. The controller, or IoT gateway, is at the heart of many solutions for Industry 4.0, allowing a user to capture data and broadcast or use that data in a manner that helps them improve quality, reduce turnaround times, and meet regulatory requirements. Software such as ActiveCockpit serves as an interactive communication platform that processes and visualizes production data in real time, easily connecting with back-end MES or ERP systems, allowing rapid diagnosis and optimization of machines and processes.

For example, Open Core Engineering principles are used with EFC variable frequency drives, which include networking capabilities for remote control and monitoring. When used with VarioFlow plus conveyor systems, users have easy access to the machine through wireless or Bluetooth connectivity. Such connectivity allows an operator to adjust speeds, inspect diagnostic codes, view machine parameters, or take any action deemed acceptable according to their clearance level – without ever opening an electrical enclosure or summoning the engineering department for support. Similarly, maintenance personnel can be alerted to problems with email or text messages and receive diagnostic codes without having to travel to the machine and connect to it.

Of course, the security of data gathered, stored, and shared through IoT and Industry 4.0 applications is a significant concern in medical device manufacturing and diagnostic industries. The more data made available, the more opportunities there are for the information to be used inappropriately. It’s unavoidable that any time there is an IoT gateway on a machine, there is a risk of leaks or hacks. Security is the biggest hurdle to complete adoption and integration of Industry 4.0 principles, so users and machine builders need to understand the risks and how they can be mitigated or reduced. Look for cloud-based apps that use certificate authentication, and an external industrial VPN is recommended for secure remote access.
CAPITALIZING ON THE BENEFITS OF INDUSTRY 4.0

The scale of capital investment required for automation in medical device and diagnostic equipment manufacturing, together with the critical nature of the products and processes, place tough demands on suppliers for robustness, accuracy, and interoperability of the parts and systems used in automation and Industry 4.0 initiatives.

As Industry 4.0 and IoT projects expand their reach across the manufacturing floor, products that were once seen as commodities – such as linear guides, ball screws, and sensors – will become key enablers of advanced functions, including real-time monitoring, predictive and preventive maintenance, and part tracking. Combining traditional automation with advanced sensing technologies, such as the XDK sensor box, which is a turnkey kit that provides instant IoT connectivity for devices or machines, is just one example of this type of integration.

Manufacturers of medical devices and diagnostic equipment are relying more and more on automation to ensure a fully robust process to meet regulatory requirements. Complete automation solutions require ease of use and interoperability. Fortunately, vendors such as Bosch Rexroth have designed products and systems with the integration of automation and IT as a core principle, allowing customers to fully embrace and capitalize on the benefits that Industry 4.0 can provide.

Bosch Rexroth
boschrexroth.com

REFERENCES:


The time sensitive networking (TSN) protocol is an addition to the IEEE Ethernet related standards and is starting to become popular for industrial networks. TSN lets network designers combine real-time control communication with non-real time information communication while maintaining deterministic performance. This is not possible with conventional Ethernet.

A major goal behind all of the IoT and IIoT efforts is to create smart factories that will autonomously optimize manufacturing processes. One of the keys to achieving this goal will be time sensitive networking.
A number of network and communication protocol developers are incorporating TSN in their protocols. Here’s a closer look at what CC-Link is doing.

CC-Link offers a number of networks. In 2007, the organization introduced CC-Link IE, the first industrial open network in the industry based on 1 Gbps Ethernet. Throughout the years, the organization has expanded its range of protocols.

- CC-Link IE Control is a trunk network that connects controllers within a factory.
- CC-Link IE Field covers general input/output control, connecting controllers with a variety of field devices.
- CC-Link IE Field Motion suits motion control applications.
- CC-Link IE Safety is for safety control

In 2016, CC-Link IE Field Basic was added to the lineup to extend compatibility to 100 Mbit devices.

Recently, CC-Link introduced CC-Link IE TSN. This specification is the first to combine gigabit Ethernet bandwidth with time sensitive networking (TSN).

TSN was added to increase openness while strengthening performance and function. It also supports more development methods, enabling easier implementation on a wider range of equipment and increasing the number of compatible products and is expected to accelerate the construction of smart factories using the IIoT.

**WHY USE TSN?**

Manufacturing continues to add automation to reduce TCO (Total Cost of Ownership) and improve quality. But it also needs to embrace new manufacturing methods such as mass customization.

With physical manufacturing and the digital industry converging, the information-driven society fueled by IT-based data continues with the development of sensing technology, higher-speed networks, the spread of cloud/edge computing, and the development of AI (artificial intelligence).

Throughout the world, manufacturing industries are moving toward the use of the IIoT, such as Industry 4.0 in Europe, the IIC (Industrial Internet Consortium) in the US, Intelligent Manufacturing in China, and Connected Industries in Japan. All of these share a common goal: the creation of “smart factories” in which everything is connected, data are used to the fullest, and optimized manufacturing takes place autonomously.

To create smart factories, essential issues include gathering real-time information from production processes, processing it with edge computing, and then transmitting it seamlessly to IT systems. Toward that end, one crucial need is a network capable of high-speed, stable control communication as well as large-volume information transmission to IT systems. In other words, it is important to combine industrial networks at production sites with IT system networks.

While a variety of industrial networks are currently in use, it is difficult to achieve interoperability between them, leading to “islands” of automation that decrease process transparency. Demand for TSN support will increase, as this technology makes it possible to mix different networks on the same trunk line and provide real-time communication through time synchronization.

CC-Link IE TSN enables easy connection from upper level IT systems to OT systems at production sites, expanding the use of a variety of applications in manufacturing industry.

To realize smart factories, productivity improvement through higher equipment performance and function is essential, along with advanced motion control.

**Smart integration of control and information communication.**

Achieve smart factories by integrating IT system information communication and other open protocols on the same network while running real time control.
This is especially true in industries such as semiconductor and battery manufacturing. CC-Link IE TSN builds on the benefits of CC-Link IE by improving communication functions and synchronization accuracy. Thus the motion control capabilities have been enhanced. It has thus been created as a next generation industrial open network to accelerate the construction of smart factories.

AN OVERVIEW OF OPEN TECHNOLOGY
CC-Link IE TSN’s protocol uses layers 3 to 7 of the Open Systems Interconnection (OSI) reference model, building on the TSN technology located in layer 2.

TSN consists of multiple international standards. The major standards are IEEE802.1AS (which defines the time synchronization method) and IEEE802.1Qbv (which defines the time sharing method). Combining these to the Ethernet standard enables punctuality, ensures transmission within a given period of time, and mixed implementation with other communication protocols.

The Ethernet standard protocols that can be used are IP at the third layer and TCP/UDP at the fourth layer. Protocols such as SNMP, HTTP, and FTP can also be used in the upper levels. This arrangement delivers more flexible network administration as general purpose Ethernet diagnostic tools can be used for network diagnosis.

COMMUNICATION METHOD
CC-Link IE TSN uses time-sharing, a revolutionary cyclic communication concept.

Conventional CC-Link IE uses a token passing method. A station transfers transmission rights to the next station after transmitting its own data by transfer of the token.

In contrast, CC-Link IE TSN uses common time synchronized across the network. The input and output communication frames are simultaneously transmitted in both directions in a fixed time. Combining this method with TSN technology shortens the network cyclic data update time.

INCREASED PROFILE SUPPORT AND DIAGNOSTICS
The CC-Link Partner Association has defined CSP+ (Control & Communication System Profile) to make it easier to start up, operate, and maintain devices compatible with the CC-Link family. By using CSP+, CC-Link IE TSN has added support for CANopen device profiles. For example, communication using international standard IEC61800-7 (CiA402) is possible.

SUPPORT FOR GENERAL-PURPOSE NETWORK DIAGNOSTIC FUNCTIONS
CC-Link IE TSN network devices can be examined using SNMP (Simple Network Management Protocol), which is widely used for monitoring IT networks. CC-Link IE TSN component information and statistical information are defined as extended MIBs (Management Information Bases), allowing general-purpose SNMP tools to be used for network diagnostics.

KEY FEATURES OF CC-LINK IE TSN
By giving a high priority to cyclic communication for device control and by allocating bandwidth preferentially over information communication, CC-Link IE TSN communicates information with IT systems while controlling system devices with real-time cyclic communication. This mixture with information communication means that devices using UDP or TCP communication (such as machine vision systems) can be connected to the network for high accuracy monitoring, diagnostics and analysis.

RAPID SYSTEM SETUP AND ADVANCED PREDICTIVE MAINTENANCE
CC-Link IE TSN is also compatible with SNMP, enabling easier diagnosis of network devices. Until now, special tools were required when collecting device status information. However, general-purpose SNMP monitoring tools can be used to gather and analyze data from devices.
If a network error occurs, the TSN protocol makes it possible to check operation logs and accurately trace events up to the error in chronological order. This can help to identify problems and can lead to quicker recovery.

The time synchronization protocol regulated by TSN calibrates time differences between devices compatible with CC-Link IE TSN, keeping them synchronized. Time information stored in both master and slave devices is kept synchronized to the microsecond. If a network error occurs, this makes it possible to check operation logs and accurately trace events up to the error in chronological order. This can help to identify problems and can lead to quicker recovery.

It is also possible to provide production site information and accurate time information to IT systems. This will allow AI enabled data analysis to provide further process improvement through predictive maintenance.

**MAXIMIZING THE PERFORMANCE OF MOTION CONTROL AND REDUCING CYCLE TIME**

CC-Link IE TSN uses the time-sharing method with time trigger and bidirectional simultaneous communication to achieve a cycle time of 31.25 microseconds or less. Adding sensors or increasing the number of servo amplifier axes required for control to expand a production line has minimal effect on overall cycle time in systems operated with CC-Link IE TSN. Cycle time may even be reduced compared with systems operated with conventional networks.

CC-Link IE TSN allows equipment with different communication cycles to be used together according to the performance of each device. Until now, devices connected to the same master station had to be operated using the same cyclic communication cycle (link scan time) throughout the entire network. CC-Link IE TSN allows for multiple communication cycles to be used within the same network.

Thus, it is possible to optimize communication cycles by the characteristics of each device. For example, devices (such as remote I/O) not requiring a high speed communication cycle can be connected while still maintaining the performance of devices requiring high performance communication cycles (such as servo amplifiers). This can also maximize the potential of slave devices on the network and improve productivity throughout the entire system.

**MORE OPTIONS FOR DEVICE VENDORS**

For conventional CC-Link IE to make effective use of its 1 Gbps bandwidth device development vendors had to implement both master and slave device functions with hardware using dedicated ASICs or FPGAs.

CC-Link IE TSN supports implementation on both hardware and software platforms. ASIC and FPGA based hardware methods are supported. Moreover, development with software protocol stacks on a general purpose Ethernet chip is also possible to optimize communication cycles by the characteristics of each device. For example, devices (such as remote I/O) not requiring a high speed communication cycle can be connected while still maintaining the performance of devices requiring high performance communication cycles (such as servo amplifiers). This can also maximize the potential of slave devices on the network and improve productivity throughout the entire system.
possible for both master and slave devices. In all cases, 100 Mbit and 1 Gbit physical layers are supported.

Device development vendors, given these options for implementation (hardware or software) and communication speed (100 Mbps or 1 Gbps), can use the best development method for devices compatible with CC-Link IE TSN. This will also benefit users by rapidly expanding the range of compatible devices.

USE CASES
General-purpose IP communication devices and high performance motion control.

In such a system, a servomotor is momentarily stopped during alignment operation, and then a work piece position accurately measured by vision. A servo amplifier and vision sensor compatible with CC-Link IE TSN could be used at this point to allow time synchronization, which would enable the vision sensor to accurately determine the position of the work piece while being moved by the servo motor. This could significantly improve cycle time and reduce wiring.

The large volume of image data from the vision sensor can be transmitted via IP communication, allowing construction of a single network system with reduced wiring and yet with no impact on servo control performance.

FUTURE DEVELOPMENTS
The CC-Link IE TSN specification uses TSN technology to enable time sharing communication over Ethernet, making it easy to use Ethernet devices. The protocol has also been redesigned for high-speed cyclic communication, significantly improving performance and function for general control and motion control in the OT field.

Development will continue with the goal of further expanding the fields in which it can be used as follows:

- CC-Link IE safety communication function support development to address applications requiring safety communication
- Optical cable support for applications requiring long distances or high noise resistance

We also plan to acquire international standards, such as IEC61784 (which has already been obtained for CCLinkIE), the SEMI semiconductor/FPD industry international standard, and national standards in countries such as China and South Korea.

We will also work toward the use of TSN technology to enhance interconnectivity with other industrial open networks, to make the best use of data through overall connection.

This will allow CC-Link IE TSN to expand into more fields and grow as an industrial open network, serving as the foundation for “intelligent factories” that aim at autonomous, optimized manufacturing.
Meet the smallest Industrial PC from Beckhoff.

The ultra-compact C6015 IPC for automation and IoT.

www.beckhoff.us/C6015

With the ultra-compact C6015 Industrial PC, Beckhoff has again expanded the application possibilities of PC-based control. Wherever space or cost limitations previously prevented the use of a PC-based control solution, this new IPC generation offers an excellent price-to-performance ratio in an extremely compact housing. With up to 4 CPU cores, low weight and unprecedented installation flexibility, the C6015 is universally applicable in automation, visualization and communication tasks. It is also ideal for use as an IoT gateway.

- Processor: Intel® Atom™, 1, 2 or 4 cores
- Interfaces: 2 Ethernet, 1 DisplayPort, 2 USB
- Main memory: up to 4 GB DDR3L RAM
- Housing: Die-cast aluminum-zinc alloy
- Dimensions (W x H x D): 82 x 82 x 40 mm

Flexible installation via rear or side panel mounting, or on DIN rail.
New Bluetooth spec gives the IoT a sense of direction

The recently released Bluetooth 5.1 specification builds in an efficient way of zeroing in on the location of BLE transmitters and receivers.

**MARK DE CLERCQ**
**DIALOG SEMICONDUCTOR**

**The newest version** of the Bluetooth communication standard emerged in January. The most noteworthy feature of Bluetooth 5.1 is an efficient way of discerning the direction of Bluetooth transmitters and receivers. The spec also introduces other advances aimed at speeding communications and boosting energy efficiency.

Makers of Bluetooth ICs have already released hardware that bakes in the features of the new 5.0 spec. Here’s a rundown of the changes Bluetooth 5.1 brings to the table, along with an example of how one supplier has begun applying it.

**WHERE IS IT?**
Bluetooth receivers have used signal strength to estimate distances to Bluetooth transmitters. The 5.1 spec provides two methods for more precise means of pinpointing locations, at the expense of using multiple transmit/receive antennae. To implement the Angle of Arrival (AoA) method, the receiver must have at least two antennae (at a minimum spacing of 6.2 cm) while the transmitter can have one. With AoA, the receiver uses its multiple received signals to deduce the angle of the source. Similarly, the Angle of Departure (AoD) method requires a transmitter with at least two antennae. The receiving device, which can have a single antenna, picks up multiple signals and from them derives the angle of the source.

**Direction finding in Bluetooth 5.1**

In the angle of arrival (AoA) method implemented in Bluetooth 5.1, a device such as a tag in a real-time locating system (RTLS) transmits a signal from a single antenna. The receiver contains multiple antennas arranged so the receiver sees a phase difference because of the difference in distance from each receiving antenna to the transmitting antenna. In the angle of departure (AoD) method, a device such as a Bluetooth locator beacon transmits a signal via an antenna array. The receiving device, such as a smartphone, uses a single antenna to pick up the signals that are decoded to calculate relative signal direction. This method of direction finding is intended for use in indoor positioning systems such as those for wayfinding.
One point to note: The range of devices following the 5.1 spec is the same as those of earlier versions. But the accuracy of locating Bluetooth sources using just signal strength falls off severely when obstacles are in the line of sight. The ability to triangulate will likely usher in capabilities such as real-time locating systems and indoor positioning systems.

The direction-finding features use in-phase and quadrature (IQ) sampling to measure the phase of RF that an antenna receives. In AoA, the sampling process is applied to each antenna in the array, one at a time, and in a sequence set by the design of the array. Sampled data is passed up the Bluetooth protocol stack via the Host Controller Interface (HCI) where an algorithm calculates the direction of one device from the other.

Certain parts of the Bluetooth protocol changed to support IQ sampling and the use of IQ samples by higher layers in the stack. The details get to be a bit complicated. For example, at the link layer, there’s a new field called the Constant Tone Extension (CTE) that provides a constant frequency and wavelength signal material against which IQ sampling can be performed.

Visible here is a development board from Dialog Semiconductor configured as a Bluetooth receiver that detects the angle of arrival (AoA) of a Bluetooth transmitter. This particular device is set to measure the angle to the transmitter ten times/sec and display the angle on the LCD.

The SmartBond DA1469x family of Bluetooth controllers from Dialog Semiconductor implements Angle of Arrival and Angle of Departure features of the Bluetooth 5.1 standard. The devices also contain a Sensor Node Controller (SNC) that runs autonomously and independently processes data from sensors connected to its interfaces. Additionally, the DA1469x family has a built-in Power Management Unit that only activates the processing cores on the chip as needed, while also eliminating the need for a separate PMIC.
Bluetooth 5.1 controllers may be designed to work with an external RF switch that is used to make connections to multiple antennas for AoA and AoD functions. An example of such a switch is the HMC7992, a silicon SP4T switch from Analog Devices that is rated for signals of up to 6 GHz.

The 5.1 spec also makes some enhancements to GATT, the Generic Attribute Profile, which defines the way two BLE devices transfer data back and forth using concepts called services and characteristics. The enhancements are generally in the interest of better energy efficiency and faster handshaking between Bluetooth devices. But some of them are in preparation for future enhancements in the works for upcoming spec releases.

Fundamentally, the 5.1 spec defines how BLE clients can skip service discovery on devices where nothing has changed since the last time the two devices communicated. A client may now deduce that a device to which it is connecting is the same type as a previous connection and with an attribute table the client has already cached. If certain details are the same, the client may decide skip parts of the connection protocol because it already has the data it needs.

The classic example of where this might come in handy is that of Bluetooth smart locks, where a smartphone opens the door as its owner approaches. Service discovery need only take place the first time the user opens the smart lock. The user may notice a delay in the door unlocking on the first time through, but from then on, they will experience a near instantaneous response.

**ADVANCED ARCHITECTURES**

The new features that Bluetooth 5.1 incorporates put an additional computational load on Bluetooth controllers. Certain architectural features come in handy when handling the extra work. For example, the process of triangulation can employ sophisticated algorithms. So architectural features that include digital signal processing and a large memory are helpful.

Additionally, because triangulation involves signals from multiple antennas, Bluetooth controllers must incorporate a means of handling the multiple RF signals involved. Because the market for single-antenna Bluetooth remains large, controllers implementing the 5.1 standard may handle the need for multiple RF paths by including architectural features for rapidly manipulating an external RF switch, rather than including the switch on the Bluetooth controller IC itself.
AoA and AoD features in Bluetooth 5.1 are aimed at bringing more precision to real-time locating systems (RTLS) and indoor positioning systems (IPS). Bluetooth RTLS setups for asset tracking employ Bluetooth receivers, often called locators, in fixed locations throughout a facility. The locators connect to a centralized server dubbed a location engine. Bluetooth transmitters commonly called tags are attached to entries the system is tracking. The tags periodically transmit a signal to the location engine which estimates the position of each locator. In an IPS, Bluetooth transmitters referred to as locator beacons reside in fixed locations. Visitors typically use an app on a smartphone to listen for locator beacons. The app uses received signal strength to calculate its real-time position.

An example of such a Bluetooth 5.1 controller chip family is the Dialog SmartBond DA1469x family. It is the first wireless multi-core MCU in production based on the ARM Cortex M33 processor. This processor features digital signal processing and floating-point capabilities that aid in triangulation computations. Additionally, these processors have I/O that let them control an external RF switch with a high degree of precision for the purpose of implementing AoA and AoD location. Handling AoA and AoD with an external RF switch, rather than a switch integrated on the Bluetooth chip, keeps down costs of single-antenna Bluetooth apps.

Additionally, the memories on DA1469x devices are expandable, useful for handling complex applications while keeping costs down for more basic uses. Because it is often advantageous to limit power dissipation in Bluetooth applications, DA1469x chips incorporate a power management function wherein sections of the chip are only active when needed. For example, the chip would power up only the portion of the circuit handling the radio and simple Bluetooth functions when applications don’t involve direction finding. The full Cortex M33 processor would come to life for tasks demanding AoA or AoD.

Another point to note about DA1469x chips is that AoA and AoD functions are available to programmers via APIs. This eliminates the need for detailed knowledge of how to handle raw AoA/AoD data.

There are several other features on DA1469x ICs that don’t specifically relate to AoA/AoD functions, but which are useful for modern IoT needs. These features include a haptic feedback driver, a step motor driver (aimed at handling analog clock movements in hybrid analog/digital clocks), an LCD driver, a high-accuracy ADC for reading sensors, and other specialized analog blocks. Finally, some versions of the IC include built-in charging facilities for lithium-ion and lithium-polymer batteries.

All in all, Bluetooth 5.1 ushers in a number of functions that will better track both people and objects while adding to the user experience.

REFERENCES:
IoT crossroads: Design, manufacturing, and supply chains will converge

Here are several key ways manufacturers can control and improve new product development and introduction processes in the age of IoT.

SCOTT REEDY
SENIOR DIRECTOR OF MARKETING
ARENA SOLUTIONS

The numbers tell the story: global technology spending on the IoT is expected to reach $1.2 trillion in 2022, and IoT devices and services will reach an inflection point of 18% to 20% adoption in 2019. The combination of artificial intelligence (AI), machine learning, and real-time data streams delivered by IoT sensors and networks are going to make IoT business cases extremely compelling in 2019.

Today, IoT capabilities are included in handheld devices, household appliances, and medical implants to monitor patients, to name just a few. The auto industry is all in: enabling greater connectivity in cars to seamlessly gather, monitor, and share data with smart city services and other vehicles. So it’s no surprise that electronics suppliers are racing to deliver more value to support consumer electronics and cars.

Indeed, one might say the manufacturing world has become obsessed with the global network of connected devices and people. Rightfully so, as these performance insights can greatly improve the way we manufacture products.

Consumer electronics manufacturers continue to introduce IoT capabilities because they provide critical knowledge that helps save money, improve product quality by tracking equipment performance, and ultimately satisfies consumers’ growing appetite to connect anytime and anywhere. But these improvements introduce complexity and risks to operations and the overall supply chain as distributed teams struggle to manage terabytes, or even petabytes, of data across multiple systems and platforms. There’s also a growing list of concerns surrounding consumer privacy as companies find new ways to tap into consumer behavior—with and without their knowledge.

IoT, along with increasing regulations and globalization of teams and partners, is changing the landscape of new product development and introduction (NPDI). Product innovators are forced to contend with a deluge of data as they struggle to effectively coordinate dispersed teams to design, validate, and build new products on ever-tighter schedules and budgets.

With greater complexity, we expect to see an increased risk of product quality issues and product launch failures. Manufacturers must seek better ways to manage their design processes, improve the customer experience, and reduce quality defects.

As devices become more connected and complex, both quality and software issues are more prevalent. As a case in point, more than 20% of recalls in Q3 of 2018 were caused by software.
At the same time, original equipment manufacturers (OEMs) and original design manufacturers (ODMs) are constantly improving the way their products integrate with a wide array of IoT protocols (e.g., JSON-LD, Wi-Fi, IPv4/IPv6, Bluetooth) and devices. Many consumer and industrial products are already equipped with wireless technologies that serve as IoT gateways to collect information from products in the field or identify design and quality weaknesses.

IoT-enabled devices generate vast amounts of data for NPDI teams to sort through, analyze, and leverage. With this new IoT paradigm, multidisciplinary design and development-team collaboration early and throughout the entire product lifecycle is essential to product launch success.

- Ideally, contributors will be connected and synchronized to the point where:
  - The entire product team can work on the same version of the product.
  - Each discipline is synchronized with the others wherever they interface.
  - Everyone can see the project details, milestones, and deliverables that lead to an on-time launch.
  - The product is designed from the ground up to meet regulatory requirements.
  - Tests are run at every phase to ensure interoperability and manufacturability.

Here are several key ways manufacturers can control and improve NPDI processes in the age of IoT.

**COLLABORATE AROUND THE ENTIRE PRODUCT RECORD**

Design teams continue to use a multitude of electrical, mechanical, and software design tools to manage aspects of complex products. But the advent of IoT has tremendously increased the amount of software included in products, increasing the need for interdisciplinary cooperation.

**COLLABORATE TRANSPARENTLY BETWEEN MECHANICAL, ELECTRICAL, AND SOFTWARE DESIGNS**

Spreadsheets and CAD-centric PLM systems only help OEMs or ODMs manage a portion of the product record and BOM. For example, spreadsheets fail to provide relational connections to associated components, change orders, quality processes, and project information, making it harder to control as more people are added to the review process. Otherwise, product design flaws could go unnoticed until later in the development cycle, increasing costs, delaying product launches, and introducing the type of quality issues that lead to recalls.

Whether companies create and manage BOMs in product lifecycle management (PLM) software solutions, spreadsheets, or even document-centric tools, they need a controlled way to manage a hierarchical, relational BOM. Upstream computer-aided design (CAD) systems also need a way to quickly pass the entire BOM directly to the design or PLM system to eliminate errors and delays.

Additionally, upon release of the final design, the design or PLM system should be able to automatically pass the entire BOM with components, approved manufacturers, and suppliers to the enterprise resource planning (ERP) system to speed planning and production.

Whenever a specification is changed for any component in a complex device, it’s critical the entire team knows which other parts, procedures, and manufacturing processes are affected. With a comprehensive BOM management solution like a PLM, the team can move quickly from requirements to design specification changes to product team approvals using automated routings.

With added IoT design complexity, the best way to manage the entire BOM, from the final assembly down to the lowest level component, is by managing all aspects of the design and associated drawings, specifications, and files in a single system. The system must be easy for all parties to use and understand to support cross-functional collaboration with engineering, purchasing, manufacturing, and less technical supply chain partners like machine shops.
Fotofab has over 50 years experience in photochemical etching.

We are focused on delivering high quality parts, with tolerances that exceed the demands of our customers. We offer print-to-prototype parts in 1 day and custom design assistance.

We do what we say and honor what we said.

Common Parts:
- EMI/RF Shields
- Optical Encoders
- Electrical Contacts
- Filters & Screens
  and much more!

Request a Quote for your custom parts!

Visit us at www.fotofab.com

Now AS9100D Certified!

Fotofab has over 50 years experience in photochemical etching.

CAD-centric PLM solutions typically focus on a single aspect of the design like mechanical CAD and are not designed to manage software and electrical designs such as printed circuit boards (PCBs). They also lack access by all impacted teams outside of engineering and are not equipped to pass the complete product design to ERP systems at the point of release.

In contrast, today’s product-centric, cloud-based PLM solutions easily aggregate product information, BOMs, and relevant files from mechanical, electrical, and software design tools. Engineering teams can develop native design in CAD and PDM, then transfer information on parts, BOMs, and viewable design files into the PLM system when it’s time to review the design with the rest of the product team. Once the product is approved, simple interfaces make downloading all relevant information to the ERP fast and easy.

LOOK AHEAD: LEVERAGING IOT FOR CONTINUOUS PRODUCT DESIGN IMPROVEMENT

The untapped potential of IoT is still unfolding. Although information shared with connected devices can produce meaningful insights during production and customer use, it has yet to be fully leveraged to automate continuous product design improvement.

Since there’s a direct correlation between product design and quality, it will also be critical for manufacturers and supply chains to collaborate in a single system with highly controlled, traceable processes and design history.

Although the advantages and potential dangers around IoT will continue to evolve, one thing is certain—the ability to effectively manage these complex product development processes will determine which manufacturers succeed and which flounder in their efforts to get high-quality products to market ahead of the competition.

Arena Solutions
www.arenasolutions.com

SOURCES:
1https://www.iotforall.com/6-key-iot-trends-and-predictions-for-2019/
Automation & Control Freak?

Same here.

... We carry more automation & control brand names than any other distributor in North America.

It’s true – we checked.
Less bullet-proof than you think:
Gauging security hazards on the IoT

Engineers developing products for the IoT need to plan security measures that grow more sophisticated over time to thwart attackers who get better at wreaking havoc.

Skepticism about Internet of Things (IoT) security seems to be high. Ironically, for many industries the key to not being hacked is simply to not have the worst security. But many people are understandably concerned about hacks of the simple devices on which our everyday lives depend, and security researchers are calling IoT a catastrophe waiting to happen.

Today’s IoT security resembles that of quantum cryptography. Often referred to as quantum key distribution, this elegant technology is unlike other key distribution schemes. Most key distribution schemes rely on assumptions about the computational complexity of factoring large numbers or the discrete logarithm problem. In contrast, quantum keys promise unconditional security based on the laws of physics.

Quantum cryptography is theoretically unbreakable, but a few weaknesses emerged in practice. Interestingly, no loopholes were discovered until a dedicated team was established to break into them. This experience brings several lessons about security. First, the hacking of quantum cryptography showed the importance of upgradable security. When the successful penetrations, called blinding attacks, were discovered, system vendors were given a grace period to patch the vulnerabilities. It turned out that the vulnerabilities could be closed via software updates. The lesson is that systems must include a means of upgrading security over their lifetime.
Additionally, there are always assumptions about the kind of potential adversaries security systems can defeat. Systems do not have binary security: they are not secure or insecure. The question one must ask is, Secure against what? The reality is that there are different levels of security, and a device can only be considered secure where the level of security exceeds the capabilities of a particular attacker.

Typically, the cost of security grows with the sophistication of the potential attackers. It is true that sophisticated attackers often go after more than just the compromised product itself. Business processes, physical security, and people all may be in jeopardy.

Attackers often become more capable over time, so security measures must improve as well. Hackers can discover vulnerabilities and publicize them, and hacking tools tend to spread.

In 1977, the data encryption standard (DES) algorithm was established as a standard symmetric cipher. DES used a 56-bit key size. Increases in available computational power made the cipher vulnerable to brute-force attacks, and a demonstration in 1997 revealed DES could be cracked in 56 hours. Since the early 2000s, even hobbyists on PCs have been able to break DES. With DES clearly broken, triple DES became the next standard secure symmetric cipher. Triple DES is basically running DES three times with different keys.

The advanced encryption standard (AES) has replaced DES. But even AES does not guarantee security. Though the algorithm cannot be easily broken, the implementation can be hacked in a manner analogous to what happened with quantum cryptography.

Differential power analysis (DPA) attacks are made by measuring the power consumption or the electromagnetic radiation of the circuit performing the cryptography. This side-channel data is then used to obtain the cryptographic keys. Specifically, DPA involves capturing a large number of power consumption traces followed by analysis to reveal the key.

DPA was introduced in 1998. Since then, companies like Cryptographic Research Inc. (now Rambus) have sold DPA attack tools, though at prices out of reach for most hobbyists and researchers. But today, hardware tools for advanced DPA attacks go for less than $300, and advanced post-processing algorithms are available free online. Thus, the ability to conduct DPA attacks has migrated from nation-states and wealthy adversaries to nearly any hacker.

Consider these events in the context of IoT-device longevity. A typical device for the industrial IoT might last 20 years. What will a potential adversary look like in 2040? One might speculate whether it will even be human.

Now consider three example IoT applications: smart home door locks, smart home environmental sensors, and life-supporting medical devices.

A smart home door lock primarily controls the perimeter of the home. The homeowner can often remotely unlock the door through a smartphone app.

It doesn’t make sense to consider nation-state attackers in the context of attacking door locks. The more likely adversaries are security researchers and advanced hackers. Advanced hackers could compromise the door to rob houses without leaving a trace. An interesting aspect of this scenario is that occupants may only belatedly realize they’ve been robbed, as has already happened in some cases.

Security researchers often publish IoT security horror stories that make end users uncomfortable with a connected door lock. The resulting hysteria has an interesting consequence: The security solution must withstand public and media scrutiny even in the face of reasonable tradeoffs. In other words, connected devices must incorporate a higher security level than what is strictly necessary.

There are other interesting considerations for smart home environmental sensors. In the broadest sense, environmental data could be used to control actuators in systems such as HVAC.

Security upgrades are necessary to let the product evolve as attackers become more sophisticated over time. A high level of security and hardware primitives (such as extra memory) maximize the likelihood that security issues can be patched in the future.
manipulation of seemingly innocuous sensor data can have a big impact. For example, suppose a triggered fire alarm automatically opens a door lock.

It can be hard to imagine up-front the impact of large-scale sensor attacks. The best practice is to assume sensor data is as sensitive as any function it controls.

In smart-home devices, two particularly interesting challenges come up: commissioning and longevity. The install process directly impacts ease-of-use. Product developers have historically made many tradeoffs between security and usability with some such tradeoffs only identified after the product is in service. The fact that smart-home devices can remain installed for decades is an argument for giving them much higher security than may seem warranted the day they go into service.

The longevity of smart-home devices raises the question of backwards compatibility. Consumers want assurances of future support and may become upset if support is suddenly removed. The best strategy is to provide a means of upgrading to the latest security protocols in the field. But this may not always be possible. Hardware constraints may prevent it – upgraded protocols may demand hardware capabilities beyond what was available at the time of the product release.

Medical device security is particularly interesting. From a safety perspective, medical devices demand strict testing and processes. But their security requirements may have been minimal. Moreover, this class of devices has already seen a number of hacks.

Nation state security may be the right adversary class for a medical device. One reason: The potential is there for hacking these devices as an untraceable way of assassinating important individuals. What is certain is that the security of these devices will be subject to standards and certifications that will, hopefully, take such risks into account.

**REGULATORY AND STANDARDS INITIATIVES**
The regulatory and standards initiatives around IoT security are too extensive to cover here, but a two key elements must be mentioned: incentive and scalability.

Vendors have conflicting interests and may have incentives to reduce device security below what is a reasonable level for society. So security regulations must incorporate ways to incentivize without thwarting innovation. A point to note is the approach taken by GDPR, the General Data Protection Regulation now enforced by the EU. GDPR fines companies that lose valuable data serves as an incentive without limiting how the companies secure their data. This approach can serve as an inspiration for IoT security regulations.

For the foreseeable future, there will not be enough security engineers in the world to secure IoT devices. Thus any IoT security scheme must be scalable. Scalability is one of the key promises of the Platform Security Architecture (PSA) from Arm.

The PSA solves the problem of scalability through a balanced certification scheme and use of off-the-shelf secure components. This approach should make it possible for those without extensive security backgrounds to evaluate vendors based on certifications and to implement secure solutions using the components. The biggest challenge for PSA is its ties to an IP-vendor. As such, it is unlikely to be acceptable for broad standardization, even if it implements a good strategy for scalability.

In all, different types of IoT devices and applications require different levels of security. The types of adversaries and the longevity of the deployed product or system can determine the appropriate security level for a given IoT application. Ultimately, security certification schemes like Arm PSA and industrywide standardization will help secure IoT devices from attacks in the longer term.

**REFERENCES:**
Silicon Labs, www.silabs.com
Discover Over a Million
Engineering Products
from Suppliers You Know and Trust

- 900+ new products added each week
- Custom services such as kitting, panel meters, enclosures, and many more!
- Market-leading online community of over 500,000 engineers
Enabling embedded devices for the IoT

Automated onboarding and security features now help speed the integration of embedded devices into IoT systems.

ARVIND RAGHURAMAN
MENTOR GRAPHICS
A SIEMENS COMPANY

As the internet of things has evolved it has also grown more complicated. There are myriad choices when it comes to choosing the right cloud platform, cloud apps, device run-time components, communication protocols and topology, and security architecture.

Consider a typical IoT system topology in use today. It includes the cloud which could be running several hosted applications. These applications subscribe to data pushed by IoT devices, process that data, and present it to users in a meaningful fashion. The IoT devices could be categorized under one of two generalized form factors: gateways, and end nodes.

A typical IoT system topology in use includes the cloud running several hosted applications. These applications subscribe to data pushed by IoT devices, process that data, and present it to users.

Life cycle of an IoT-enabled embedded device
End nodes are leaves in an IoT topology. They typically connect and push data to a cloud or gateway-type back-end. Gateways typically serve as data aggregation points that provide first level processing for data from end nodes. Gateways usually implement localized analytics or other filtering functions that process dense incoming information from end nodes. After first-level processing, gateways push processed data to the cloud.

Let’s go over considerations a system designer should take into account to enable an embedded device to participate in a secure IoT system architecture. We’ll start with device onboarding. This can be discussed under two heads; cloud/gateway, and device side infrastructure.

Cloud platforms typically host device management applications that provide users the interfaces and workflows needed for creation and management of device identities. When a device identity is created, associated device security credentials are generated. Public key based asymmetric authentication schemes are typically used to enable device authentication workflows. The generated security credentials and other important metadata (including the URL of the device management/rendezvous server back-end the device should connect to for onboarding) should be provisioned to the device by the user.

On the device side, on power-up, the device should check the integrity and origin of software being booted on the device. Secure boot architecture is an important consideration to protect devices from rooting-type attacks. The device’s system design should consider inclusion of tamper-proof secure storage and associated software APIs to access and manage secure storage. Secure storage is typically needed to store security keys for device onboarding and secure boot, and other sensitive device specific secrets. Once device software is successfully booted, a device application would typically present the user provisioned credentials to a back-end device management application. The back-end could be running on the cloud or on a gateway type device. The back-end app would authenticate the device identity and securely onboard the device.

**Secure On-boarding**
- Create device identity on back-end
- Device Provisioning - manual, or client initiate (bootstrap server)
- Secure boot - verified boot of device software

**Configure, Monitor, & Control**
- Configure, Monitor: read and write to variables
- Control: Execute methods and commands: reboot, factory reset, etc

**Secure Telemetry**
- Transmit device data to back-end
- Receive asynchronous data, alarms and event notifications

**Software Update and Maintenance**
- Receive and validate firmware, apps, and data
- Apply SW update
- Firmware rollback capability
- Report firmware health

---

Device discovery and profiling are functions that can be automated via tools such as the Mentor Embedded IoT (MEI) Framework.
Next, let's consider device communications with the backend. With the device securely on-boarded, device applications must create a secure communication channel between the device and the back-end. Depending on the protocol used, the communication session is typically secured using symmetric encryption schemes. Once secure communication is established, the device can push data to and receive asynchronous data from the back-end.

To formalize communications between the device and backend, data models are often employed. Once secure communications are established, a data model is established between the device and the backend. This model can be provisioned by the back-end to the device or instantiated and exposed by the device to the back-end.

The data model typically consists of device-specific parameters, methods and commands. Using the data model, back-end apps can subscribe to device data and engage device services. For example, a back-end application could subscribe and plot a temperature parameter exposed by the device; it could invoke an update method to trigger a software update, and on completion it could issue a reboot command to boot new firmware on the device. Data flowing from the back-end to the device could also include asynchronous messages signaling alarm conditions or event notifications which the device would process and act on.

Finally, let's consider device maintenance. A secure infrastructure for creation and delivery of software updates targeted at the device operating system, or at application software and data, is an essential element for IoT device maintenance and security. Most use-cases require privacy, integrity, and authenticity attributes of update artifacts be assured before update artifacts could be consumed by devices. A comprehensive software update infrastructure should include: tooling for encryption and digital signing of update artifacts, a cloud or on-premises-based infrastructure to deliver updates at scale to the device fleet, and device run-time software to receive, authenticate, and implement the update.

On the device side, suitable mechanisms should be present to enable software run-time to assess health of updated software. In case of improper or incomplete updates, device firmware should have the ability to revert the device software stack to a previously known working version.

For devices that are capable of running a GPOS like Linux, application development, deployment, and migration using container-based approaches are becoming widely used. A container-based approach for application management provides several benefits; portability, ease of migration, scalability, standardization, continuous integration (CI) and delivery (CD) flows, application life cycle management, health monitoring, and availability of a rich open-source eco-system of run-time software and tools for management and orchestration of containerized applications, to name a few.

Under the umbrella of device maintenance, health monitoring is another important topic. Device run-time software should expose OS and application specific health parameters to the backend. The device data model could include system health information. Health monitoring applications in the backend would leverage...
this information to present device health information to users.

Obviously, the process of commissioning and securing IoT devices can be quite involved. So device software frameworks have emerged to help manage the process. An example is the Mentor Embedded IoT (MEI) Framework. It is a collection of software components which compiles into a library. The library comes with a device agent which can be incorporated into the device runtime to start up on device boot. The framework library allows devices to readily onboard and establish communications with widely used cloud platforms that include AWS, Azure, and Siemens’ MindSphere (coming soon).

Incorporating the Mentor Embedded IoT (MEI) Framework library into an IoT device gives the device IoT connectivity. In a typical scenario, a gateway could be running Linux and within it, the MEI will appear like a library with a resident agent which boots up on device boot. The agent would be provisioned with the device credentials. On boot up, it would present the credentials to the configured cloud back-end and onboard the device.

In addition to out-of-the-box operability with supported cloud platforms, the Mentor Embedded IoT Framework (MEIF) could be configured to enable device operability with several widely used open-source cloud applications that provide device management and monitoring functionality.

In a nutshell, MEIF Framework is a library and an agent with associated host-side tooling that can be integrated into a gateway or end-node-type device. The MEIF Framework enables an embedded device to readily onboard and communicate with supported cloud platforms. In addition, the library readily enables the device to operate with several open-source device management and monitoring applications that could be hosted on the cloud or on a local on-premises environment.

The MEIF Framework deployed on Mentor Embedded run-time operating systems, like Nucleus RTOS and Mentor Embedded Linux, provide out-of-the-box, comprehensive device-side software enablement to enable embedded devices for secure IoT connectivity, software updates, and device maintenance.

**REFERENCES:**

Mentor Graphics MEI, www.mentor.com
Battery self-discharge and designing for long life

Battery chemistries each have special qualities that can make certain cells impractical for varying kinds of internet-of-things applications.

Circuit designers often find themselves in the position of trying to squeeze as much life as possible out of a battery. Today there is much discussion about boosting battery life through use of low-power chipsets or more efficient communication protocols. But the potential savings available do not make up for the loss of operating life arising from battery self-discharge.

Long-life batteries help reduce the total cost of ownership by powering low-power devices maintenance-free for up to 40 years, demanding incredibly low battery self-discharge.

Until recently, high-current-pulse applications had to employ spiral-wound cells, resulting in greatly compromised performance. Combining a lithium-thionyl-chloride chemistry with a hermetically sealed hybrid layer capacitor (HLC), Tadiran Pulses Plus cells employ a bobbin type construction with advantages that include a high capacity, 19 Ah for a D size cell (versus 10 to 13 Ah with spiral wound) and a lower self-discharge rate, less than 2% per year (versus 5% per year with spiral wound cells).
LONG-LIFE LITHIUM BATTERIES

Many Industrial Internet of Things (IIoT) devices use two-way wireless communications. This wireless connectivity allows big-data analytics and artificial intelligence (AI) to enhance workflow, make people more productive, and companies more profitable. Remote wireless devices connected to the IIoT commonly require industrial-grade lithium batteries that deliver reliable, long-term power to remote locations and challenging environments.

A prime example is in the modern oil refinery, which is equipped with an average of 30,000 sensors, many of which are interoperable using the decades-old HART (Highway Addressable Remote Transducer) protocol. Unfortunately, the majority of HART-enabled devices were never fully integrated because the cost of hard-wiring is prohibitive, estimated at roughly $100/ft for any type of hard-wired device, even a basic electrical switch. And wiring costs can be much higher in remote locations and extreme environments. Fortunately, the development of the WirelessHART protocol has eliminated the costs associated with hard-wiring.

A remote wireless device drawing just microwatts of energy which must have a long operating life will likely be powered by an industrial-grade primary (non-rechargeable) lithium battery. Conversely, a device drawing average daily current in the milliamp range could deplete a primary battery quickly. Here, it may be better to employ some form of energy harvesting device combined with a lithium-ion (Li-ion) rechargeable battery able to store the harvested energy.

Remote industrial wireless applications are rarely powered by consumer-grade alkaline batteries. These cells suffer from high annual self-discharge rates that exhaust the cell capacity in a few years or less. Alkaline batteries also employ a water-based chemistry that is prone to freezing, making them ill-suited for extreme environments. Although inexpensive, consumer-grade alkaline batteries can make overall costs higher when the recurring expenses associated with replacing batteries are factored in.

Specially modified bobbin-type LiSOCl2 batteries can be adapted for use in the cold chain, where wireless sensors monitor the transport of frozen foods, pharmaceuticals, tissue samples, and transplant organs at temperatures as low as -80°C.

HOW TO CHOOSE AN INDUSTRIAL-GRADE BATTERY

The process of selecting an industrial-grade lithium battery starts with prioritizing the most important technical requirements including: the amount of current consumed in active mode (along with the size, duration, and frequency of pulses); energy consumed in stand-by or sleep mode (the base current); storage time (as normal self-discharge during storage diminishes capacity); expected temperatures (including during storage and in-field operation); equipment cut-off voltage (as battery capacity is exhausted, or in extreme temperatures, voltage can drop to a point too low for the sensor to operate); the annual self-discharge rate of the battery (which can approach the amount of current drawn from average daily use).

Key considerations include:

- **Reliability** – Is the remote wireless device going into an inaccessible spot where battery replacement is difficult or impossible and loss of data caused by battery failure is unacceptable?
- **Long operating life** – Does the self-discharge rate of the battery approach or exceed the average daily energy consumption? If so, the application calls for a high-capacity battery.
- **Miniaturization** – Batteries with high capacity and high energy density support a smaller footprint.
- **Extended temperatures** – Certain lithium battery chemistries can operate in extreme temperatures without a significant rise in their self-discharge rate.
- **Higher voltage** – Specifying batteries with higher voltage may enable the use of fewer cells.
- **Lifetime costs** – Determining your true cost of ownership must include all expenses related to future battery replacements, along with the risks associated with battery failure.

Lithium batteries are preferred for long-term deployments because of their high intrinsic negative potential, which exceeds that of all other metals. As the lightest non-gaseous metal, lithium offers the highest specific energy (energy per unit weight) and energy density (energy per unit volume) of all available battery chemistries. Lithium cells operate within a normal operating current voltage (OCV) range of 2.7 to 3.6 V.
The fact they contain no water also allows lithium batteries to endure extreme temperatures without freezing.

Numerous primary lithium chemistries are available including iron disulfate (LiFeS₂), lithium manganese dioxide (LiMnO₂), lithium thionyl chloride (LiSOCl₂), and lithium metal-oxide chemistry.

LiFeS₂ cells are relatively inexpensive and typically are deployed to deliver high pulses to power a camera flash. LiFeS₂ batteries have performance limitations that include a narrow temperature range (-20 to 60°C), a high annual self-discharge rate, and crimped seals that may leak.

LiMnO₂ cells, including the widely used CR123A, are commonly used to save space in cameras and toys, as one 3-V LiMnO₂ cell can replace two 1.5-V alkaline cells. LiMnO₂ batteries can deliver moderate pulses but have limitations such as low initial voltage, a narrow temperature range, a high self-discharge rate, and crimped seals.

LiSOCl₂ batteries can be constructed two ways: bobbin-type and spiral wound. Bobbin-type LiSOCl₂ batteries exhibit a low annual self-discharge and are thus preferred for long-term deployments that use low average daily current including AMR/AMI metering, M2M, SCADA, tank-level monitoring, asset tracking, environmental sensors, and extreme temperature applications.

Bobbin-type LiSOCl₂ batteries feature the highest capacity and highest energy density of any lithium cell, along with an extremely low annual self-discharge (under 1% per year for certain cells), thus permitting up to 40-year battery life for certain applications. Bobbin-type LiSOCl₂ batteries also deliver the widest possible temperature range (-80 to 125°C) and feature a superior quality glass-to-metal hermetic seal.

Some lithium batteries feature operation over extended temperature ranges. An example is the model TLH-2450 which is used in autoclavable RFID tags found in medical settings as well as in tire pressure monitoring systems.

Lithium batteries can have either a spiral-wound or bobbin-type construction. Bobbin-type LiSOCl₂ chemistry offers the highest capacity and highest energy density of any lithium cell, along with an extremely low annual self-discharge rate (less than 1% per year) but are generally reserved for lower-current applications because of their low electrode surface area compared to that of spiral-wound cells.
BATTERY SELF-DISCHARGE

Specially modified bobbin-type LiSOCl₂ batteries can be adapted for use in the cold chain, where wireless sensors monitor the transport of frozen foods, pharmaceuticals, tissue samples, and transplant organs at temperatures as low as -80°C. Bobbin-type LiSOCl₂ batteries can also handle extreme heat. For example, these cells have served in active RFID tags that track the location and status of medical equipment without having to remove the battery prior to autoclave sterilization, where temperatures can reach 125°C.

Be aware that the annual self-discharge rate of bobbin-type LiSOCl₂ batteries may vary significantly based on their method of manufacture and the quality of the raw materials. For example, a top-quality bobbin-type LiSOCl₂ cell can have an annual self-discharge rate as low as 0.7%, retaining over 70% of its original capacity after 40 years. By contrast, a lower quality bobbin-type LiSOCl₂ cell can have a self-discharge rate of up to 3% per year. While this difference may not seem overly significant, it really adds up. A lower-quality cell can lose up to 30% of its available capacity every 10 years, eliminating the possibility of a 40-year battery life.

The impact of a higher self-discharge rate may not become apparent for years, and theoretical test data can be highly misleading. Thorough due diligence is a must if the application demands long-life power, especially in extreme environments. Ask all potential battery suppliers to provide fully documented long-term test results and in-field performance data from similar applications, along with customer references.

For example, it pays to choose the cell with the lowest annual self-discharge rate when specifying a long-life bobbin-type LiSOCl₂ battery for meter transmitter units (MTUs) in AMR/AMI utility metering applications. Here, a large-scale battery failure can disrupt customer billing systems and disable remote service start-up and shut-off capabilities. The possibility of such wide-scale chaos could force a utility to prematurely invest millions of dollars to replace batteries early so as not to jeopardize data integrity.

HIGH PULSES
The IIoT includes numerous remote wireless devices that require periodic high pulses to power advanced two-way wireless communications. A standard bobbin-type LiSOCl₂ battery cannot deliver high pulses because of its low rate design, but it can easily be combined with a patented hybrid layer capacitor (HLC) to support such needs. The standard bobbin-type LiSOCl₂ cell delivers low daily background current while the HLC handles periodic high pulses. The patented HLC also features a special end-of-life voltage plateau that can be interpreted and programmed to deliver low-battery status alerts.

Many consumer electronic products employ supercapacitors which deliver high pulses electrostatically rather than chemically. Supercapacitors have inherent limitations that keep them out of industrial applications. These include their short-duration power, linear discharge qualities that prevent use of all the available energy, low capacity, low energy density, and high annual self-
discharge rates (up to 60% per year). Supercapacitors linked in series also require the use of cell-balancing circuits, which add to cost and bulkiness and consume energy to reduce their shelf-life.

High pulses invariably draw additional current, so intelligent energy management requires techniques such as using a low-power communications protocol (ZigBee, WirelessHART, LoRa, etc.), low-power microprocessors, and other techniques to minimize the amount of energy consumed during data interrogation and transmission.

A growing number of wireless IIoT applications are good candidates for combining energy harvesting devices with Li-ion rechargeable batteries, especially applications that draw enough average daily current (milliamps) that would quickly exhaust a primary lithium battery. One prime example is a solar-powered tracking device that continuously monitors the health of animal herds. Another example is a solar-powered parking meter that automates billing and fee collection while also identifying open parking spots to reduce pollution and traffic congestion.

Photovoltaic (PV) panels are the most proven form of industrial energy harvesting. Energy can also be harvested from equipment movement or vibration, temperature variances, and ambient RF/EM signals.

Consumer-grade rechargeable Li-ion cells may work if the device is easily accessible, needs an operating life of just five years and 500 recharge cycles, and operates within a moderate temperature range (0 - 40°C), with no high pulse requirements. However, industrial-grade rechargeable Li-ion batteries work best for long-term deployment in a remote location or extreme environments, and/or if high pulses are required.

Industrial grade Li-ion batteries can lower the cost of ownership by operating maintenance-free for up to 20 years and 5,000 full recharge cycles, with an expanded temperature range of -40 to 85°C, delivering the high pulses powering two-way wireless communications. These ruggedly constructed cells feature a hermetic seal that delivers superior safety protection not found in consumer-grade rechargeable Li-ion batteries.

### REFERENCES:

Tadiran Batteries, www.tadiranbatteries.com

<table>
<thead>
<tr>
<th>Industrial vs consumer (18650) lithium batteries</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLI-1550 (AA) Industrial Grade</td>
</tr>
<tr>
<td>Diameter (max) [cm]</td>
</tr>
<tr>
<td>Length (max) [cm]</td>
</tr>
<tr>
<td>Volume [cc]</td>
</tr>
<tr>
<td>Nominal Voltage [V]</td>
</tr>
<tr>
<td>Max Discharge Rate [C]</td>
</tr>
<tr>
<td>Max Continuous Discharge Current [A]</td>
</tr>
<tr>
<td>Capacity [mAh]</td>
</tr>
<tr>
<td>Energy Density [Wh/l]</td>
</tr>
<tr>
<td>Power [RT] [W/liter]</td>
</tr>
<tr>
<td>Power [-20C] [W/liter]</td>
</tr>
<tr>
<td>Operating Temp deg. C</td>
</tr>
<tr>
<td>Charging Temp deg. C</td>
</tr>
<tr>
<td>Self Discharge rate [%/Year]</td>
</tr>
<tr>
<td>Cycle Life [100% DOD]</td>
</tr>
<tr>
<td>Cycle Life [75% DOD]</td>
</tr>
<tr>
<td>Cycle Life [50% DOD]</td>
</tr>
<tr>
<td>Operating Life [Years]</td>
</tr>
</tbody>
</table>
Hidden pitfalls of IoT antenna design

It is easy for developers to get tripped up when cramming multiple antennas into the small spaces that characterize IoT applications.

Traditionally there has been a wall between industrial design and RF (radio frequency) engineering when companies develop products that have wireless capabilities. The process typically starts with product designers assembling a list of design requirements that determine the look, feel and function of the product. Only with the product development process well under way are RF engineers tasked with squeezing in wireless capabilities. Simply put, the wireless antenna and its performance can be afterthoughts.

The problem, of course, is that wireless products designed this way run the risk of underperforming and being impractical – perhaps forced to use off-the-shelf antennas inappropriate for the constrained location and proximity to perturbational materials. Stick-on antennas, for example, can be detuned by most plastics. Volume constraints introduced by prescribed industrial and mechanical designs often suggest the use of a “chip” antenna. However, many chip antennas require a printed circuit board (PCB) footprint and features that may not comply with the size constraints.

It is remarkable that many manufacturers don’t integrate the RF and industrial design teams to avoid making costly changes late in development. A well-integrated team can define early boundaries for the product that could simplify antenna design later. Moreover, designing the antenna and PCB layout without input or constraints from industrial designers can lead to missed opportunities for optimizing the shape, performance, size, cost, assembly, and desirability of the product.

For example, it may not occur to RF designers operating alone that it may be advantageous to integrate antennas right into the product housing, essentially creating a Molded Interconnect Device (MID) -- basically, an injection-molded plastic with integrated circuit traces. The MID can be an internal part or integrated into the exterior of the product. There are several ways to produce MIDs and some of them require less tooling than others.

This sort of design thinking takes a team of industrial designers and antenna designers who work side by side, simulating antenna patterns, building prototypes, and testing real physical prototypes. In this scenario, RF engineers make sure industrial designers know about limitations as well as spatial and material challenges for the chosen antennas. They can also factor in spatial and material limitations such as those imposed by adjacent ground and dielectric planes, human body interactions, and resistive loss characteristics of metallization materials and processes.

The Revie Flex is a flexible PCB antenna with a broad frequency range for LTE CAT M1 and NB-IoT devices.

RICH WALTERS • BRIAN PETTED
LAIRD CONNECTIVITY
ANTENNA DESIGN

Products ranging from smartphones to the PlayStation 4 all contain at least one antenna comprised of a printed circuit board trace. A trace antenna has several advantages. Good performance, virtually no additional cost, and small size for frequencies exceeding 900 MHz are some of the reasons trace antennas are popular.

There are several factors helpful to keep in mind when implementing a trace antenna. Standard printed or trace antenna designs that are widely used include various monopoles, dipoles, loops, notches, slots, and PIFAs (planar inverted-F antennas). Standard PIFA-type antennas are the most extensive and offer the best trade-off between size, efficiency, and are reasonably omni-directional. A meandering trace can be used to compact the PCB area, but at the cost of performance.

Of course, the PCB trace length determines the antenna resonant frequency. Each antenna requires a keep-out area around the antenna trace where no copper traces or ground fill can exist on any layer of the PCB. The trace can either be gold flashed or covered with solder mask. The antenna's electrical performance will be determined by the type of substrate material, its thickness, relative dielectric constant ($\varepsilon_R$), and metallization resistivity.

Most non-dipole PCB trace antennas must have an image ground plane to be effective. The shape and size of the ground plane relative to the antenna affects the antenna impedance and performance. The ground plane should have vias along the entire edge of the antenna keep-out area to connect ground planes in multi-layer designs.

A mismatched antenna can greatly reduce the total RF link budget and range due to mismatch losses, therefore the addition of a matching network at the antenna feed point is a best practice. Additionally, the final tuning and matching should take place in the actual product enclosure, not in open air. Maximum RF power transfers when the antenna impedance matches the source impedance (usually 50 $\Omega$). Ideally, a return loss below -9 dB or 2.0:1 voltage-standing-wave ratio (VSWR) is often taken as a figure of merit for a good antenna match, which translates to 12.6% of the incident power reflected due to mismatch. For band-edge frequencies, a degradation of return loss from -9 to -6 dB (25% reflection of incident power) is conventionally accepted.

Plastic enclosures, metal components, and the presence of other components close to the antenna all affect the antenna tuning and radiation pattern. Avoid placing the antenna close to metallic objects, nor enclose the antenna in a metallic or metallized plastic enclosure. Ideally, keep external influences in the antenna far field.
The FlexMIMO is the industry’s first flexible PIFA antenna for 802.11 Wi-Fi MIMO applications and contains two integrated 2.4/5-GHz dual-band antenna elements.

All PCB antennas are on the dimensioning of the lateral and vertical geometries of antenna element patterns as well as the electrical parameters that make up the structure of the specific design. This implies that the simple copying and translation of an existing design probably won’t work well without adjustments. Gain and radiation patterns will vary as the dimensioning and material properties in the surrounding areas change. The length of the antenna will typically require adjustment in response to these variations.

Diversity antenna array placements create a challenge in that one must place and orient independent antennas such that each antenna’s pattern does not couple to the same space as the other (patterns are not correlated to a common phase center). This is true for Selection Diversity (select antenna with best signal) as well as Multiple-Input-Multiple-Output (MIMO) antenna systems.

Typical methods of reducing antenna pattern correlation is to create space between the elements (up to a quarter wavelength) or to create an orthogonal (90°) relative orientation (or both). Compaction of these array placements requires close attention not to degrade the diversity gain performance of the system.

There exist dual-element sub-arrayed antennas to simplify the compaction and placement process. Examples include the world’s first flexible PIFA (planar inverted F antenna) for Wi-Fi MIMO applications (patent pending). The FlexPIFA MIMO is specifically designed for 802.11 a/b/g/n as well as 802.11ac Wi-Fi modules that use MIMO or Wi-Fi Diversity. The Laird FlexPIFA MIMO drastically simplifies the size, cost and technical requirements for implementing the two antennas necessary for 802.11 MIMO because the two integrated antenna elements are oriented and spaced in an optimum way for MIMO radio performance.

Some antennas are purposely designed to be placed in direct contact with particular packaging materials. These antennae usually are slot type, or post-loaded dipoles. An example of these types of antennae are the FlexNotch and Mini NanoBlade Flex. Another notable flexible antenna is the Revie Flex for use in LTE CAT M1 and NB-IoT devices. The antenna is optimized for mounting to plastic via a supplied adhesive backing. It operates within the 698 - 875 MHz and 1.71 – 2.5 GHz bands and is ground-plane independent.

CERTIFICATIONS AND COMPLIANCE

Radio regulatory certification is a critical step in every wireless product launch, but obtaining it isn’t always straightforward. Successful navigation of the FCC certification landscape is critical for getting to market quickly. Pre-scans are an effective way to reduce the risk of failing – basically, checking the product for emissions while still in development.

Unfortunately, many teams get to the final stage of development before thinking about regulatory testing. Products can fail regulatory certification on the first test attempt and in light of empirical experience, wireless products with embedded radios are even more likely to exceed regulatory limits, problematic because resolution of these failures typically requires last-minute hardware changes.

The integration of antennas within the packaging dictated by product form and function should be a team effort between RF engineering and Industrial-Mechanical design. Common considerations amongst the co-development team should be harmony with the industrial and mechanical design, while maintaining a firm observation of best-practices for antenna placement and implementation for radio performance and success of regulatory testing and compliance. This effort can be synthesized from raw materials and design know-how or can be implemented with off-the-shelf solutions that reduce design risk and cycle-time.

REFERENCES:

Laird Connectivity, www.lairdconnect.com
## AD INDEX
INTERNET OF THINGS HANDBOOK

<table>
<thead>
<tr>
<th>Allied Electronics</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anritsu</td>
<td>BC</td>
</tr>
<tr>
<td>Beckhoff Automation</td>
<td>23</td>
</tr>
<tr>
<td>Coilcraft</td>
<td>22</td>
</tr>
<tr>
<td>Digi-Key</td>
<td>IFC</td>
</tr>
<tr>
<td>Fotofab</td>
<td>30</td>
</tr>
<tr>
<td>Integrated Device Technology (IDT)</td>
<td>IBC</td>
</tr>
<tr>
<td>Keystone Electronics Corp.</td>
<td>1</td>
</tr>
<tr>
<td>Master Bond</td>
<td>26</td>
</tr>
<tr>
<td>Memory Protection Devices</td>
<td>3</td>
</tr>
<tr>
<td>Newark, An Avnet Company</td>
<td>35</td>
</tr>
<tr>
<td>Tadiran</td>
<td>9</td>
</tr>
</tbody>
</table>

### SALES

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jami Brownlee</td>
<td><a href="mailto:jbrownlee@wtwhmedia.com">jbrownlee@wtwhmedia.com</a></td>
<td>224.760.1055</td>
</tr>
<tr>
<td>Mike Caruso</td>
<td><a href="mailto:mcaruso@wtwhmedia.com">mcaruso@wtwhmedia.com</a></td>
<td>469.855.7344</td>
</tr>
<tr>
<td>Garrett Cona</td>
<td><a href="mailto:gcona@wtwhmedia.com">gcona@wtwhmedia.com</a></td>
<td>213.219.5663</td>
</tr>
<tr>
<td>Bill Crowley</td>
<td><a href="mailto:bcrowley@wtwhmedia.com">bcrowley@wtwhmedia.com</a></td>
<td>610.420.2433</td>
</tr>
<tr>
<td>Michael Ference</td>
<td><a href="mailto:mference@wtwhmedia.com">mference@wtwhmedia.com</a></td>
<td>408.769.1188</td>
</tr>
<tr>
<td>Mike Francesconi</td>
<td><a href="mailto:mfrancesconi@wtwhmedia.com">mfrancesconi@wtwhmedia.com</a></td>
<td>630.488.9029</td>
</tr>
<tr>
<td>David Geltman</td>
<td><a href="mailto:dgeltman@wtwhmedia.com">dgeltman@wtwhmedia.com</a></td>
<td>516.510.6514</td>
</tr>
<tr>
<td></td>
<td>@wtwh_david</td>
<td></td>
</tr>
<tr>
<td>Neel Gleason</td>
<td><a href="mailto:ngleason@wtwhmedia.com">ngleason@wtwhmedia.com</a></td>
<td>312.882.9867</td>
</tr>
<tr>
<td></td>
<td>@wtwh_ngleason</td>
<td></td>
</tr>
<tr>
<td>Jim Powers</td>
<td><a href="mailto:jpowers@wtwhmedia.com">jpowers@wtwhmedia.com</a></td>
<td>312.925.7793</td>
</tr>
<tr>
<td></td>
<td>@jpowers_media</td>
<td></td>
</tr>
<tr>
<td>Courtney Nagle</td>
<td><a href="mailto:cseel@wtwhmedia.com">cseel@wtwhmedia.com</a></td>
<td>440.523.1685</td>
</tr>
</tbody>
</table>

### LEADERSHIP TEAM

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike Emich</td>
<td><a href="mailto:memich@wtwhmedia.com">memich@wtwhmedia.com</a></td>
<td>508.446.1823</td>
</tr>
<tr>
<td></td>
<td>@wtwh_memich</td>
<td></td>
</tr>
<tr>
<td>Scott McCafferty</td>
<td><a href="mailto:smccafferty@wtwhmedia.com">smccafferty@wtwhmedia.com</a></td>
<td>310.279.3844</td>
</tr>
<tr>
<td></td>
<td>@SMMcCafferty</td>
<td></td>
</tr>
<tr>
<td>Marshall Matheson</td>
<td><a href="mailto:mmatheson@wtwhmedia.com">mmatheson@wtwhmedia.com</a></td>
<td>805.895.3609</td>
</tr>
<tr>
<td></td>
<td>@mmatheson</td>
<td></td>
</tr>
</tbody>
</table>
SDAWIR03 Sensor Connectivity Kit

Enables easier design of complex IoT solutions and applications

- Offers real-time sensor data collection that integrates into sensor management services hosted on the AWS cloud
- Firmware has no license fee and no royalties
- Supports Over-The-Air updates

Learn more at idt.com/sdawir
Anritsu’s IoT test and measurement solutions help bring high-quality, leading edge mobile broadband and IoT technologies to market confidently and quickly.

ASSURING QUALITY CONNECTIONS FOR IoT

WIRELESS LAN | BLUETOOTH | CELLULAR

www.anritsu.com

© 2019 Anritsu Company