WHITE PAPER

New Dawn for x86 Computers in the Industrial Internet of Things

Edison Huang
Moxa Product Manager

MOXA®

Preface: The industrial Internet of Things

The Internet of Things (IoT) has the potential to reduce costs, improve flexibility and open new markets—so it is no surprise that interest in the IoT concept is growing around the world. The IoT spirit is for all devices to be connected together—coordinated by centralized management, uploading data to a control center, and analyzing that data to derive new value from it. These concepts have obvious applications to the world of industrial automation, where there are huge opportunities for improvements in efficiency, safety, and operating and maintenance costs—if only the numerous hardware controllers, sensors, and other devices could communicate and coordinate intelligently with each other and staff, instead of working in isolation. Industrial users are eagerly studying the IoT to see how they can benefit from it.

Traditionally, industrial automation has focused mainly on the accuracy and sensitivity of control. Unlike modern systems, there was usually relatively little emphasis on data acquisition, data analysis, and communication between devices. As a result, simpler hardware, such as programmable logic controllers (PLC), comprises a large proportion of deployed industrial automation equipment. However, as today's manufacturers look for new ways to make their factories work smarter and cheaper, there is a shift towards remote data acquisition and management, and this trend is making communication just as important as control for industrial automation. Manufacturers are looking for ways to bring the IoT to industry, and we are witnessing the birth of the Industrial Internet of Things.

However, building the Industrial Internet of Things poses some real challenges for hardware developers and systems integrators. These challenges include: limited space inside cabinets, high temperatures that can disable critical components, the huge cost of connecting all those IoT devices together, interoperability with legacy devices, and a torrent of raw data that can clog up networks and overload processors.

Released on October 16, 2015

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

New demand from industrial automation and Industry 4.0

Industry 4.0 can broadly be described as "digitally connected manufacturing." It represents a next generation of industry that takes full advantage of new technologies and concepts, such as the Industrial IoT and the Industrial Internet of Services (IIoS). This trend reflects the growing importance of communications as a key enabler of more powerful forms of industrial automation. Together, these technologies and services make new kinds of smarter factories possible, and they are more efficient, more flexible, and more cost-effective than traditional manufacturing facilities.

We can categorize industrial automation into two classes: the traditional systems that originated from proprietary hardware, and the newer Information Technology-based systems that make much more use of general-purpose computer hardware, such as industrial PCs (IPCs). Traditional Industrial Automation (IA) commonly uses programmable logic controllers (PLCs), programmable automation controllers (PACs), and Remote Terminal Units (RTUs) for control and data acquisition—their strengths are sensitivity and accuracy.

IPCs are clearly winning market share from traditional systems. The IPC share of the industrial control hardware market is projected to grow to 18% by 2017, up from 16% in 2014, according to IHS Technology. Over the same period, the market share for PLCs and PACs is forecast to shrink, from 46% down to 44%. In fact, PC-based devices and IPCs have an even higher market penetration rate than indicated in these surveys, because a significant number of mid-range to high-end PLC products are actually using PC-based technology, according to Jan Zhang of IHS Technology.

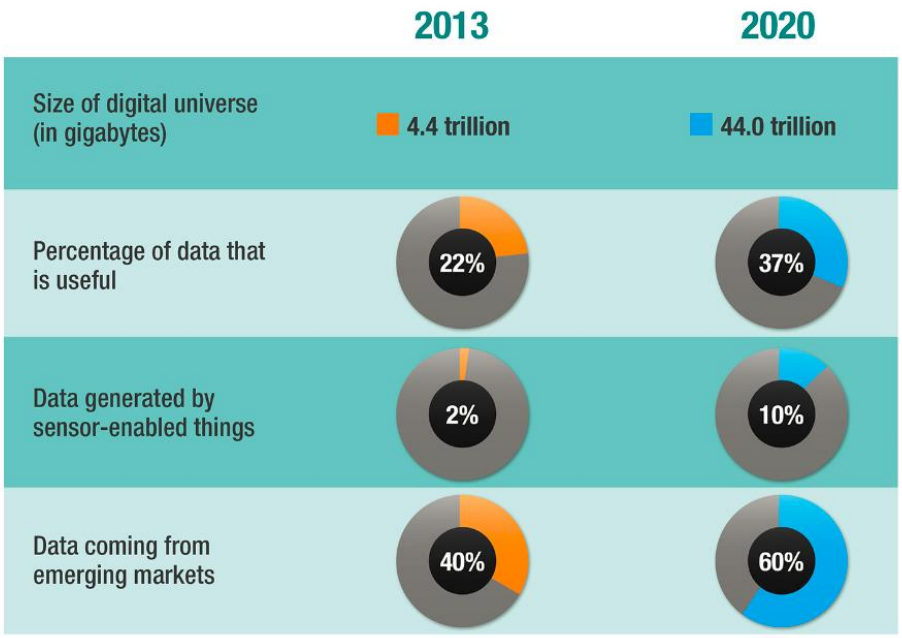
Today, owing to the growing importance of the Industrial IoT as a part of Industry 4.0, IA users are eager to enhance the communications capabilities of their devices or even increase their computing power to take advantage of the explosive growth in the amount of data they can collect. This is one reason why adoption of IPCs is quickly catching up with the systems based on PLCs, PACs, and RTUs, which have dominated industrial automation for decades. It's now possible for IA systems integrators to connect a compact IPC upstream from the PLC or to simply replace the PLC with an IPC for data storage, analysis, and transmission.

In the IT-based IA market, where data analysis and communication between devices are more important, people are tending to replace PLCs, PACs, and RTUs with IPCs. IPCs are generally faster and less expensive because they use off-the-shelf hardware wherever possible. There is also a shift in the talent pool. Young programmers entering industry today mostly come from an IT background rather than an IA background, because x86-based computers dominate the PC market—computers are a part of everyone's daily life, so people are becoming more and more familiar with them.

Preprocessing to control the data flood

To realize the full benefits of the enhanced communications features offered by the Industrial IoT, data preprocessing is essential. Why is data preprocessing so important? One of the major reasons that the Industrial IoT concept is spreading so fast is because of the growing importance of real-time business. And to get maximum value from real-time business applications, users need systems that can process large volumes of data with minimal latency.

However, the world is drowning in data. The amount of data created and copied annually is huge and growing rapidly: It was 4.4 trillion gigabytes in 2013 and is projected to increase 10 times to 44 trillion gigabytes in 2020, according to the IDC/EMC Digital Universe Study. However, currently, only 22% of this data is useful, and this ratio is only expected to improve a little during the next decade.



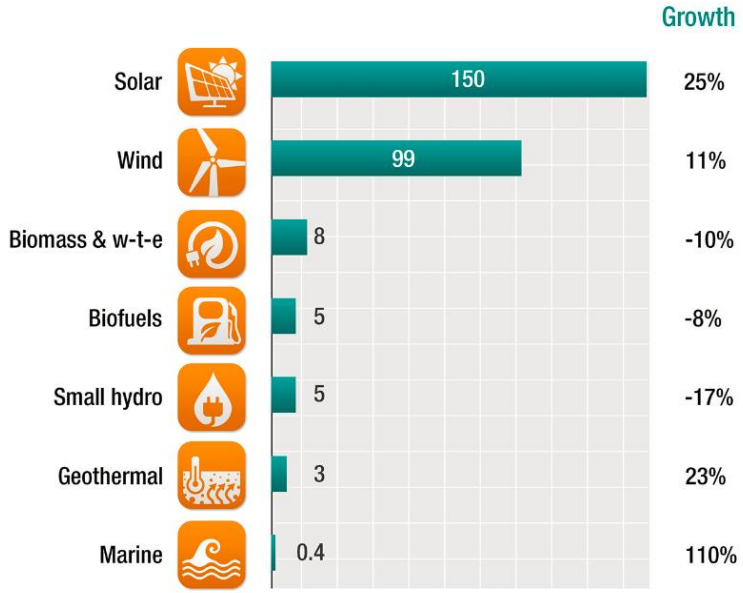
Source: IDC, EMC Digital Universe Study (The Wall Street Journal)

The huge amount of bandwidth wasted on useless data represents a challenge—and an opportunity—for systems integrators. In Industrial IoT applications, devices in the field may now collect so much data that traditional approaches to batching data and processing it at scheduled intervals will no longer suffice. Networks and computer systems will simply be overloaded by the torrent of information converging towards the center. If the data can be preprocessed, then non-essential data can be discarded close to the source, so it will not saturate the network or distract control staff. Therefore, ensuring that data can be processed in real-time—and closer to the edges of the network—is becoming an essential feature of Industrial IoT applications.

Processing data requires computing power, so computers have a paramount role in the Industrial IoT. Due to limited bandwidth (and the potentially limited computing power of central servers) equipment in the field and on the factory floor should only upload necessary data to the upstream servers. Therefore devices closer to the edges of the network need the ability to preprocess data. This can reduce the time and network bandwidth required for big data processing and streaming. In addition, staff who are not overloaded with unnecessary raw data can make decisions more rapidly, and this can cut costs and prevent losses.

Significant demand from the renewable energy sector

The energy industry is one of the major sectors interested in the Industrial IoT. Given the global concern over climate change, renewable energy infrastructure is expanding rapidly—especially in the wind and solar power sectors, which account for over 90% of overall global investment in renewable energy. In 2014, investment in solar jumped 25% to $149.6 billion, and investment in wind jumped 11% to $99.5 billion, according to the Frankfurt School-UNEP Collaborating Centre.



New investment volume adjusts for re-invested equity. Total values include estimates for undisclosed deals.
Source: UNEP, Bloomberg New Energy Finance

Both solar and wind power generation require continuous data processing for functions such as dynamically adjusting solar panel angles, windmill blade angles, and other parameters. An x86 computer is probably the most suitable choice to handle these tasks, because these types of jobs typically require the type of heavy computing power that a RISC computer is unable to provide. High computing power can handle real-time processing of the huge amount of complex data continually generated by rotors, gears, and other devices. But, despite these demands, the computer's power consumption has to be low and the dimensions have to be small, because it usually needs to fit in a confined space and it needs the ability to operate for long periods on limited power from a back-up battery. Furthermore, renewable energy power stations are mostly located in areas that suffer from harsh environmental conditions, such as intensely hot direct sunlight or extreme temperature variations between day and night. The computer usually has to withstand temperatures from -40 to 70°C, and sometimes as high as 85°C. General-purpose consumer grade computers are not rugged enough to keep operating reliably under such conditions. The only choice is an industrial grade computer, however, as we will explain later, even IPCs face challenges with temperature-sensitive components.

For the reasons we have discussed here, a compact, rugged industrial x86 computer is very suitable for renewable energy infrastructure. And if the computer also has a wide variety of interfaces, including network connections, the renewable energy facility can use Industrial IoT concepts to improve efficiency and lower costs. To take just one example, the Industrial IoT approach can add redundancy and fault tolerance: if equipment failure or radio interference prevents a wind turbine from communicating directly with the control center, it can still communicate via a shorter range link to another nearby wind turbine.

Interoperability: essential for smooth upgrades

While the powerful communications features of modern devices help make the Industrial IoT possible, they offer another benefit: interoperability and backward compatibility. Legacy devices and equipment in the industrial, energy, and transportation sectors use a variety of data interfaces, including digital input/output (DIO), RS-232/422/485, Ethernet, and USB. If an IPC is compatible with these standards, this makes it much easier to upgrade older industrial facilities with modern equipment and it therefore allows users to create new business opportunities.

This versatility can ease transitions, because, obviously, it is usually impossible for an industrial user to upgrade a whole factory or transport network all at once. There must be an interim step during which old and new devices will work side-by-side. Therefore, to create an Industrial IoT system, computers must support a wide variety of I/O interfaces and they must be able to understand and convert a wide range of communications protocols.

Wireless can save time and money for industrial IoT edge computing

The Industrial IoT helps operators to connect all of their legacy devices together and to the control center for central management. As well as providing multiple I/O interfaces to connect with downstream devices, the computer also has to send the data upstream. Traditionally, Ethernet is used for many of these connections, but there is a growing problem with Ethernet deployment. As the IoT concept sees more and more devices joining the network, the amount of cable required to connect them all is growing, and wiring costs are also growing. In addition, industrial networks are being asked to connect more widely-separated devices, exacerbating this issue.

Wireless networks provide an answer to this dilemma. As use of the Industrial IoT grows, industrial equipment and sensors are being wirelessly connected to the Internet. Wireless is convenient, covering a wide variety of use cases, in various environments, and serving diverse requirements. With wireless, engineers can quickly install networked devices in locations that are not yet wired, saving their time and lowering installation costs.

For industrial IoT, stability is the key

For industrial applications, the most important requirement—the one that every IPC vendor focuses on—is always stability. Therefore, if wireless is going to replace traditional wired network connections, the stability and performance of the wireless link will be the biggest challenge for Industrial IoT devices. Wireless signals travel through the air, so it's no surprise that wireless performance is closely related to environmental conditions, according to wireless module suppliers' technical specifications and design guidelines. Temperature is considered to be the most critical environmental factor. Guaranteeing stability—not only of the devices but also the wireless connection—is the greatest difficulty facing IPC vendors.

Wireless performance and thermal issues

The table below shows the expected performance of a typical wireless module at various temperatures. Class A represents the range of temperatures within which the device can function normally; Class B is an extreme temperature failure mode, in which limited critical functions are still available; Class C represents the temperature range outside of which the device will stop operating. Obviously, Class A is the desired mode, as we want wireless modules to operate reliably with all functions available. So ideally, we want to keep the wireless module's temperature as close to this range as possible.

Mode	Details
Class A	• Temperature range: **-30°C** to **+70°C** • Functions normally • Supports 3GPP, 3GPP2, or other appropriate wireless standards
Class B	• Temperature range: **-40°C** to **+85°C** • Remains functional • Remains able to establish a voice, SMS, or DATA call at all times
Class C	• Temperature range: below **-40°C** or above **+85°C** • Non-operational

Note that the temperature range shown in the table is the environmental temperature directly around the wireless module, not the temperature outside the computer. The temperature inside the computer case is usually 15 to 20°C higher than the external temperature (depending on CPU usage, the device dimensions, and airflow). And this significantly higher temperature is the actual environmental temperature that the wireless module has to handle—a major challenge.

In addition, wireless modules themselves can generate significant heat that must be dissipated in the host computer for safety and performance reasons. Cellular/mobile 3G/LTE modules can get particularly hot. To stabilize the temperature and remove heat energy from the wireless components, the host computer needs excellent thermal design, and a dedicated thermal solution, such as a heatsink. If the wireless module is removable (for example, a mini-PCIe card) then this makes it much more difficult to create an effective thermal solution in the host device. Many IPC companies are trying to conquer these thermal issues, so they can offer stable wireless performance in all environmental conditions.

Summary: Meeting the thermal challenge

Industry has an opportunity to simplify building new facilities or upgrading old ones, by using wireless networks to bring all equipment—both new and legacy—into the Industrial IoT. However, to ensure these systems are stable, and relieve the industry's concerns about relying on wireless networks for industrial applications, it is essential to deal with thermal issues that degrade the performance of wireless modules. Right now, it is hard to find an industrial x86 computer that can keep a 3G/LTE wireless module operating throughout a wide range of operating temperatures. Despite being fanless (for greater reliability), the Moxa V2201 series supports Wi-Fi and 3G/LTE with an operating temperature range from -40 to 70°C. These are the first such devices to provide such a wide operating temperature range with an LTE module installed. The thermal design includes a heatsink that protects removable modules from extreme temperatures. In addition, the V2201's diverse I/O interfaces provide compatibility with a wide range of devices, including legacy equipment. Their powerful x86 CPU options, tiny dimensions, and rugged design are all perfect for Industrial IoT applications. By using these rugged, palm-sized or compact-sized wireless-enabled x86 computers, customers will be able to greatly reduce data latency, installation costs, and maintenance costs.

Moxa V2201