



electronics maker

The Most Popular Electronics Monthly Magazine

Home	Electronics News	Articles	Magazine	Spotlight	Interviews	Videos	Events
Editorial	Advertise	Design Ideas	Kits & Projects				

HOME » FEATURED ARTICLES » REALIZING IOT & INDUSTRY 4.0 REVOLUTION

Realizing IoT & Industry 4.0 Revolution

2 days ago by **electronics** Comments Off on Realizing IoT & Industry 4.0 Revolution



The first industrial revolution began in the 18th century when the power of the steam engine was harnessed and manufacturing first became mechanised. The second revolution came about when mass production techniques were deployed in the early 20th century. And the third (the one we're in now) came over the next few decades as electronic systems and computer technologies helped to further automate production lines. So what's next?

To fully realize the promise of IoT, disparate systems need to securely connect, interoperate, and communicate. A key step in helping industrial companies capitalize on IoT, and a related technology concept called Industry 4.0 specifically addressing the industrial or factory environment, involves establishing better horizontal (i.e., shop floor), machine-to-machine communications. Such a move addresses an issue often identified as "islands of automation" in which machines and/or machine modules do not fully communicate with one another.

Industrial automation has a history of adopting commercial technology as it becomes mainstream, and applying IoT technologies to improve performance and enable better integration with business systems is a logical step.

According to some industry experts from the likes of Siemens and Bosch, a new period of manufacturing technology dubbed "Industry 4.0" will be upon us within the next couple of decades. At its core are cyber-physical systems made up of software, sensors, processors and communication technologies, according to Brian Holliday, divisional director of Siemens Industry Automation.

Industry 4.0 is an initiative of the German government to promote computerisation in traditional industry sectors, such as production engineering. The goal of the project is the Smart Factory, to include fundamental technologies like cyber-physical systems and the internet of things.

The term Industry 4.0, which is almost exclusively used in Germany, denotes the fourth stage of the industrial revolution. Following on from the invention of steam-driven machines, conveyor belts and office computerisation, the focus is now on the integration of web technologies in products and production engineering. Outside Germany, Industry 4.0 is better known as Industrial Internet.

The second technology inherent in Industry 4.0 is the internet of things. The idea behind this is that devices can be interconnected via the internet and communicate with each other.

The Industrial Internet of Things can perhaps be looked at as a broader, more international movement than Industry 4.0, albeit one with the same underlying characteristics, such as using industrial Ethernet protocols to connect networks all the way from the factory floor to enterprise IT.

Philipp Wallner, Industry Manager and Sameer Prabhu, Director, Industry Marketing, MathWorks shares how MathWorks support customers to bring Industry 4.0 technology for their applications.

"Industrial automation equipment & machines market have become integrated mechatronic systems with growing importance of embedded software where a significant portion of the value of the equipment comes from software related features. Automation components (like sensors or drives), production machines, and entire production lines are connected to each other, continuously exchanging information and collecting data. This not only supports the increasing demand for high production quality (e.g. through sophisticated control algorithms implemented in software and operating in real-time) but also machine efficiency and uptime (e.g. condition monitoring algorithms informing the operator to service specific parts of the system before they break so that 24/7 operation is guaranteed, automatic optimization of the load of different available production lines). Furthermore connecting different manufacturing systems to enable them to exchange information allows flexibility in production schedules and output, which is a desired market attribute. Industry 4.0 takes into account these changing aspects and makes the 'Internet of Things' more tangible for the industry.

However, we also see that Industry 4.0 has not yet fully arrived in the thinking of industrial companies. Many of them are still mechanically focused and have elaborated workflows for mechanical construction but when it comes to software design they are still stuck in conventional methods for programming and testing. This is where MathWorks supports our customers by providing them with a way of designing their mechatronic systems – by using Simulink for modeling the mechatronic system and its environment, testing it using simulations before hardware is built, and then deploying the validated software functionality on real-time systems like DSPs, FPGAs, PLCs, etc.

As this approach allows the design of sophisticated embedded software that is thoroughly tested before it is implemented on the production system, this enables new opportunities and business models. Today's machines and plants have a life span of more than twenty years. During this time span they are rarely modified in order to avoid production loss. Being able to design and test new software separately from the machine will enable innovative companies to provide (paid) upgrades to their customers in order to expand the capabilities of the machine (e.g. with a new software functionality that was not available before / is not available on the standard machine) and/or improve the product quality (e.g. by implementing improved controls strategies).

Another aspect of Industry 4.0 is that MathWorks is helping our customers address the growing amount of data collected during operation. Sensors, drives, production machines & lines, power plants – they all collect an increasing number of data points during operation. However, collecting data does not provide any value on its own. It is the information 'inside' the data that has to be extracted in order to gain additional knowledge about your product quality, process, machine health status, etc. This is where MATLAB is used by our customers to analyze data that has been collected and stored in files, data bases, in the cloud, etc. to derive actionable insight from this data. Some leading edge companies have even started to offer this as a (paid) service to their customers.

Indian manufacturing has historically focused on low to mid manufacturing technology and manufacturing value add processes, and Industry 4.0 presents an opportunity to change this dependence on low manpower cost based manufacturing. One key enabler for India the availability of engineering and scientific talent, which when provided with the required interdisciplinary training and experience, can become a key competitive advantage for India. This can be made possible by strong collaboration between government, commercial, and educational institutions and industry associations. Also, similar to how the wireless technology revolutionized the telecomm infrastructure in industry by leapfrogging over the need to have wireline telecomm infrastructure, Indian manufacturers have an opportunity to leapfrog others in greenfield investments instead of relying solely on an incremental approach to update existing legacy manufacturing footprint. When coupled with Industry 4.0 benefits of flexible production processes that allow products to be tailored to a customer segment of one at relatively low marginal cost, this can become a key competitive advantage for Indian manufacturers."

Maxim Integrated



**Maxim's
Micro-
PLC
Technology**

**Platform to
meet Industry
4.0 Concept**

**Duc Ngo, Director
of Systems and Applications of
the Mass Market Solutions
Business Unit of
Maxim Integrated**

A lot of people think that to reduce size we need to focus on the digital technology. That is not true in the case of PLCs because the digital chips occupy less than one fourth of the board space of the PLC modules. The real issue is the space for analog ICs and discrete components and they do not scale easily like digital chips. Maxim have been looking for ways to combine multiple discrete functions into a single IC to provide system designers with significant advantages in size, power and cost. **Mr. Duc Ngo**, Director of Systems and Applications of the Mass Market Solutions Business Unit of Maxim Integrated explains...

From an IC supplier's perspective, what are the new requirements PLC providers have on control ICs?

This is an interesting question because after almost half a century of existence, people may think that PLCs are at such a mature state that does not have much room for improvement yet we see the demand on new control ICs are higher than ever. Beside the requirement of increased resolution, higher speed, smaller in size, less power hungry and lower price, security and authentication is also in high demand.

Which PLC features need to be improved in order to meet the concept demands of Industry 4.0 and Smart Factory?

Industry 4.0 and Smart Factory mean that we are in a stage in which fundamental changes are needed so that factories will be more interconnected than ever before can respond to latest sensor technologies as well as process "big data" as fast as possible in a most safe and secure environment. In that environment there is no place for single point of failure. The system has to be smartly self-adjusted and be able to maintain accurate performance during all conditions. Therefore, expect a lot of output monitoring, power supply tracking to reduce heat and higher levels of integration.

From Maxim's perspective, which features on PLC chips will be enhanced for the next generation?

Power efficiency is one of the key features. For example, as you know 24V is frequently used for PLC backplanes while 12V is used for on-board distribution. If we can use 48V across the board we can reduce currents by a factor of 4 and thus reduce the power dissipation by a factor of 16. In order to do that we need to have an IC that has high-voltage point-of-load DC-DC converters to eliminate the need for an intermediate DC-DC conversion stage.

Under the trend of Industry 4.0, how does Maxim improve the efficiency of PLC chips? Or how does Maxim change PLC chips?

Like I mentioned earlier, higher levels of analog integration and improve power efficiency are the key features that Maxim have been focusing on. Besides, due to highly interconnected PLCs as an integral part of Industry 4.0, factories must be protected against all kinds of threat including hackers, malware, and viruses etc. System-level software is not enough and one needs to look at hardware-based security to protect against all of these. Maxim has more than 20 years of experience in hardware security implementation for ATMs, POS systems and consumables such as printer cartridges. Thus one can find in our security product portfolio a wide range of products from simple authentication engines to complex secure microcontrollers that can implement advanced standards-based encryption algorithm.

To cater for future trend, does Maxim have any solutions for IO-Link?

We have quite a few IO-Link solutions such as IO-Link light sensor, IO-Link proximity sensor, IO-Link 16-channel digital input hub. You can find more details of these solutions on our website under reference designs. The URL is: <http://www.maximintegrated.com/en/design/reference-design-center.html>

Infineon Technologies



Success of the Internet of Things

**INTERNET OF THINGS
Secure Authentication
and Communication
are Prerequisites for
Business Success**

Dr. Stefan Holschen,
Division Director Chip Card
& Security of
Infineon Technologies AG

The real and virtual worlds are growing together even further to become the Internet of Things through the networking of machines, people and businesses. More and more devices and machines interact independently in networked systems and applications such as Industry4.0, autonomous driving or smart home. Especially in the context of Industry4.0 and the automotive industry, the increasing connectivity renders a great number of opportunities for the economy and for Germany as a business location. Yet, it also presents great challenges for businesses, foremost in questions of data security. How can business secrets and intellectual property be protected on the open internet? How is data protection and confidentiality ensured? How secure is the communication between the different devices or components? And how can hacker attacks be recognized and potential damage prevented? In short, data security and system integrity are essential for the success of new business models because they ensure the availability and reliability of products and services.

Security controllers protect networked IoT systems from unauthorized access and manipulation

Industry has come to understand that connected systems cannot be adequately protected with software alone. The combination of software and hardware offers significantly more efficient protection against attacks and manipulation. Depending on the application scenario, there are special security chips that take the required security standard and the application's efficiency optimally into account.

Internet of Things in the example of Industry 4.0

The next revolution in industrial production, the so-called smart factory or Industrie 4.0, presupposes a secure data exchange. Intelligent machines, storage systems, production facilities and intelligent products are connected globally. This networking increasingly also takes place between supplier and customer, especially for large or mid-sized companies. Figuratively speaking, Industrie 4.0 opens the doors to the factories. This openness increases the need to prevent manipulation and sabotage of networked production systems and avert related financial losses. After all, smart factories can only be put into practice and accepted when they can be implemented in a stable and efficient manner, and when the process know-how and intellectual property (IP) is protected reliably.

At the IT Summit 2014 in Hamburg, Infineon, Deutsche Telekom, Fraunhofer SIT, TRUMPF, WIBU-SYSTEMS and Hirschmann (a Belden Company) demonstrated how a security solution made in Germany" can be implemented in industrial applications. The demonstration shows how seamless communication security works beyond the boundaries of sites or businesses. An employee at the Munich site starts a production order on his tablet PC and transmits it via a secured communication channel to the production site in Hamburg. The order is then automatically executed by a production machine there.

To secure the communication from one end of the value chain to the other (Figure 1), security controllers – in this case Trusted Platform Modules (TPMs) – are integrated in all devices of the IT network (tablet PC, wireless access point, router, production machine). They function as data resource, and as encryption and authentication components. They fulfill multiple functions at the same time:

- Similar to electronic identity verification, they securely identify the individual system components. Only authorized persons and devices obtain access to the network.
- At the device level, they are the basis for detecting manipulation or attacks on components or on the device itself. This way, both logical as well as physical attacks can be detected and corresponding pre-defined measures can be initiated.
- As a Secure storage location, they secure secret information that is needed to encrypt a secure communication channel.

The solution fulfills particularly high security requirements because the security controllers are evaluated and certified by the BSI (Federal Agency for Security in Information Technology) as well as according to "Common Criteria", an international standard. The certification meanwhile is not only granted at the product level but also includes the complete production and supply chain. This affords the greatest possible security to the users and increases flexibility in the users' own production.

A secured complete system was presented as the first prototype at the IT Summit and the solution is to be marketed as soon as in 2015. The hardware components already exist today, so that further scalable solutions can be developed for every other application case.



Trusted Platform Module as security anchor for end-to-end communication

Thus far, communication within company networks is primarily secured by means of pure software solutions. However, these harbor a few drawbacks compared to hardware-based security such as a TPM (Figure 2) and they are only inadequately secure over the long term. Software in principle always consists of written code that can usually be read, copied or overwritten relatively easily, which enables attackers to bypass the security functions programmed by it. The TPM in contrast can serve as a security anchor for components and software: keys that are stored in the TPM do not leave the security chip and can thus not be used without authorization.

At the same time, the TPM that is installed on the motherboard uses international standardized cryptographic algorithms. Integration is provided via standard interfaces like I2C or LPC. The module also permits for example, that keys, data and digital signatures are stored securely, verified and transmitted. The TPM is equipped with a special internal processor for the purpose of the aforementioned authentication and encoding, which enables it to generate keys in a trustworthy environment. At the same time, a specialized crypto processor system ensures the quick calculation of RSA cryptography at up to 2048 bits and thus permits the secured execution of complex cryptographic operations. A non-volatile memory with its own encryption ensures that important data and keys stay preserved on shut-down but that they are secured nonetheless.

The integrity of the software structures and the executed programs on the system can be checked in that the boot process of the system is logged and confirmed against stored cryptographic checksums. Any manipulation of the software can thereby be recorded and stopped by shutting down the affected components or disconnecting them from the network. This way, also the execution of malware like viruses, Trojans and worms can be detected and their spread stopped. Otherwise, this malware can execute unnoticed in the boot process and even spread throughout an enterprise without detection.



Long-term planning reliability – the Trusted Computing Group (TCG) sets standards for industry and consumers

TPMs are based on the open standards of the Trusted Computing Group (TCG) and have already been used for many years in PCs and notebooks. New applications benefit from this experience of many years. In its certification program, the TCG documents all those TPM products that officially meet the standard and thereby provides better orientation in the market for all users. The standard furthermore presents additional benefits: the detailed specifications of the TCG improve the compatibility of the multitude of different operating systems and customer applications. Users can combine different solutions at any time in the design of the system architecture and thus they also have long-term planning reliability.

More and more networking, however, also raises the security requirements in other areas. The TCG already reacted early on to this development and designed the new TPM 2.0 Standard in such a way that a multitude of applications can be covered. Special attention has been given to security in embedded systems for everything from routers to automobiles and medical devices.



Ninan Preman, Senior Sales Manager,
Molex India

The vision of Industry 4.0 is essentially the vision of the Internet of Things (IoT), shares *Ninan Preman, Senior Sales Manager, Molex India*

Industry 4.0 is a vision that has been made possible by technology convergence. A key aspect of the convergence process has been the development of a range of sensor chips. Many of those sensor chips were made possible by advances in microelectromechanical-system (MEMS) technology. For example, temperature and pressure sensors are central to the rise of Industry 4.0. A second factor is the belated arrival of IPv6 addressing which enables an almost limitless number of people and devices to communicate via the Internet. Thirdly, we have seen the development of several competing protocols for ultra-low-power (ULP) wireless which enable sensor-based networks to consume only a fraction of power. These key developments set the stage for Industry 4.0 – a hyper-connected industrial environment where almost every aspect of production can be monitored, supervised and controlled through a mesh networked automation systems and

data analytics, for optimal efficiency and lower costs.

The vision of Industry 4.0 is essentially the vision of the Internet of Things (IoT) although there will be many technical challenges ahead, if the IoT is to realize its full potential.

There are two major challenges that the vision of Industry 4.0 faces. The first one is that it is constantly accelerating demand for communications bandwidth. The datacomm industry is in the process of migrating to 40- and 100 Gbps connectivity. 400 Gbps is already on the horizon and will require further major investment in fiber-optic infrastructure. Those who wish to be players in the development of the IoT should be making this communications migration now while also examining their options for ULP wireless networking.

The second challenge is that there will need to be another major build-out of industrial automation systems with further development of communications protocols and Human-Machine Interface (HMI) technology.

Fiber-optic interconnects will be a major contributor to Industry 4.0 and the rise of the IoT. Molex has developed the compact zCD™ Interconnect System. Based on single-mode silicon-photonics technology, Molex Active Optical Cable (AOC) assemblies for the zCD connector are able to transmit over distances of up to 4km for a fraction of the cost and power of long-reach optical modules. The zCD AOC assemblies are primarily designed for 400 Gbps Ethernet applications and will function with InfiniBand and proprietary protocol applications.

A key element in industrial automation are distributed control systems. Typically, a Human-Machine Interface (HMI) is linked by a communications network typically, over Ethernet to programmable controllers. The controllers are then linked over a fieldbus to the various units involved in automated operations such as; actuators, electric motors, sensors, switches and valves.

Molex is active in provisioning the fieldbus, a computer network using protocols designed for real-time distributed control. Molex supplies interconnect solutions for four fieldbus technologies. In particular, DeviceNet, PROFIBUS, PROFINET and EtherNet/IP. DeviceNet and PROFIBUS are considered fairly traditional fieldbuses for industrial automation while the current trend is to their replacement by the Ethernet-based PROFINET and EtherNet/IP.

Globalization and economic development. Social, mobile and the cloud. Booming Internet traffic. All of these trends are changing the way enterprises operate. Popular consumer applications have become commonplace tools for business networking, marketing, news and tech support. The Internet of Things (IoT) and ubiquitous sensors made "Big Data" a reality that can be a powerful tool to improve efficiencies and boost productivity in manufacturing, mining, agriculture, oil and gas and utilities. These and other demanding industries require integrated networks with high data rates and precision control often in harsh environments. Delivering higher bandwidth, download speeds and storage capacity, Ethernet/IP enables a range of these and other enterprise applications. The open concept with intelligent switches and routers provides a solid technical platform to easily link machines, robots and other field level devices to the enterprise on a single network. Yet, companies across multiple industries are limited by existing infrastructures for industrial telecommunications, automation and wireless networks. Ultimately, many will need technology updates to realize the advantages of real-time data acquisition, device and machine level control, integrated safety, and enterprise-level production insights. In the foreseeable future, we expect a continued transition from proprietary legacy systems. This will be a major driver of opportunity, specifically industry demand for new network installations, enterprise refresh and equipment upgrades.

Praveen Ganapathy, Director Applications-Processors, Sales & Applications, Texas Instruments (India) comments on how IoT will be a big thing for Industrial Automation.

The vision of Industry 4.0 is ensure that smart factories use information and communication technologies to digitize their processes and in return, derive benefits in the form of improved quality, lower costs, schedule predictability and increased efficiency. This would be accomplished through manufacturing, flow optimization, real time inventory control, automated asset tracking, better employee safety and preventive maintenance. Praveen answers how TI is taking this technology ahead and benefits to customers.



Praveen Ganapathy, TI India

1. Do you think this revolution is the next big thing for IoT?

From building and home automation to wearables, from healthcare to automotive, from smart cities to smart manufacturing/industrial automation and much more, IoT touches every facet of our lives. All of these application areas will certainly see significant changes in the coming future.

2. How are you taking this technology opportunity for your customers?

TI, through its unique offerings, focuses on all 'blocks' that go in to making an IOT solution for customers:



TI offers the broadest range of wired or wireless standards from low power Wifi to ZigBee, EtherCAT, PLC-PRIME/G3, NFC, RFid, 6LoWPAN, Bluetooth, BLE, Ethernet/IP and so on. Moreover, low power being critical in various IoT applications, TI offers a host of low power microcontrollers and efficient power management solutions. Last but not least, since security is extremely critical within the connected world, TI offers a host of built-in hardware and software solutions which enable customers prevent, detect and respond to unintended or malicious behavior.

3. Can you comment on future potential? What are the challenges?

Industry 4.0, a much talked about concept, is seeing India as one of the top markets for manufacturing. Industry 4.0 also is a platform which looks to facilitate new ways of creating value and novel business models. Frost & Sullivan, in its recent study on 'Industry 4.0', has unveiled describing this as a platform that shall enable in the future, the unification of information amongst participants in the entire value chain – from product inception to design, manufacturing, services, and even refurbishment. The end result will be a grand system in which all processes are completely integrated and will exchange information in real time. This revolution will transform the manufacturing processes in sync with the speed of change in customer needs – which implies, making the production process flexible without taking excess time.

The major challenges in realizing the potential of Industry 4.0 would be in terms of upgrading the IT infrastructure to comprehend the real time monitoring and management of systems in a secure and reliable manner as any risks to the security or reliability of such manufacturing flows could be catastrophic. The other major challenge is in terms of transitioning talent to be able to handle the highly automated flows and systems associated with the transition to smart manufacturing.

4. Can you throw light on the Industry 4.0 perspective for the India manufacturing scene?

With the global manufacturing industry gearing up for the next level of industrial revolution – Industry 4.0, the Indian manufacturing sector has arrived at a stage of inflection, providing a distinct opportunity to synchronise with this trend and leverage manufacturing to emerge economically stronger in the future.

The rapid development of integrated information and communication technologies will look to provide further impetus for wider deployment of automation and enterprise technology solutions. This shall enable dramatic improvement in productivity and efficiency in all activities associated with various manufacturing operations ensuring promptness / responsiveness. The economic compulsions also mandate India to focus on incentivizing manufacturing by leveraging the new Industry 4.0 trends.

5. How it will benefit India small and medium scale industries?

The benefit to small and medium scale industries will essentially be better inventory control, improved quality, lower costs, scheduled predictability and increased efficiency, which would in turn, translate to significant customer satisfaction and better margins.

 Tags: featured, Industrial Automation, Internet of Things



electronics

Get Updates

Subscribe to our e-mail newsletter to receive updates.

Share This Post



Related Articles

- All Constructions will be Solar Powered – Haryana Government
- Pickering Reed Relays
- How the IoT Will Bring Healthcare Anywhere
- MORNSUN 100W AC/DC Capacitor Charging Module Power Supply Designed for Power Distribution Network
- ON Semiconductor releases revolutionary DSP chip for Audio