BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

WP00006

Communication for the Industrial Internet of Things

Dr. Tobias Heer,
Manager- Embedded Software Development

Dr. Oliver Kleineberg,
Manager- Advanced Development

Subhajit Bagchi,
Vice President-Engineering

Table of Contents

Executive Summary

The term Internet of Things (IoT) first surfaced a few years ago. At its core, it describes a scenario where intelligent devices communicate with each other to enhance functionality and improve operational efficiency without any human interaction.

IoT devices have a physical interface to the real world that enables them to capture, analyze and act on all kinds of data. These devices can learn about their environment and adapt to it; communicate and cooperate with one another; and perform very specific functions within a specific context.

Industrial Internet of Things (IIoT) applies to application areas, like factory automation, process automation, energy infrastructure or transportation. While the idea and vision behind it are the same as in other areas, deterministic behavior, cyber security and redundancy are some of the aspects that are especially important for the IIoT.

IoT will change the way we live and work, and it will transform our world into a connected world.

IoT Application Fields

IoT enables a more efficient world.

In a **smart home**, IoT technology connects heating and cooling systems, appliances like refrigerators, washers and dryers, television and home entertainment systems, home security systems including alarms and cameras and many other devices to make life more convenient for users, as well as save energy, time and money.

In **smart cities**, it connects public transportation systems, trains and airlines to their customers and even individual cars to the roads for intelligent traffic routing. IoT enables continuous monitoring of vehicles, provides intelligent street lighting and tracks the delivery of goods. Electrical distribution systems are able to connect to electricity producing systems as well as electricity consuming devices for advanced and more efficient smart grids.

In **smart health**, IoT-enabled devices support patient care and monitoring, automatic medical data acquisition and analytics of patients' health data and remote health diagnostics.

Finally, there is the **smart factory** – the manufacturing of the future. In this area, IoT often is called the Industrial Internet of Things, or IIoT. Here, the goal is to optimize industrial production processes and increase flexibility through real-time control and analysis of all relevant data.

These are only a few application areas. More will follow once the technologies and products are available.

IIoT for Industrial Applications

Industrial Internet of Things (IIoT) applies to application areas, like factory automation, process automation, energy infrastructure or transportation. While the idea and vision behind it are the same as in other areas, the industrial space has some additional requirements to consider.

Communication in IIoT must be able to:

1. Connect a large number of devices, provide enough bandwidth to transfer all the data and offer a deterministic behavior with low latency.
2. Deliver data "in time." Industrial applications have real-time needs and requirements.
3. Offer high reliability. Loss of data can significantly disturb production processes.
4. Protect and secure data. Often, industrial information is very sensitive, so both intentional attacks and unintended threats must be avoided.
5. Be actively managed. Understanding at any time the status of the communication network is important to guarantee the required high availability.

In IIoT, there are typically more rugged and challenging environmental conditions. The products used must be able to handle mechanical stress, operate under extreme climatic conditions (e.g., high or low temperature, humidity), tolerate extended electromagnetic exposure and function in hazardous locations.

For these reasons, IIoT products have some additional requirements.

IIoT in Action

Many of the existing devices, like programmable logic controllers (PLCs), human machine interfaces (HMIs), and actuators and sensors already form a kind of IIoT. But, of course, the vision of IIoT has potential far beyond the current state.

Instant access to more data offers many benefits. Real-time information about all processes and more detailed status information – as well as the combination of this information (not only for a specific process step, but the complete product life cycle) – will bring new insights to enhancing processes and products.

With IIoT, it will be possible to monitor all parameters and detect any deviation from required quality indicators; predict future events and trends; continuously optimize and improve product quality; reduce time and effort; save money; and lessen environmental impacts. Controlling every step in the life cycle of a product enables new business opportunities and will significantly change manufacturing.

Manufacturing

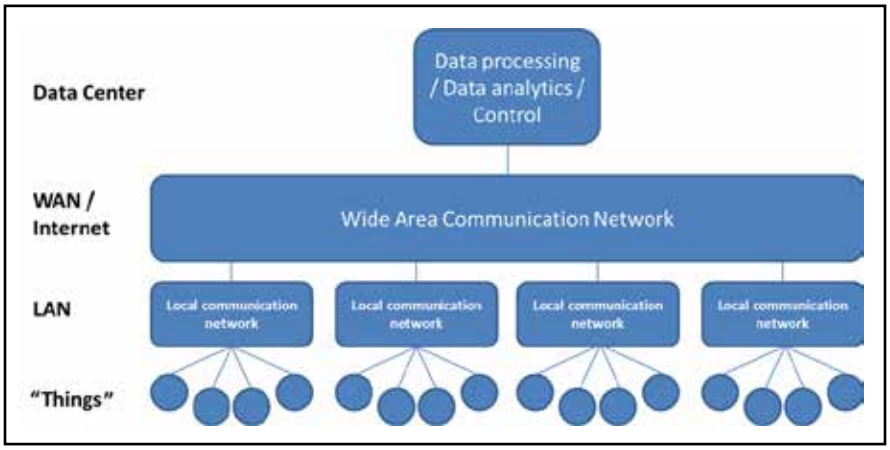
One specific application example of IIoT in action is optimizing maintenance schedules. Sensors monitor all kind of activities, from measuring process values for direct supervision to tracing the production process itself. Sensors also help determine the right time for service activities. Additional uses include monitoring indirect values (e.g., temperature, vibration, humidity, energy consumption). This data can be sent to an analytics tool that senses and detects unusual activity and can predict possible process degradation, output variation or other pending problems. By continuously monitoring operating conditions, actions can be taken before a problem surfaces, which can save time and money for scheduled maintenance operations. Instead of having a maintenance cycle every month, maintenance can take place when it is really required. And this also helps to reduce downtime, because any potential problem can be detected before a failure occurs.

This concept can also be applied beyond local production sites through remote access, which allows the manufacturer of a system (who knows its product best) or a specialized maintenance service provider to do the work. And as an added benefit, the manufacturer of the system can access more information about its product's in-the-field performance, and ultimately derive information on how to improve the product in the future.

Similar scenarios will apply in process automation, like oil and gas, chemical, or food and beverage industries. By monitoring all relevant process values and environmental conditions, in combination with an intelligent data analytics tool, it will be possible to continuously optimize processes, equipment and products.

Power Utility

In smart grid applications, monitoring operation parameters (e.g., electrical voltage, current and phase angles) and combining it with other information, such as the temperature of transformers, weather information and power consumption information, will enable optimal use of existing equipment. This also provides better stability for the power grid and better aligns the operation of power producers with the needs of power consumers. This crosses all elements, like conventional power plants; renewable sources (i.e., photovoltaic, hydroelectric power plants, distributed energy resources, energy storage systems, inverters); power transmission and distribution systems, including transformers, switchgear and load tap changers; and finally, the individual power consumers.



IIoT Communication Architecture

The technology will enable new concepts, for instance, virtual power plants, where dedicated parts of the local energy grid will automatically optimize the operation within its area.

Transportation

Intelligent traffic control systems are another field of IIoT application. Many sensors can be used to collect information about traffic flow, traffic speed or traffic congestion, as well as weather conditions. Analysis of the acquired data, control of traffic flow using traffic information systems and traffic lights, and possibly in the future, direct interaction with cars and public transportation systems will ultimately help to optimize traffic flow, reduce congestion, and save time, energy and money.

What Are the "Things" in IIoT?

In industrial applications, IIoT will connect sensors and actuators.

A sensor is a device that detects, reads or senses any physical values or events. Examples of industrial sensors include flow sensors, level sensors, photoelectric sensors, pressure sensors, temperature sensors, rotary encoders, barcode scanners, light detectors, vision sensors, cameras, acceleration sensors, distance sensors or humidity sensors. Input/output (I/O) modules, voltage and current transducers, or even communication systems can provide sensor data.

Typical actuators in industrial applications are drives, motors, power converters, inverters, motor starters, protection devices or circuit breakers. All of these "things" can influence the real world by serving specific purposes within the larger process.

The Elements of an IIoT System

IIoT is a complex system of devices, communication infrastructure, data processing, data analytics and control systems. Typically, the "things" are devices with an interface to the real world and an interface to a communication network. The network infrastructure typically consists of a local area network (LAN) connecting devices located close to one another. Those LANs are connected to a wide area network (WAN), which typically will be the Internet. And finally, there is a processing unit for capturing, storing and analyzing the data in order to interpret valuable information from the large quantities of data elements.

Intelligent devices are located anywhere relevant data can be captured or actions can be performed. The LAN will do some data aggregation, and the WAN will transmit the data to any point that can make use of it, whether that's somewhere in the cloud, or a dedicated server, controller or other system.

1. **The "Things"**
   The "things," or connected devices, are typically built from four main components:

   a. **Physical interface with sensor/ actuator**
   Each "thing" has to interact with the real world, meaning it needs to have physical interfaces to connect to the process it monitors or controls. If the interface is a sensor, its task is to acquire information. If it is an actuator, its task is to control a physical object. Sensors can detect physical values (e.g., temperature, pressure, flow, light, humidity, vibration or others); certain substances, if it's a chemical sensor or biosensor; and also physical events, including changes, movement of objects, etc.

   Sensors can be based on different technologies. More and more sensors today use semiconductor technologies, and thus can be integrated into chips. Micro-electromechanical systems (MEMS) even integrate complex sensor and actuator systems onto tiny pieces of silicon, like accelerometers, gyroscopes, pressure sensors or a complete "lab-on-chip."

   An actuator can be a type of motor that moves and controls an object; a valve that can open or close a flow of liquid or gas; an electrical switch to turn electrical energy on and off; or other objects that can physically influence the environment. An actuator needs a mechanical, hydraulic, pneumatic or electrical component to act, and has electronic control elements.

   b. **Embedded processing unit**
   Each "thing" needs a processing unit that takes the data from the sensor or sends data to the actuator, completes some data processing and formatting,

Many of the existing devices, like programmable logic controllers (PLCs), human machine interfaces (HMIs), and actuators and sensors already form a kind of IIoT. But, of course, the vision of IIoT has potential far beyond the current state.

and then runs the communication protocols connecting to the Internet. In addition, it handles management of the device, cyber security measures and many other tasks.

IIoT applications will significantly benefit from progress in semiconductor technologies. Smaller silicon structures and higher integration of different functions onto a single System on Chip (SoC) will reduce power needs, as well as space, on the printed circuit board. While today the electronics of a device typically need one or several microprocessors, memory, communication controllers, transceivers, I/Os, and other peripheral controllers, there are already some chips available that integrate these functions on one single piece of silicon. This kind of highly integrated chip is currently found in typical intelligent smart phones.

In the future, chips that integrate all the electronic functions of an intelligent IIoT device will be available. This includes placing several processor cores, I/Os, sensor electronics, communication controllers, and safety, security and other functions into a single, tiny, low-power SoC. And, if those chips are produced in large quantities, the system cost will be driven down significantly, which then will enable new and additional applications.

c. Communication interface

The communication interface is critical for any IIoT application. This interface can either be wired or wireless. Wired interfaces typically are Ethernet-based, which means they follow the specifications of IEEE 802.1 and 802.3 standards. Or, they can be wireless interfaces, implementing Wi-Fi according to one or several of the IEEE 802.11[1] standards. Other interfaces are possible as well, like power line communication, wireless sensor networks according to IEEE 802.15.4[2] (e.g., ZigBee or Wireless HART), and others. However, one mandatory feature in order to be directly integrated into IIoT is to have an Internet protocol (IP) interface.

Another mandatory requirement will be to address cyber security requirements[3]. Cyber security has to be integrated into the device from the beginning. Internet is an open protocol with the risk of intentional or inadvertent attacks to the system. Protecting the device is an absolute must.

d. Power supply

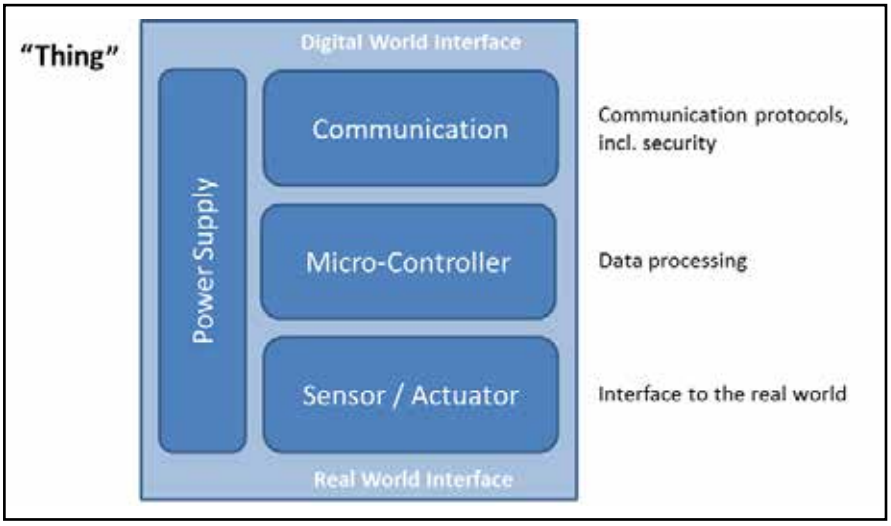
Every "thing" needs electrical energy to work. This means there must be a power supply unit, which either is connected to an external power source (e.g., AC power source, low voltage DC power supply) or has an internal power source, like a battery. The devices in an IIoT application should typically be low-power designs. For very low-power applications, it is even possible to use energy harvesting to power the device. Energy can come from photovoltaic, piezoelectric, thermoelectric or other sources.

2. Communication Infrastructure

IIoT devices typically connect to a LAN. This will either be a wired Ethernet network or access can be given to the LAN via a wireless access point.

If the device does not have a direct Ethernet or Wi-Fi connection, then a conversion in a gateway device must take place first. The LAN segments then will have a connection to the Internet or to another WAN. This connection will have to be protected by a firewall or other means to secure the local communication.

Finally, the WAN can use any technology that fulfills the requirements and offers the needed quality of service. In most cases, this WAN will be a provider network – only in very special cases will there be a dedicated, private WAN. But even in those instances, there will be



IIoT is a system of devices, infrastructure and applications.

connectivity to the Internet. In critical applications, a service-level agreement will be needed to guarantee the required service characteristics.

3. **Application Area**
   There should also be a place where all the acquired data will be collected, stored, analyzed and then transformed into valuable information. This can be a dedicated server located anywhere in the network, a data center, or run virtually anywhere in the cloud. Cloud services can be either a public cloud offered from a service provider or a private cloud operated by the company itself.

   Finally, business applications must take the last step – using the resulting information to spur action for process optimization and control, enabling new business opportunities, or whatever else the IIoT system might be used for.

Communication Technologies for IIoT

Many communication technologies, protocols and standards are available today. But there will be a need to improve certain aspects to better address the specific requirements of IIoT. Let's look at the different communication aspects and see what is needed and what will come.

Network Topology

The number of connected devices in future IIoT scenarios will clearly be much higher than today. This will influence network topologies and the way devices will be connected. More devices requires more cabling, more installation time and more commissioning costs, as well as additional attention to ongoing operations and maintenance. So what will the IIoT LAN look like in the future?

The challenge will be to connect a large number of field-level devices in a simple, cost-efficient manner, while meeting the demanding requirements for performance and reliability.

One of the characteristics of the IIoT vision is the desire to collect as much real-time data as possible that is directly or indirectly relevant to the process. For this reason, the quantity of connected devices will at least double or triple in the next five to 10 years.

All of these systems will need a powerful network connection. The use of traditional field buses will not work; there is a necessity for consistent and unified communication via an Ethernet network. All communication will be based on IP protocol families and Ethernet will be the underlying communication protocol, regardless of whether the connection is wired or wireless.

The network of a large number of devices should be hierarchical to simplify network management and operation. The field level must be divided into effectively manageable communication areas, like a machine, a production unit, or any other logical or physical unit. This is not much different from present structures. The difference will be that the amount of data generated in the cells will be significantly higher than today.

If a wired network will be used, it can either be a star, line or ring topology, or a mix. The use of star topologies, however, will increase because there are some advantages – such as lower latency and higher reliability – compared to other topologies. Of course, the failure of a switch in a star network will disconnect all attached devices, but simulations clearly show that one larger switch has a higher total reliability – more precisely, a higher Mean-Time-Between Failure (MTBF) – compared to a system consisting of many cascaded, small switches. This is the reason why star topologies are used in data centers today.

Of course, line or ring topologies will be used too, because of certain advantages in cabling. Additionally, use of more complex structures, such as extensively meshed network topologies, will increase. With the use of new protocols, these networks will bring more benefits and will need less management efforts.

Wired or Wireless

So what will communication systems look like in the future? Will all devices be connected by cables and wires, or will everything be wireless? In the industrial applications of the past, communications were almost exclusively based on wired networks. In recent years, however, wireless

systems have found increasing use, though mostly in non-critical industrial applications, like configuration and monitoring (WLAN according to IEEEE 802.11), transfer of peripheral data (using IEEE 802.15 wireless sensor networks or proprietary protocols) and in applications, such as mobile workers.

Radio is a "shared media," i.e., all devices share a certain frequency range. If a device is transmitting, the channel is busy. Radio communication can also be error prone. Other radio systems, electromagnetic influences or objects within the radio propagation path can affect the transmission and significantly deteriorate quality, bandwidth and latency. The sporadic loss of data packets is the norm in some radio systems and has to be handled by the applications. This is done at the expense of throughput and latency. While this may be acceptable in enterprise wireless deployment environments (like in offices and businesses), industrial wireless products need to be designed from the ground up for reliable performance in an industrial environment.

Well-designed industrial wireless products are now employing techniques, like enhanced electrostatic discharge (ESD) protection for hazardous environments, wireless mesh technology for quick network reconfiguration and service assurance, and redundancy protocols, like parallel redundancy protocol (PRP) for wireless communications. Intelligent wireless communication techniques are helping industrial wireless systems dynamically adapt to the variation in the performance of various radio channels.

Reliability requirements will also impact the choice of communication technology, wired or wireless, in IIoT. Significant use of wired communications can be expected, but the flexibility of deployment of wireless connectivity – especially in hazardous areas – will drive increasing usage of industrial wireless products designed for such environments.

Data Rates

Wired Ethernet data rates continue to increase. Today, Fast Ethernet with 100 megabits per second (mbps) is the standard in factory applications. In the IT world, Gigabit Ethernet (1000 mbps) has been state-of-the-art for quite some time. Most new PCs have such an interface. Even if Fast Ethernet is good enough for the amount of data produced by an automation device, the trend is to go for Gigabit in the long term.

New chip developments often integrate Gigabit Ethernet interfaces, thus decreasing the cost for a faster connection. Advances in semiconductor processes also will lead to lower power consumption, so that today's price and power consumption arguments will soon be irrelevant. The move to Gigabit Ethernet will happen in the near future in the same way that Fast Ethernet has almost completely replaced traditional Ethernet with 10 mbps.

Along with wired network speeds, wireless network speeds are also increasing. New WLAN technologies, like IEEE 802.11ac and .11ad, are enabling wireless to quickly close the performance gap with the speed of wired communications. Such technologies

are being perfected now in enterprise deployments. Their adoption in IIoT networks is expected over time.

Improvements in the Physical Layer
There are new specifications and definitions in the physical layers of wiring systems, as well[4]. One element is to make cabling simpler. While Gigabit Ethernet today needs four pairs of copper wire, developments are underway to bring Gigabit Ethernet to a single pair, but with some limitations in distance. In addition, Fast Ethernet will also be able to run on a single pair, likely without any restrictions in distance.

Similarly, there is progress with fiber optic communication and it is already in use for some applications. This progress could simplify topologies and offer higher data rates and lower latencies. But, it is still challenging to predict whether newer fiber optic technologies will find their way to IIoT applications or not.

Power Consumption
Another consideration, regardless of whether a system is wired or wireless, is power consumption and miniaturization. Progress in semiconductor technologies will enable smaller silicon structures, which will lead to higher integration and reduced power consumption.

Low-power wireless LAN approaches will enable the use of Wi-Fi for small, low-energy devices, such as battery-powered sensors. While there are many low-power radio standards and technologies working in a similar way, the advantage of low-power WLAN is the system wide consistency it provides – using Ethernet frame formats and IP protocols throughout the entire system. There are also ways to apply precise time synchronization, improved quality of service guarantees and bandwidth reservation for Wi-Fi systems.

Deterministic Behavior
Many IIoT applications will need deterministic behavior, which means maximum latency guarantees for data transfers. The exact requirements are dependent on the specific application, but the requirements will definitely increase. And unlike today, this is not strictly limited to a single unit or within a single machine. Rather, these data transfers will take place between different areas, different production cells and even to locations outside a single plant.

There is a need to have a guaranteed maximum latency from the data source to the destination and within a control loop back to the source. The timing requirement is primarily related to the process. It can be broken down to the physical processes, computer processing and communication components.

Communication infrastructure must offer specific service guarantees. There are some real-time Ethernet protocols available, which are able to fulfill these timing requirements. But, none of those is specified in an Ethernet standard. Real-time capability will be achieved in future networks through the use of one or more elements, such as:

- **Time Synchronization, Based on IEEE 1588**
  Precision Time Protocol (PTP) allows accurate synchronization of clocks distributed into all components. Its use allows decentralized distributed clocks to run synchronously with an accuracy of less than one microsecond (µs). These precise clocks make it possible to fully de-couple the processes from communication.

  Any actions can be time-controlled rather than being event-driven. PTP is already in use in many applications. Just recently, the IEEE group 1588 started standardization work on the further development and improvement of PTP. It is likely to be available in 2016, resulting in a third version of the protocol.
- **Higher Data Rates**
  Increasing the data rate also brings significant improvement for real-time applications. This is due to the reduced latencies of data packets and improved data forwarding mechanisms inside high-performance switches. Due to reduced latency of data packets, the switch is blocked only a fraction of the time. On the other hand, the likelihood that a packet blocks the switch and causes delays is also much smaller – because the utilization of the network will be much lower.
- **Ethernet Standards for Real-Time Applications**
  In addition to these two first effects, there is another technology that will significantly improve the real-time capability of Ethernet. This solution is currently being defined in a small workgroup, under the umbrella of IEEE 802, called the Time Sensitive Networking (TSN) task group[5].

  The TSN group is committed to defining a deterministic version of Ethernet and going to the limits of what is technically feasible, thereby covering the most demanding applications. Their specialists come from a wide range of application fields, such as automotive, instrumentation, avionics or broadcast, and are working together.

  The technical concepts behind TSN include:

  - A Time-Aware Shaper inside the switches, which controls the flow of real-time packets in a time-triggered way. It uses exact, pre-defined time slots throughout the network.
  - A bandwidth reservation protocol that enables a fixed reservation of all required resources in the network.
  - A Frame Preemption method, which interrupts lower-priority packets so high-priority packets will not be delayed or blocked.

  Work on these new technologies has just begun and the standards are planned to be completed in 2016.

The TSN group is committed to defining a deterministic version of Ethernet and going to the limits of what is technically feasible, thereby covering the most demanding applications. Their specialists come from a wide range of application fields, such as automotive, instrumentation, avionics or broadcast, and are working together.

Cyber Security

Increasing connectivity and the use of information and communication technology based on open standards are essential ingredients of IIoT. If all relevant data is available in real time, faster and smarter decisions can be made, and more flexible, efficient processes can be designed.

The downside of this approach is the significantly larger risk of vulnerability to the system. Ubiquitous networking and openness increases the possibilities of interference with the system and makes it absolutely necessary to ensure cyber security for all equipment and systems to guarantee:

- Availability – avoiding any system failures so access to required data and information is possible at all times
- Confidentiality – permitting data access only for authorized users, either a person or a technical unit, and preventing unauthorized access
- Integrity – maintaining authenticity of the data by preventing (or at least detecting) any modification of the data, whether intentional or unintentional
- Accountability – clearly identifying any transactions

Research indicates that only about 20 percent of security incidents are deliberate. Cyber security for IIoT will need to detect, prevent and protect against threats from deliberate attacks, as well as from unintentional human errors and device flaws. Organizations need to have processes in place to analyze vulnerabilities; adopt measures to prevent, protect and defend data; and define procedures and rules, which describe how to guarantee data security and maintain compliance. This may also include defining and implementing an Information Security Management System (ISMS).

The IIoT network will need to support security functions, including:

- Encryption to ensure confidentiality of the data and prevent any unauthorized interception of data, which is particularly important for data traffic running over public networks
- Access control to ensure that only devices allowed to communicate with each other can do so, to prevent unauthorized access during operation
- Creation of zones and conduits to separate critical sections of the system from non-critical sections, and application of zone security controls for industrial protocols to protect against deliberate attacks and prevent unintentional threats from affecting critical assets
- Authentication as another element of access control to block devices and users without explicit access to the elements of the network

Using concepts, such as Trusted Computing Group's Trusted Platform Module[6] specifications and other similar concepts, a security chain can be built by the devices from the hardware and firmware up to the applications. This helps ensure that each component in the system – software, connection and transaction – is trustworthy, safe and secure.

Other security measures include the detailed logging of all events and changes via log files to track exact network activity. Network management and security tools can be used to monitor the network behavior and traffic. They can also detect potential threats, like abnormal traffic patterns or unauthorized access attempts, and take appropriate countermeasures.

Reliability

One aspect of reliability in an IIoT network is network redundancy, or the behavior of the communications network in the event of a failure. Disturbances and interruptions in the network can never be completely avoided. Failure of a cable or connector due to mechanical overload, the failure of a power supply unit, or even short-term shutdowns for maintenance reasons can affect network traffic.

In such cases, the goal is to ensure that only the smallest possible part of the system

is affected. Network media redundancy provides redundant communication paths. A communication network is designed in a way that it can redirect traffic in case of a failure to an alternative path. A basic requirement for each Ethernet network is to avoid loops. Only one active path between source and destination is allowed at any time.

Alternative paths are needed for media redundancy, however. A redundancy control protocol is required to resolve this contradiction, which ensures that there is only one logical path between any two devices, even if there are multiple physical paths. Only one of the paths must be active and transfer data, while the other paths are in standby mode.

This requires the monitoring of all the paths, detection of any failures, and then a means to switch to an alternative path once a failure has been detected. This principle always leads to some interruption time in communication.

There are a number of protocols on the market based on this procedure, which differ both in the switch over time and the supported topology. These include:

- Rapid Spanning Tree Protocol (RSTP) works for a variety of topologies, including meshed networks, but there are restrictions on the number of switches between transmitter and receiver.
- Media Redundancy Protocol (MRP)[7] is limited to ring topologies, but has the advantage of very fast and deterministic switchover characteristics.
- Parallel Redundancy Protocol (PRP)[8] and the High Availability Seamless Ring (HSR) are a completely different approach – based on networks with two independent active paths between two devices. The biggest advantage is the uninterrupted communication that avoids any downtime in the event of a failure and provides the highest availability.

There also are other approaches currently in the works, such as a distributed link aggregation protocol (Distributed Resilient Network Interconnect) and the Shortest Path Bridging (SPB) protocol[9]. For IIoT applications, the required network redundancies must be analyzed carefully before a protocol is chosen. Often, there will be a mix of network segments that use full redundancy based on PRP, and other areas where using RSTP, MRP or distributed link aggregation will be the best choice to achieve network reliability.

Network Management

Another important aspect for network infrastructure is the monitoring and diagnosis of operations. Failures of communication can be critical to production. Potential problems must be recognized as early as possible so that they can be solved before a critical situation arises.

But diagnosis and troubleshooting are only part of future network management solutions. The requirements for tools will go much further and need to be more intelligent. Future tools will support users in network planning, installation and commissioning, operation, maintenance, and troubleshooting.

Today, a significant portion of the costs and expenses for the network already come from operation. The cost for the infrastructure makes up only a relatively small part. Engineering efforts for network planning, cabling, installation, configuration, acceptance testing, monitoring, troubleshooting, and maintenance, as well as the ongoing optimization of the network, require a lot of manual and expensive work.

In the future, it will be even less possible to cover all this manually. And it will get more difficult to have sufficient qualified staff for this purpose. More and more tasks will have to be automated and executed by intelligent tools. These tools must be capable of supporting and automatically processing specific network management tasks, thus minimizing manual intervention.

Future IIoT applications will be electronically designed using computer models. All processes will be simulated and optimized

digitally. A digital plan for the system will be developed even before construction begins.

The individual physical components will be derived from the digital models and descriptions with the use of intelligent engineering tools. Within this step, there will be an assignment of logical functions to physical resources, like servers, dedicated controller devices, or intelligent actuators and sensors. Then, as a next step, a model of the required communications network can be derived from the communication relationships, timing requirements, factory layout and physical locations.

An intelligent network planning tool can automatically design a network plan; define the required switches and routers, including required data rates, port counts and port types; and create wiring diagrams and generate all the specific configuration files for each network device.

After the installation of the network, an automatic check of wiring quality parameters and end-to-end connectivity can be performed and documented. If the physical connectivity is correct, then the individual devices will be provided automatically with all the configuration settings that optimally fit the application.

During operation, all traffic flows are monitored, changes and modifications are tracked, trends in communication patterns and network characteristics are analyzed, anomalies are detected, and corresponding instructions, warnings or alerts are sent to the operator.

Together, this will deliver reliable communication services for all elements of the system.

Wide Area Networks

IIoT, per definition, does not stop at the border of the local area. One of the major elements is communication over the Internet with other devices, with cloud services or data centers, and with humans using the provided data. For this reason, connectivity to the Internet, or generally to a WAN, has to be provided. Depending on the specific application, the communication has to be reliable and provide real-time performance, sufficient bandwidth and cyber security.

In most cases, the communication will be provided by a communication service provider. For access to the broadband infrastructure there will be a variety of connection options. These include digital subscriber line (DSL) access; wireless, like Wi-Fi or 3G/4G mobile access technologies; and direct IP connection or others. Many IIoT applications will use mobile networks, with long-term evolution (LTE) as the most promising protocol.

Whether it uses the Internet or private networks, the provider must comply with appropriate service-level agreements.

Cyber security will also be extremely important. IIoT traffic has to be protected on its way through the Internet. Using encrypted channels, setting up Virtual Private Networks (VPN), controlling access by authentication and authorization mechanisms, and having intelligent firewalls at the edge of each network segment will be a must.

IIoT – When Will It Be Reality?

There are many different opinions on what IIoT is and when it will become reality.

Of course, some parts of the IIoT are already here today. Many devices do communicate within a factory or in other industrial applications, without any human interaction. This is reality in automation applications. And many devices already communicate over long distance, called machine-to-machine (M2M) communication. So, IIoT is not starting from zero. But the vision of IIoT goes far beyond what is here today. Many more applications and new business opportunities will come up, while more data will be acquired, transmitted and processed.

Many enabling technologies are here, or will be realized in the next few years. Investors and big companies are willing to invest billions of dollars in this field, because they expect large business in the future. And government funding in all areas of the world will help in bringing those visions forward.

There is already a lot of hype about IoT in general. There are predictions forecasting a market of 8 billion, 20 billion, 60 billion or even more than 100 billion connected devices in 2020. The total business value of IoT will be in the range of hundreds of billions of dollars, maybe even beyond $1 trillion. And while those revenues include the devices with their hardware and software, most of the revenue will come from the associated services: managed services, cloud services, value-added application services, network services and more.

It's important to be careful as many of the market segments, especially those in industrial applications (IIoT segments), still have critical prerequisites that will need to be met and barriers that will have to be overcome. There are many standards, for communication, data presentation, data processing, data exchange formats, storage, device management, analytics and so on. There are significant cybersecurity issues that will need to be carefully specified and designed. To make the vision of IIoT possible, at the very least a certain unified standard system must be agreed on, so that seamless interoperability is possible. Otherwise, the effort and cost to use those systems will be far too high.

Then there are other questions. How fast can the growth rate realistically be in this market? What new business benefits are required to enable the investment in those systems? How many engineering efforts are necessary to develop all the different elements needed for this big picture and what new business benefits are required to enable the investment necessary for these engineering efforts? Are all the engineering resources and foundation technologies available to make it a reality?

It's clear that there are still some questions to be answered and technologies to be perfected. But, IIoT is real and it's here

now. The benefits are evident – companies now need to determine how they will take advantage of what IIoT has to offer and they need to carefully select the right partner to help with this critical transition.

Belden Solutions for IIoT

Belden—as a global expert in mission-critical signal transmission systems in the broadcast, enterprise and industrial markets, and a pioneer in critical infrastructure security—is best suited to fulfill the various requirements of the IIoT transition.

Belden enables its customers to deploy a true industrial Ethernet infrastructure that already incorporates and supports the communication technology and security needs of the IIoT. With its market leading industrial products portfolio, Belden and its Hirschmann and GarrettCom brands already offer products like Ethernet switches, routers, security devices, wireless access points and software tools enabling highly reliable communication solutions in the industrial space. With its Tofino and Tripwire security solutions, Belden also enables its customers to secure the industrial Ethernet infrastructure and applications from the get-go.

As the IIoT standards become a reality, Belden products will support all the necessary requirements of the gradual migration to IIoT technologies that enable customers to make the transition in a secure and scalable manner while maintaining business continuity.

To support this transition, Belden is working with many standardization bodies and industry groups defining the missing pieces of the IoT infrastructure solutions. Belden is also working with universities and academic organizations promoting and contributing to groundbreaking research on Smart Factory and Industry 4.0.

Expect to see many new and innovative solutions from Belden over the coming years.

Learn More

Discover more Industrial Internet of Things content on Belden's dedicated IIoT web page. You can link to experts, download additional technical resources, and explore industry standards.

REFERENCES

1. IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS, The Working Group for WLAN Standards, http://www.ieee802.org/11/
2. IEEE 802.15 Working Group for Wireless Personal Area Networks, http://www.ieee802.org/15/
3. Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report, Forschungsunion / Acatech, April 2013
4. IEEE 802.3 ETHERNET WORKING GROUP, http://www.ieee802.org/3/
5. IEEE 802.1 Time-Sensitive Networking Task Group, http://www.ieee802.org/1/pages/tsn.html
6. Trusted Computing Group, http://www.trustedcomputinggroup.org/
7. Industrial communication networks - High availability automation networks - Part 2: Media Redundancy Protocol (MRP), IEC 62439-2
8. Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC 62439-3
9. IEEE 802.1 Interworking Group, http://www.ieee802.org/1/

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.belden.com and follow us on Twitter @BeldenInc.

Phone: **1.800.BELDEN1**
www.belden.com

COMMUNICATION-FOR-IIOT_WP00006_INET_BDC_0315_A_AG