HIRSCHMANN
A BELDEN BRAND

White Paper

WP00004

Communication Technologies for the Smart Factory of the Future

Building a communications infrastructure for Industry 4.0 and the Internet of Things

Andreas Dreher
Strategic Technology Manager at Hirschmann Automation & Control in Neckartenzlingen

Table of Contents

Executive Summary

The terms "Smart Factory," "Smart Manufacturing," "Intelligent Factory" and "Factory of the Future" all describe a vision of what industrial production will look like in the future. As its name suggests, the Smart Factory will be much more intelligent, flexible and dynamic. Manufacturing processes will be organized differently, with entire production chains – from suppliers to logistics to the life cycle management of a product – closely connected across corporate boundaries.

The Smart Factory will have a highly complex structure that requires a holistic approach to control and management. The individual production steps need to be connected seamlessly. This will impact processes, including factory and production planning; product development; logistics; enterprise resource planning (ERP) and manufacturing execution systems (MES); control technologies; and individual sensors and actuators in the field.

In a Smart Factory, machinery and equipment will have the ability to improve processes through self-optimization and autonomous decision-making, instead of continuing to run fixed program operations, as is the case today.

To do this, the future structure of factories will be much different: an inter-connected combination of intelligent production technologies, with the newest high-performance information and communication technologies. This will provide digitally integrated engineering and horizontal integration across the entire value chain, as well as vertical integration and connectivity across all levels of production.

In Germany, a large publicly funded project has been set up to define these concepts of industrial production – called "Industry 4.0" – which will create the fourth industrial revolution[1]. Similar projects are being established in other countries as well[2] (See Figure 1).

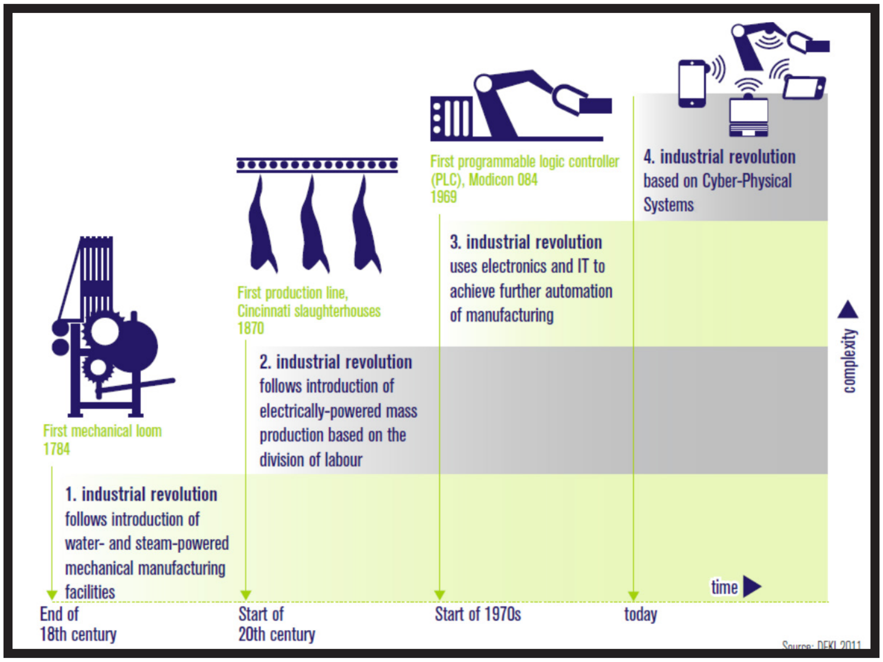

First mechanical loom
1784
1. industrial revolution
follows introduction of water- and steam-powered mechanical manufacturing facilities
First production line, Cincinnati slaughterhouses
1870
2. industrial revolution
follows introduction of electrically-powered mass production based on the division of labour
First programmable logic controller (PLC), Modicon 084
1969
3. industrial revolution
uses electronics and IT to achieve further automation of manufacturing
4. industrial revolution
based on Cyber-Physical Systems
complexity
time
End of 18th century
Start of 20th century
Start of 1970s
today
Source: DFKI 2011

Figure 1: Industry 4.0 - the 4th industrial revolution (Source: DFKI)

High-performance, reliable communication technology will exceed what is currently in use. This technology will make it possible to:

- Transfer large amounts of data in real-time and with minimum delay
- Connect a large number of individual devices in a very reliable manner and with the highest standards of data security
- Utilize more and more wireless technologies, within the factory or plant, and also for remote connectivity
- Operate in an energy-efficient manner

This article describes the requirements of Smart Factory communication and the future technologies that will be available to solve these requirements. You will learn:

- How future automation systems will be structured
- How network topologies will be adapted to connect more devices
- How wireless technology will be integrated into industrial networks
- How communication infrastructure will impact data rates, data transfers and power consumption demands
- How to minimize system vulnerability to improve security and reliability
- How to diagnose and troubleshoot system issues

It should be emphasized that these concepts and trends are not only relevant for the vision of the Smart Factory. In fact, many other critical applications in industrial automation will benefit, such as the process, energy and transportation industries.

The focus of this white paper is industrial local area networks (LANs) – the networks within local manufacturing facilities. Certainly, there are additional requirements and technical procedures for communication outside of the factory. Wide area networks (WANs) are equally important for the success of the Smart Factory. However, this will not be discussed in detail in this article.

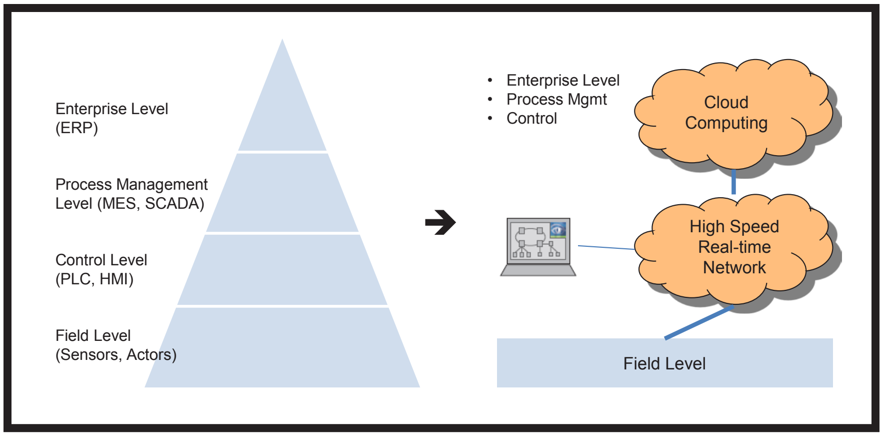


Figure 2: The automation pyramid will disappear

Changing the Automation Landscape

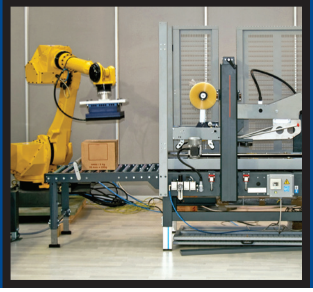
Prior to discussing individual aspects of communication, it's important to consider the structure of future automation systems. Today, automation consists of several clearly separated levels (see Figure 2). This represents the well-known automation pyramid with actuators and sensors at the field level; control devices, I/O modules and operator terminals in the control level; and then the process management level with computers for engineering, supervisory control and data acquisition (SCADA) and MES systems. Finally, there is the enterprise level with business processes and ERP systems, typically located on servers in the IT data center.

Each of these levels is relatively well structured; individual devices can be clearly mapped to one of the levels. With Industry 4.0, this will change to a certain point. If you consider the equipment, the field level will remain as a separate dedicated level. The actuators and sensors are the physical interfaces to the process, so they will always exist, but they will embed more and more intelligence. As parts of "Cyber Physical Systems," they will autonomously perform many processes.

All functions located above the field level will potentially move to high-performance servers located in a server cluster, data center or in a "cloud." Virtualization, the separation of specific functions and processing hardware, which is already state-of-the-art in the IT world, will find its place in the factory, as well.

Ultimately, the big advantage is to reduce the variety of devices, which results in easier management, better utilization of resources and a clear cost savings. This approach has not yet been adopted in automation because of issues related to performance, required determinism, reliability and the lack of fast, low latency communication from the servers to the field level. These issues will be addressed in new and upcoming systems.

The future performance levels of IT and communication systems together with the requirements of the Smart Factory vision will bring about enormous increases in efficiency.



Communication within the Factory LAN

The following sections describe the requirements and solutions for communication within a manufacturing site's LAN.

Network Topology

The number of connected devices in a future Smart Factory LAN will clearly be higher than it is today. This will influence network topology and the way devices will be connected. More devices require more cabling, more installation time and more commissioning costs, as well as additional attention to ongoing operations and maintenance. So what will the Smart Factory LAN look like in the future? (See Figure 3)

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

One characteristic of the Smart Factory 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 double or triple.

All of these systems will need a powerful network connection. The use of field busses will decrease significantly to make way 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 manageable communication cells, like a machine, a production unit, or any other logical or physical unit, which 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.

The network will still use either star, line or ring topologies, 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.

Lines or rings will be used too, because certain topologies might have 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?

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 more in non-critical industrial applications, like configuration and monitoring (WLAN according to IEEEE 802.11[3]), transfer of peripheral data (e.g., using IEEE 802.15[4] wireless sensor networks or proprietary protocols) and in applications like 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, other 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 drive the choice of communication technology, wired or wireless, in the Smart Factory. 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 PCs today 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 longer 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 the Smart Factory is expected over time.

Improvements in the Physical Layer

There are new specifications and definitions in the physical layers of wiring systems, as well[5]. 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, however, with some limitations in distance. In addition, Fast Ethernet will also be able to run on a single pair, probably without any restrictions in distance.

Likewise, there is progress with fiber optic communication and it is already in use for some applications. This progress could simplify topologies and offer high data rates and low latencies. But, it is still very hard to predict whether newer fiber optic technologies will find their way to the Smart Factory 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 help here. Smaller silicon structures and higher integration of different functions onto a single "System on Chip" reduces power, as well as space on the printed circuit board.

Low-power wireless LAN approaches will enable the use of Wi-Fi for small, low-energy devices, e.g., 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 systemwide consistency it provides. It uses Ethernet frame formats and IP protocols throughout the entire system.

Deterministic Behavior

Smart Factories need deterministic behavior, which means maximum latency guarantees for data transfers. The exact requirements are dependent on the specific application, but already it is clear that the requirements will

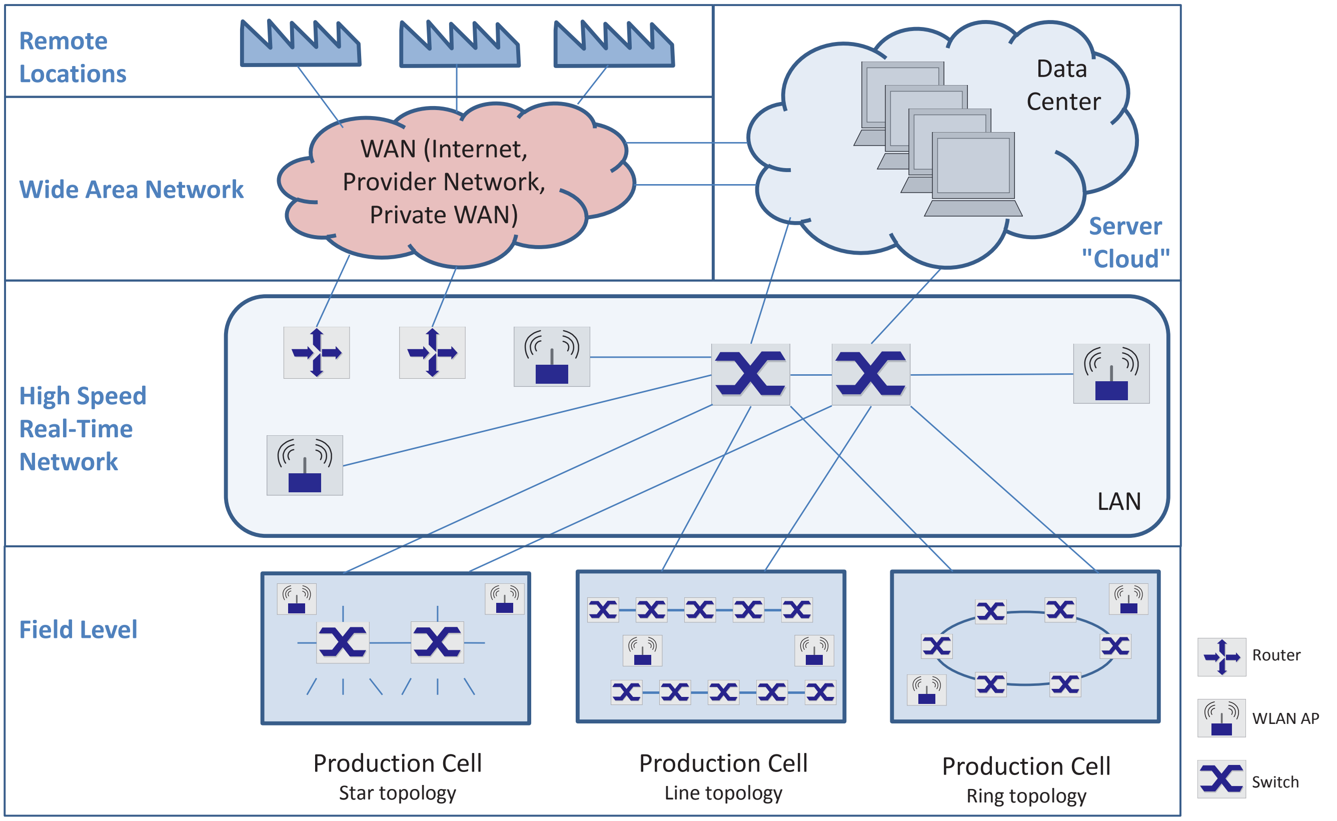
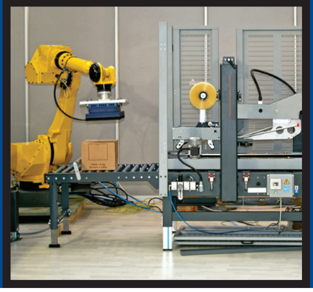


Figure 3: Smart Factory Network Topology



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 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 that 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 synchronized clocks distributed into all components. Its use allows decentralized distributed clocks to run synchronously with an accuracy of far below 1 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[6].

  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 exactly pre-defined time slots throughout the network.
  - A bandwidth reservation protocol that does 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.

Cyber Security

Increasing connectivity and the use of information and communication technology based on open standards are essential ingredients of the Smart Factory. 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 it is absolutely necessary to ensure cyber security for all equipment and systems to guarantee:

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

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

The Smart Factory network will need to support security functions, including:

- Encryption to ensure the 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 factory 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 specifications[7] 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 a Smart Factory system is network redundancy, or the behavior of the network in the event of a failure. Disturbances and interruptions in the communications 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 the 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 stand-by 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). It 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). This one is limited to ring topologies, but has the advantage of very fast and deterministic switchover characteristics[8].
- Parallel Redundancy Protocol (PRP) and the High Availability Seamless Ring (HSR). This is 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[9].

There also are other approaches that are currently in the works, such as a distributed link aggregation protocol (Distributed Resilient Network Interconnect) and the Shortest Path Bridging (SPB) protocol[10]. For Smart Factory 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 the network infrastructure is the monitoring and diagnosis of operations. Failures of communication can be critical to the production. Potential problems must be recognized as early as possible so that they can be solved before a critical situation arises.

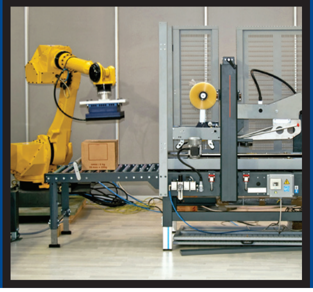
But diagnosis and troubleshooting are only part of network management solutions for the Smart Factory. The requirements for the tools of the future will go much further and need to be more intelligent. Future tools will support the users in network planning, installation and commissioning, operation, 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 will be executed by intelligent tools. These tools must be capable of supporting and automatically processing specific network management tasks, thus, minimizing manual intervention.

The factory of the future will be electronically designed using computer models. All processes will be simulated and optimized digitally. A digital plan for the factory 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, the factory layout and the 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 and data exchanged for all elements of the Smart Factory.

Wide Area Networks

The Smart Factory does not stop at the border of the plant. One of the major elements is the communication along the entire value chain. This includes suppliers, logistics, customers and all other stakeholders.

Therefore, communication external to the factory must provide reliability, real-time performance, security and sufficient bandwidth. In most cases, the communication will be provided by a communication service provider.

Whether it uses the Internet or private networks, the provider must comply with appropriate service-level agreements. In terms of broadband infrastructure, there will be a variety of connection options in the future. These include traditional DSL access, wireless technologies, like LTE, direct IP connection, MPLS networks, Carrier Ethernet, or direct access to optical networks.

Cyber security will also be extremely important. Smart Factory 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.

Summary

The success of the Smart Factory vision largely depends on achieving required performance levels by the underlying communication technologies. If the communication infrastructure cannot meet the demanding requirements, many applications will not work as intended.

Currently, there are many ongoing efforts to close the remaining gaps with new, innovative enhancements in data communication technologies. Communication still has several challenges to overcome, but from today's perspective, it will be possible to provide all necessary solutions to make the Smart Factory vision a reality.

HIRSCHMANN

A **BELDEN** BRAND

References

[1] Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report, Forschungsunion / Acatech, April 2013

[2] National Network for Manufacturing Innovation (NNMI)

[3] IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS, The Working Group for WLAN Standards, http://www.ieee802.org/11/

[4] IEEE 802.15 Working Group for Wireless Personal Area Networks, http://www.ieee802.org/15/

[5] IEEE 802.3 ETHERNET WORKING GROUP, http://www.ieee802.org/3/

[6] IEEE 802.1 Time-Sensitive Networking Task Group, http://www.ieee802.org/1/pages/tsn.html

[7] Trusted Computing Group, http://www.trustedcomputinggroup.org/

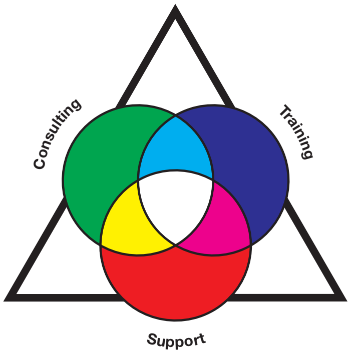
[8] Industrial communication networks - High availability automation networks - Part 2: Media Redundancy Protocol (MRP), IEC 62439-2

[9] Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC 62439-3

[10] IEEE 802.1 Interworking Group, http://www.ieee802.org/1/

Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge plays a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world's first certification program for industrial networks. Up-to-date manufacturer's expertise, an international service network and access to external specialists guarantee you the best possible support for products. Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.



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/hirschmann**