SIEMENS

Technical article

Industrial Communication – a Prerequisite for Digitalization

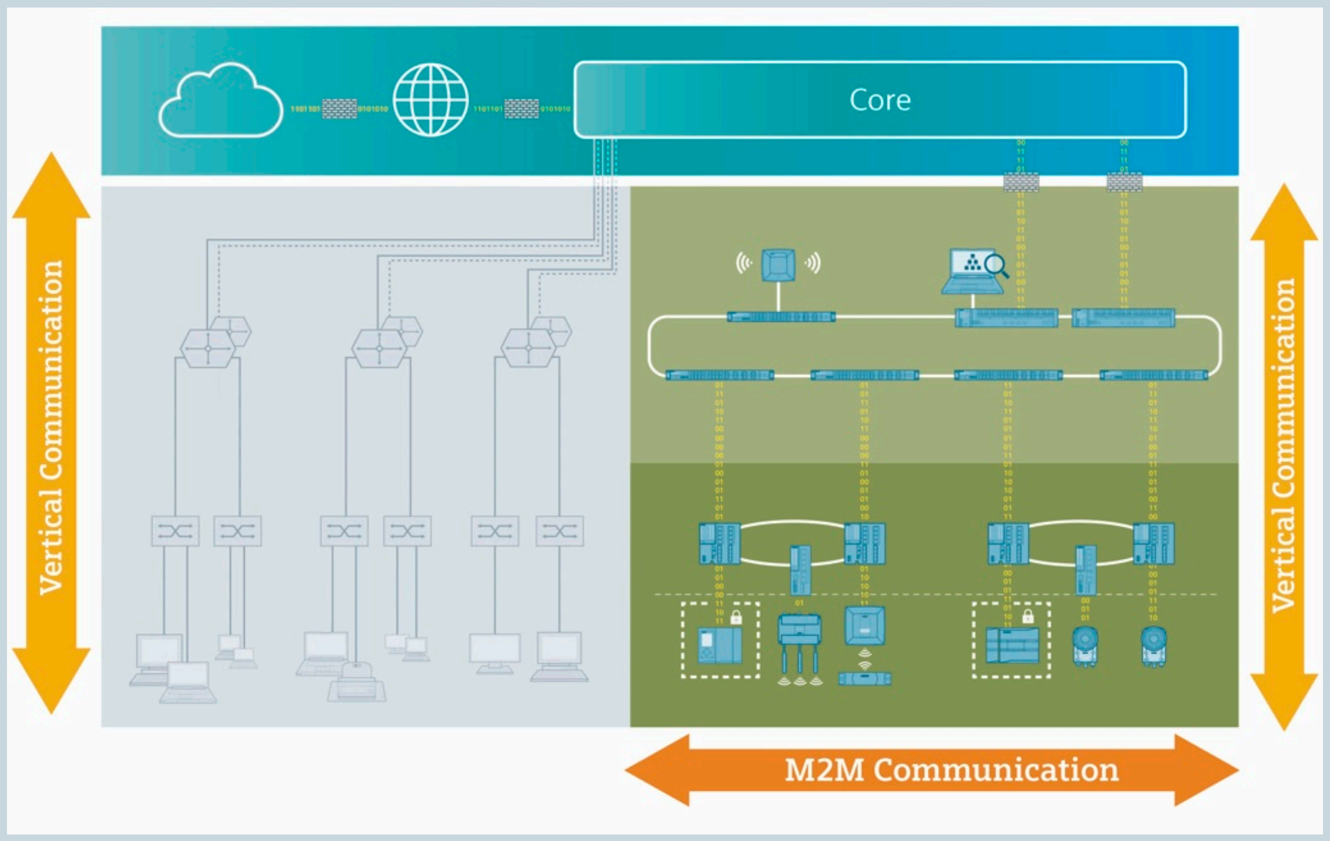
Fail-safe, protected, transparent, future-proof

Within the framework of digitalization and Industrie 4.0, an integrated and future-proof communication will represent a crucial factor in the value chain of production facilities going forward. Key here is that in light of the digitalization and ever increasing networking of machines and plants, data security is always taken into account. The use of industrial security solutions precisely tailored to the needs of industry is therefore of fundamental importance – and should be inseparably linked with the industrial communication.

Increased requirements on information, communication, and automation technologies make completely new demands on existing or to be designed industrial networks. To meet these demands relating to reliability, protection, transparency, and future-proofness, a number of aspects must be considered.

Modern production sites already create lasting value and contribute greatly to economic growth. In the face of growing global competition and increasing requirements on production environments, they need to be further professionalized. It is certain that the structures of the information, communication, and automation technologies at production sites will change significantly. Value chains are optimized through horizontal and vertical integration of all industrial processes.

To be ready for a seamless migration into the age of smart automation solutions, the existing production must already be prepared today as best as possible for the coming structures and tasks. To optimally run an industrial network, the essential aspects listed below should be taken into account:



Typical communication structure of industrial networks

Coupling of IT – two Perspectives meet

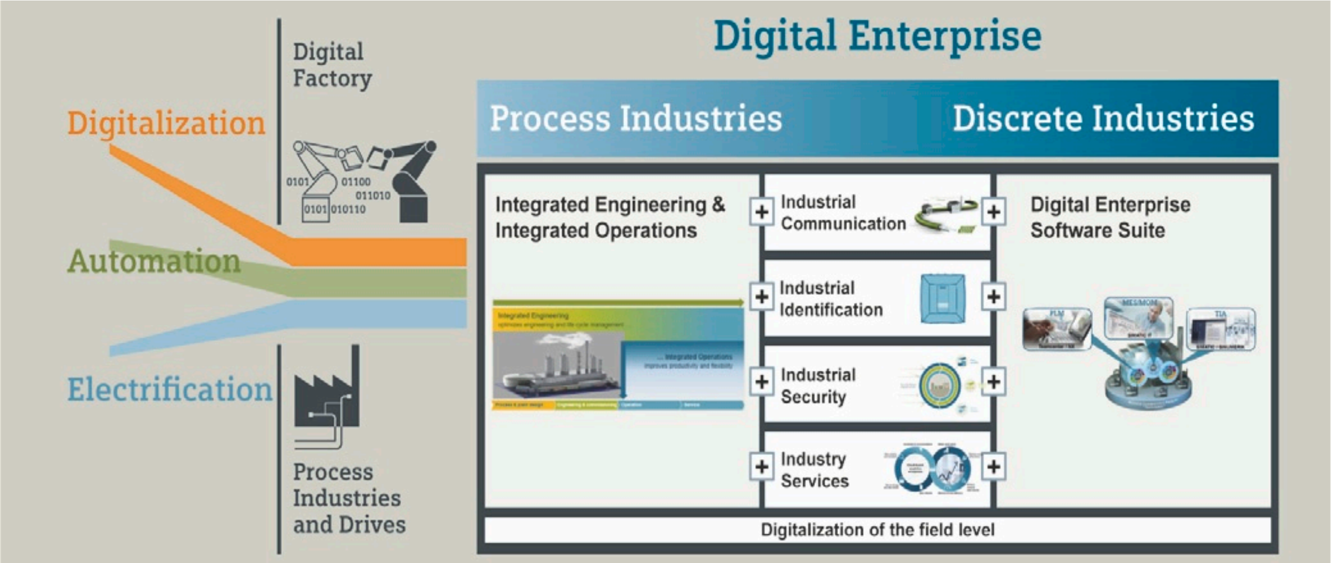
While classic information technology (IT) focuses on the transmission of telegrams, the production has its applications in mind. These two fundamentally different perspectives become evident at the latest, when the fundamentally different network components and topologies deployed in the areas mentioned are examined. Particularly in larger companies, where the classic IT and the production (OT) are attended to and planned by different departments, the coupling of both areas needs to be optimally implemented. Devices employed for this should support the necessary mechanisms and protocols with regard to production. They, however, also have to be optimally suitable towards IT, for example, through the support of CLI (command line interfaces) or the connection of IT with a 10-Gbit transmission rate. Furthermore, OT also requires functions in the industrial network that are not known to IT, such as wireless safety with Industrial WLAN, PROFIenergy, or the use in Ex-Zones in process automation.

Partners – together into the Future

On the global market, there are many manufacturers of LAN/WLAN/WAN components. When choosing a supplier, the persons in charge should ensure that the firm offers a comprehensive product portfolio for the task assigned, and also operates globally, to optimally support the expansion of one’s own company. It is also important that the production operation can be accompanied by the automation partner throughout the entire lifecycle of the plant. In many industry sectors, these cycles extend to 20 years, and then as well, the appropriate spare part should still be available.

Technology – taking added Value into Account

Despite the ever increasing cost pressure, which generally rules the purchasing negotiations, it is extremely worthwhile for the later operation of the plant to not only define the components used by price, but to develop a holistic perspective. Added value is also created by properties that can not be nominally compared: Quick and transparent diagnosability, a matching scope of functions, the interaction of different components, the construction with respect to environmental conditions, possibilities for energy saving, or high availability (i.e., minimum downtimes, high MTBF – mean time between failures) can all bring about enormous savings over the years, which at the beginning of a project are often not yet apparent.



Industrial communication and identification as well as industrial security are essential factors for the digitalization in many industry sectors

Planning – future-proof already today

Many times, a running production has to be halted during the operating phase to carry out expansions, which could have been avoided with a more farsighted planning. Networks can no longer be simply "plugged together". Nowadays, it is essential to carefully design the network.

Redundancy – coping with Errors

Faults are possible even in perfectly planned networks. In most cases, they are caused by external influences and are thus hard to avoid. The operator can gain protection by installing corresponding redundancy mechanisms, which enable the industrial network to cope with the failure of a component or cable, without affecting the communication. Frequently, the components employed already support a number of redundancy protocols. Redundancy therefore not automatically means higher investment costs.

Plant Protection – professional Security Concepts

In the field of industrial communication, the trend is towards open standard systems – away from proprietary systems. However, with the enormous opportunities also come risks. The security aspect is thus becoming more and more important. Nowadays, it is indispensable to prevent attacks on the know-how of a firm. The use of a firewall, however, far from completes the subject of security. Security is multilayered and complex. The firewall is as much part of the security as the disabling of certain services on PCs. The subject thus has to be viewed holistically. Data security not only has to be planned well, but also consistently practiced by the user. A professional industrial security concept reliably protects the production operation against faults, without hindering it. This can be achieved through a professional approach and the establishment of a security process, which, e.g., includes regular risk analyses in order to set the right priorities.

Transparency – also across Plants

Industrial networks often do not originate on a greenfield. Instead, they are constantly expanded or existing plant areas are linked with each other. Due to the increasing advance of Industrial Ethernet, e.g., by means of PROFINET, large networks with a huge number of participants can be found especially in the production. The documentation of the current situation becomes an important task here, which, however, can no longer be performed manually. This task is assumed by modern systems, which record and document the industrial network. Network structures, but also I&M (identification and maintenance) data, e.g., the firmware version, are thus always available in their current state. Thanks to the resulting transparency, weak points can be quickly located, or networks be easily expanded and optimized. Particularly web-based solutions have the advantage here in that the information obtained can not only be accessed locally, but also by other plants.

Diagnostics – minimizing Downtime

Diagnostics is often perceived as a burden, since it initially does not represent an added value in the production process. At the latest, however, the benefit of the diagnostic tools implemented can be financially measured, when downtimes in the industrial network have been reduced or even been prevented. Diagnostic tools that continuously monitor the network have now become almost indispensable. Problems can thus be corrected before they lead to a failure. For instance, badly laid cables can quickly result in incorrectly transmitted telegrams, which, however, do not directly cause failures. In this case, production pauses can easily be utilized to remedy the problem. It is also important to use tools that can be integrated well into the existing HMI/SCADA landscapes. Only then can it be ensured that messages or fault notifications are not lost or noticed too late. Diagnostics thus considerably increases the availability of plants.

A holistic industrial security concept for the protection of production facilities against errors, unauthorized access, and data loss is a mandatory prerequisite for the digitalization

Management – keeping the Network up-to-date

Once a network is in productive operation, the management aspect of the network components comes to the fore. For firmware updates or changes to parameters, only small timeframes are provided in this phase. These maintenance windows therefore must be utilized effectively. Network management tools, in which tasks such as firmware downloads or parameter changes can be planned in advance, make it possible for networks to always be matched to the current needs.

Know-how – Focus on Employees

Industrial networks – also in production-related environments – are becoming increasingly complex, but at the same time also offer many more diagnostic possibilities. Despite the cost pressure, especially with regard to personnel, the focus should always be on training employees. Problems can not only be corrected by reading an error message. Rather, basic knowledge of the technology used often helps in recognizing relationships – in order to independently evaluate faults and provide a remedy. The subject of security thus also has to be precisely tailored to the industry sector and the employees, because industrial security solutions are of fundamental importance today, tomorrow, and the day after– and should be inseparably linked with the industrial communication.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

© Siemens AG 2016
Subject to change without prior notice
PDF
Technical article
FAV-391-2016-PD-PA
BR 112016 En
Produced in Germany

The information provided in this brochure contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.
All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

siemens.com/industrial-communication