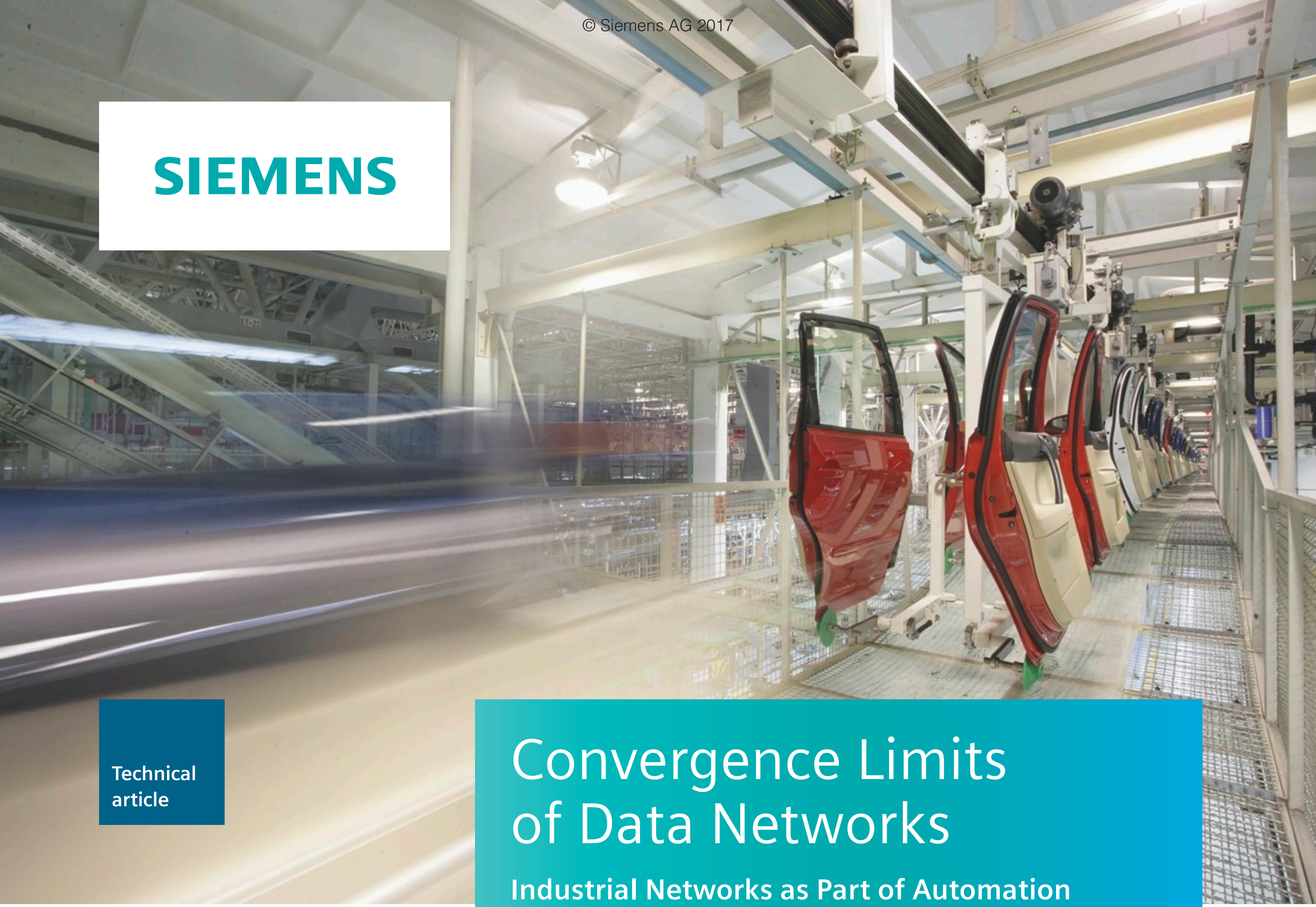


SIEMENS

Technical article

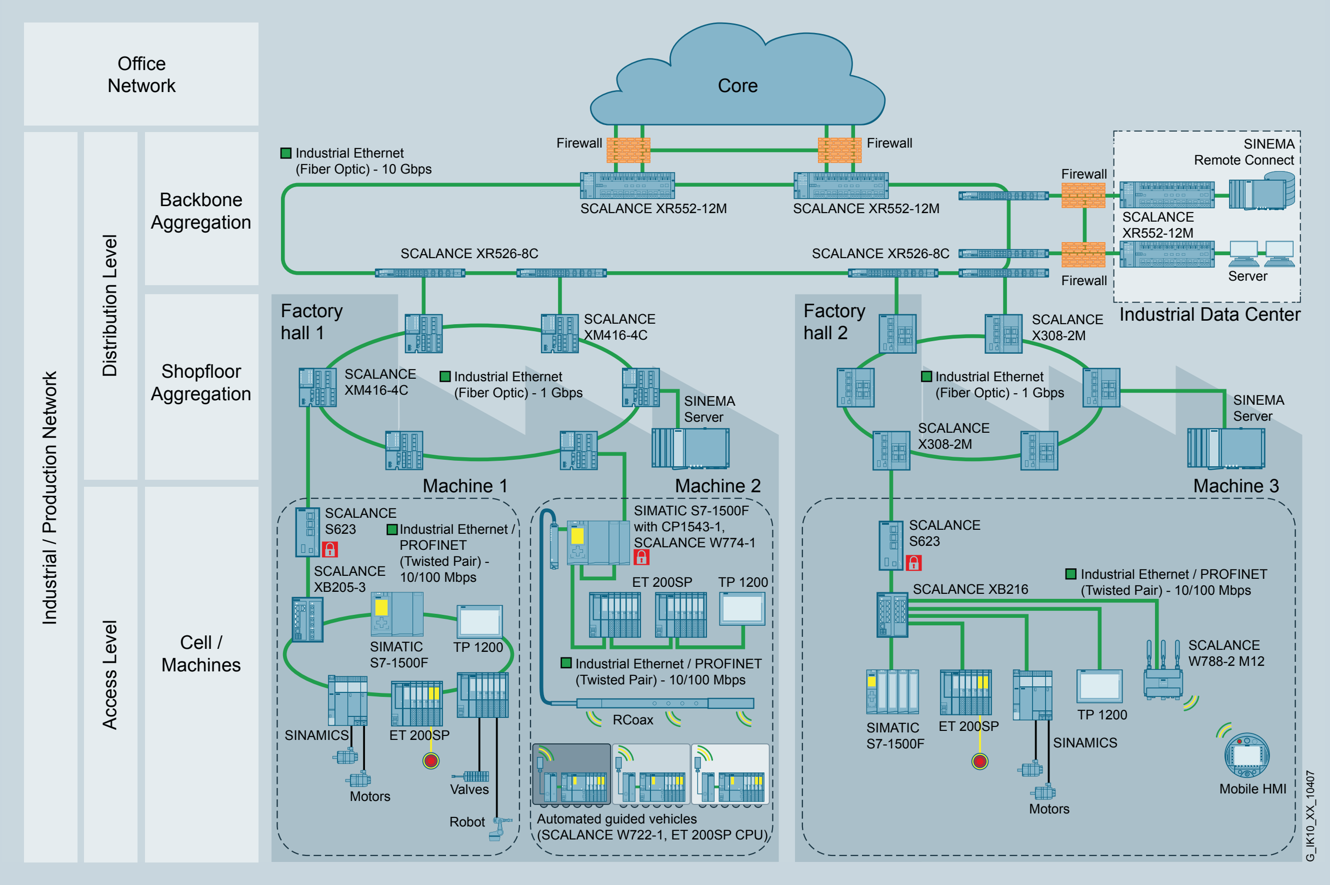
Convergence Limits of Data Networks

Industrial Networks as Part of Automation

The well-thought-out connection of office and data center networks to automation networks is a major challenge for companies – especially in view of the tasks involved with the digitalization of industry and the accompanying comprehensive networking of all corporate areas and the extensive exchange of data. Experience shows that not every Ethernet-based network can be planned, implemented, and operated in the same way – and an inappropriate approach to achieving complete network convergence can turn out to be very costly for customers.

Since more and more companies today rely on Ethernet-based communication in industrial networks, special network designs – geared towards the requirements of the applications – have found their way into various industry sectors. Many IT departments are attempting to implement the connection required for the production networks using well-known procedures for the design and operation of office networks, break up existing industrial network structures, and integrate the automation devices into the existing IT infrastructure. However, this entails substantial risks for the companies.

First of all, it should be noted that experienced providers consider the industrial network to be an integral part of the automation – and choose an entirely different approach to tackling greenfield and brownfield projects as compared to the planning of office and data center networks. The goal is to combine functional data exchange with failsafe automation.



Schematic diagram of industrial network infrastructure for a manufacturing company with discrete production, e.g. in the automotive industry, with connection to the office IT.

Structural and technical characteristics of an industrial network

Industrial network infrastructure differs depending on the specific requirements of the individual industry sector.

In manufacturing companies, for example, the relevant areas of the industrial network part – depending on the network structure – range from the cell level and machine level (also called the access level) to the distribution level with the cell aggregations (including the shop floor aggregation, hall or station aggregation), and the connection of a possible industrial data center to the backbone aggregation. The latter, in turn, must be connected to the core area of the corporate network comprising the data center network structure via suitable interfaces and taking the security policy into consideration.

The data flow

The data flow in industrial network infrastructure is characterized by horizontal and partly by vertical communication. In contrast to the purely vertical client-server communication in office IT, in many industrial networks data is exchanged directly between devices (horizontal communication). The vertical communication also differs to some extent, for example between a device and a controller.

Cyclic communication with deterministics, clock synchronicity, and very low jitter[1] is a key prerequisite for industrial control components to operate smoothly. This requires a continuously active communication connection which does not, however, exist in any other part of the company's IT in the case of client-server-based Ethernet communication operating according to the "best-effort principle". As a rule, an industrial plant must function without interruption, i.e. ensure a high degree of availability over a long period often exceeding ten years. The design of the industrial network with rugged components and suitable redundancy procedures, such as seamless redundancy for motion applications or system redundancy for process applications, provides the basis for the increased availability of a production plant and can even maintain the operation in case of a fault.

[1] Unwanted variation in frequency during the transmission of digital signals

Service or troubleshooting

If service or even troubleshooting become necessary despite best efforts, an industrial facility cannot generally be restored quickly enough under the usual IT SLAs (Service-Level Agreements). Even constantly available service may not be enough if a response time of between two and four hours is defined in the SLA. What matters is fast restoration, i.e. that the plant runs smoothly again within the shortest possible time. Especially in complex network infrastructure fast and simple fault localization is not possible without the use of suitable integrated diagnostic and monitoring tools that automation personnel can also operate. The tools must also monitor all relevant end devices connected – including control and drive units and peripherals – and not just be restricted to infrastructure devices such as servers and switches. What is the benefit?

In order to replace defective components and bring them back into operation as quickly as possible, it also makes sense to also arrange the aggregation networks, such as the industrial backbone, directly in the plant – thus keeping the service path and the response time low. The ambient conditions in a production facility, a distribution station, or a filling or transfer line differ greatly from the climatic conditions in a data center or office. It therefore goes without saying that rugged components, for which spare parts will be available even after many years, must be used.

Rugged access point; version designed for special environmental requirements and use on buses and trains.

To ensure plant availability, a hotline familiar with the entire plant should be available at all times. Experience has shown that a homogenous concept and focusing on a single automation manufacturer greatly facilitate fast and effective solutions for control and network components.

Outsourcing and personnel

The outsourcing of office IT has become common practice for many companies. However, in order to ensure the necessary high availability of industrial facilities, the corresponding networks are hardly ever outsourced. Employees of the company itself are responsible and capable of handling maintenance work and malfunctions – and spare parts for particularly critical areas are kept on site.

Furthermore, when planning and operating industrial infrastructure, care must be taken to have enough trained personnel available on site to ensure trouble-free operation. Not every company is able to have IT professionals available at all times. It therefore comes as no surprise that the contact persons are typically automation experts with IT knowledge and not IT specialists. Considering this, the network technology should be designed in such a way that it can also be handled by trained automation technicians, since "non-IT specialists" often have to service individual components.

In any case, this role must be filled by skilled personnel who can form an interface between automation technology and IT and serve as a competent contact for both sides. Besides the wired industrial IT architecture, this role also involves the management of radio channels (WLAN, BT, Wireless HART, ...) in industrial environments.

Safety and security

In industrial environments a distinction is made between safety – that is functional safety, and security – i.e. data security.

Safety covers all the functionalities that serve to protect people, machines and plants. In an emergency it must be possible to transfer individual machines, plant segments, or entire plant complexes to a safe state. This requires fast and direct data transmission to the critical control elements. The safety signals must be reliably transmitted with the highest priority independently of the media used. If network sections are implemented with "emergency stop" functionality, the corresponding network connection must be ensured – in both wired and wireless network infrastructures (such as Wireless LAN). To meet the security requirements of industrial networks, special cell protection and firewall concepts, for example, need to be implemented. These must protect each production area against unauthorized access. Especially for sensitive remote access, professional security concepts are required, for example in order to perform maintenance work on defined plant sections according to clearly defined rules. Version management also differs from the typical office IT: Patches for industrial plants must be loaded within the time slots scheduled for maintenance, because updates during operations can result in critical performance losses. For example, unplanned network scans can unintentionally bring entire plants to a standstill.

Considering all these aspects, an integrated network concept based on a physical network separation with a connection concept fulfilling both security and performance requirements is highly recommended for a failsafe industrial plant. Users should treat convergence concepts that simply integrate the industrial network like any other logically separated network, or do not even provide a VLAN separation, with the utmost care. As has been proven in countless industrial applications, the network – as part of the automation – plays a crucial role for smooth operations. It is therefore of prime importance for the success of industrial companies that industrial networks are planned and implemented on the basis of key criteria.

Properties of industrial network components

- **Increased plant flexibility and cost savings**
  Clear ring and line network structures with compact devices in the plant ensure high flexibility and reduce maintenance and service costs.
- **Investment protection of existing plants**
  Long-term spare parts availability and modularly expandable active components ensure the long service life of existing plants.
- **Investment protection of future plants**
  Future-proof technologies and the continuous further development of available products ensuring end-to-end compatibility. Innovative technologies specifically designed for tasks in industrial environments.
- **Optimum machine and plant availability**
  Maximum reliability of the products during operations. Plus service and support around the clock (24/7), worldwide.
- **Reliable planning and know-how protection**
  Long product life and availability safeguard long-term plant concepts and ensure the use of employee know-how.
- **Compatibility**
  Consistent products and accessories enable the integration of additional components for extensions allowing the establishment of a complete industrial infrastructure.
- **Worldwide use**
  Industrial network devices with worldwide approvals.
- **Developed for our customers**
  The development processes of components and services already consider future applications and solutions during the planning stage. This means that our products are always easy to integrate and have been implemented and tailored to the needs of users and end customers.

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 2017
Subject to change without prior notice
PDF
Technical article
FAV-285-2016-PD-PA
BR 022017 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-networks