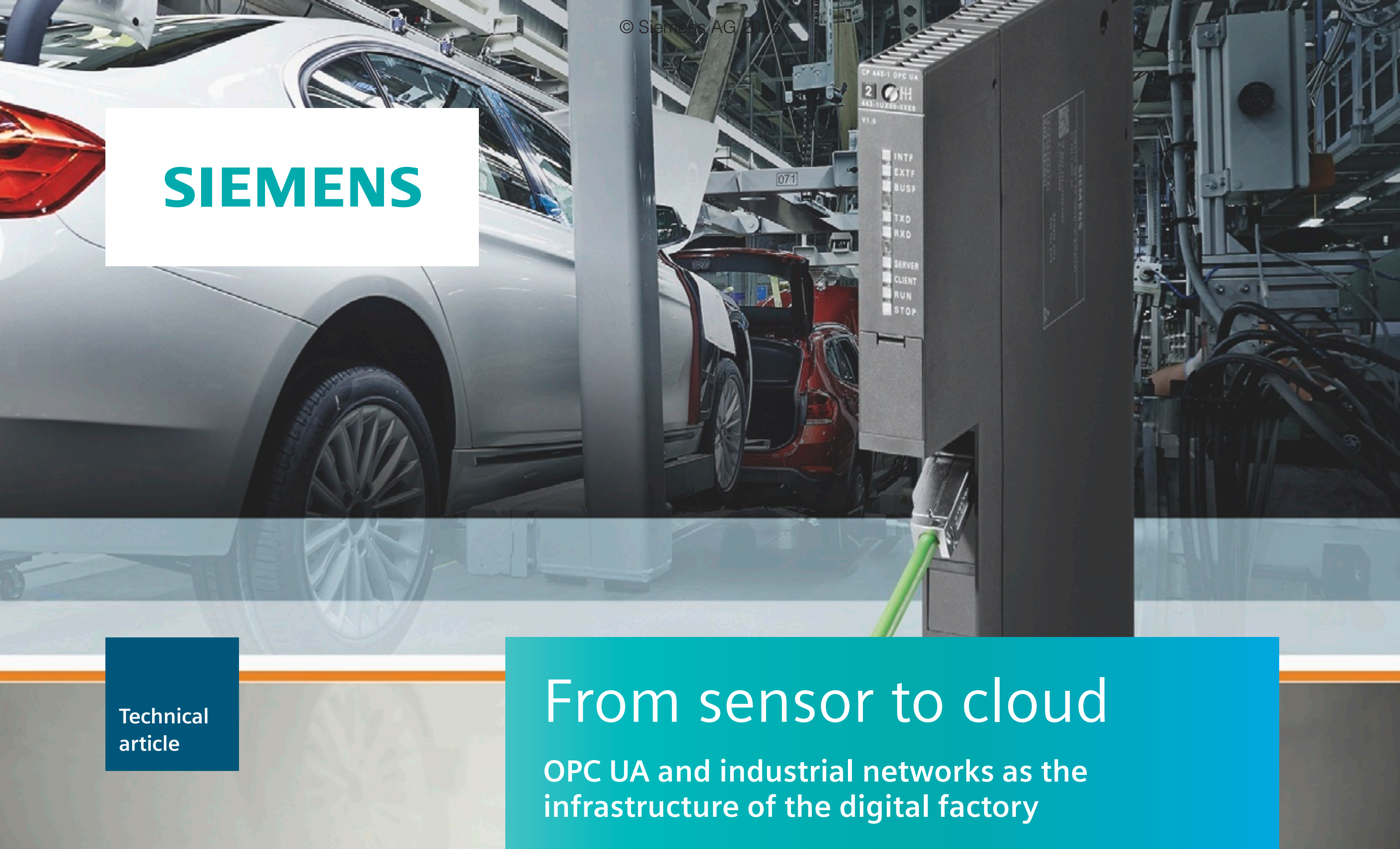


SIEMENS

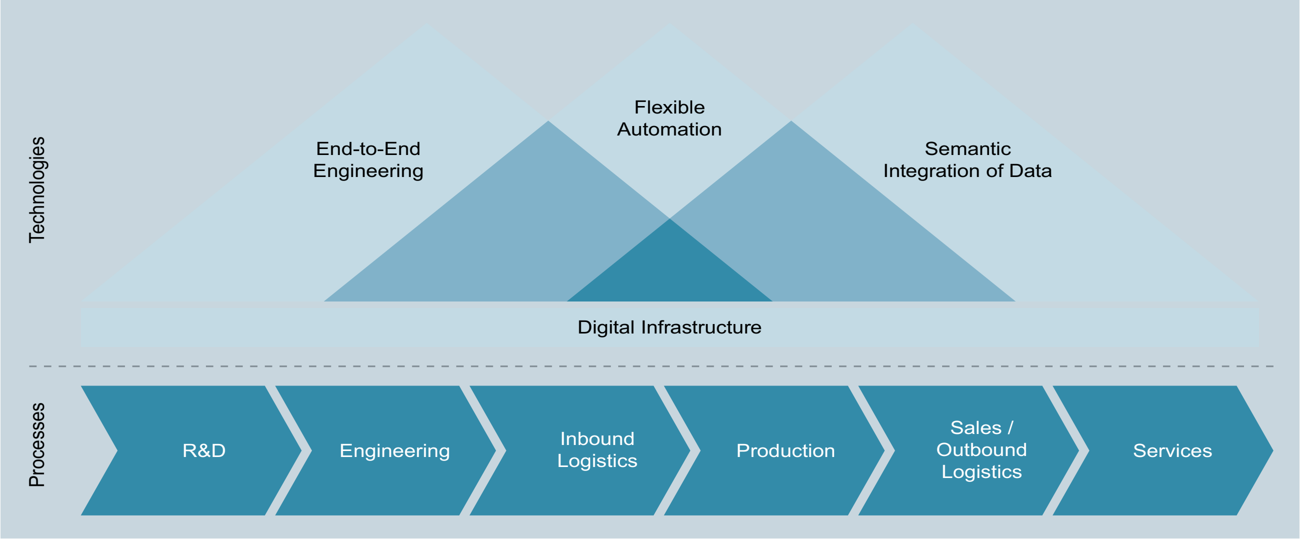
Technical article

From sensor to cloud

OPC UA and industrial networks as the infrastructure of the digital factory

The integration of different systems into an IT or automation infrastructure is complicated because there are no standardized interfaces and protocols. So what sort of communication architecture is required for networking the ten-thousand devices in the digital factory? In this respect, industrial networks and the OPC Unified Architecture are regarded keys to the digital infrastructure.

The extent of the challenge becomes clear when one considers the application scenarios in the digital factory in closer detail. These can be divided into three areas



The essential technology areas of the digital factory require a common digital infrastructure.

siemens.com/industrial-communication

Firstly, the end-to-end engineering means that the data from product design can be used for the production engineering, to create control programs, for example. This enables different aspects of an event to be recorded and developed in a standardized data model, which simplifies changes, helps to avoid errors, and considerably reduces the engineering times, including the time required to implement production.
Secondly, flexible automation is aiming to resolve the (apparent) contradiction between flexibility and automation, in order that a variety of products can be manufactured in the same plant. Collaborative robots, which assist their human colleagues, are one example of how the consistent performance capability and precision of a machine can ideally complement the human capabilities of handling complex and dynamic situations. This aspect includes such new production methods as 3D printing.
And thirdly, with the collection and integration of data across the entire life of a machine, new services become possible, for maintenance purpose, for example.

Vertical and horizontal integration

Present-day solutions usually follow a typical "automation pyramid" pattern. In other words, the individual layers, from the sensor, via the controller and HMI level, to the MES and ERP system, are hierarchically constructed and often permit no direct access from the top level systems to the layers further below – unless explicit routing through the intermediate layers is provided for this purpose.

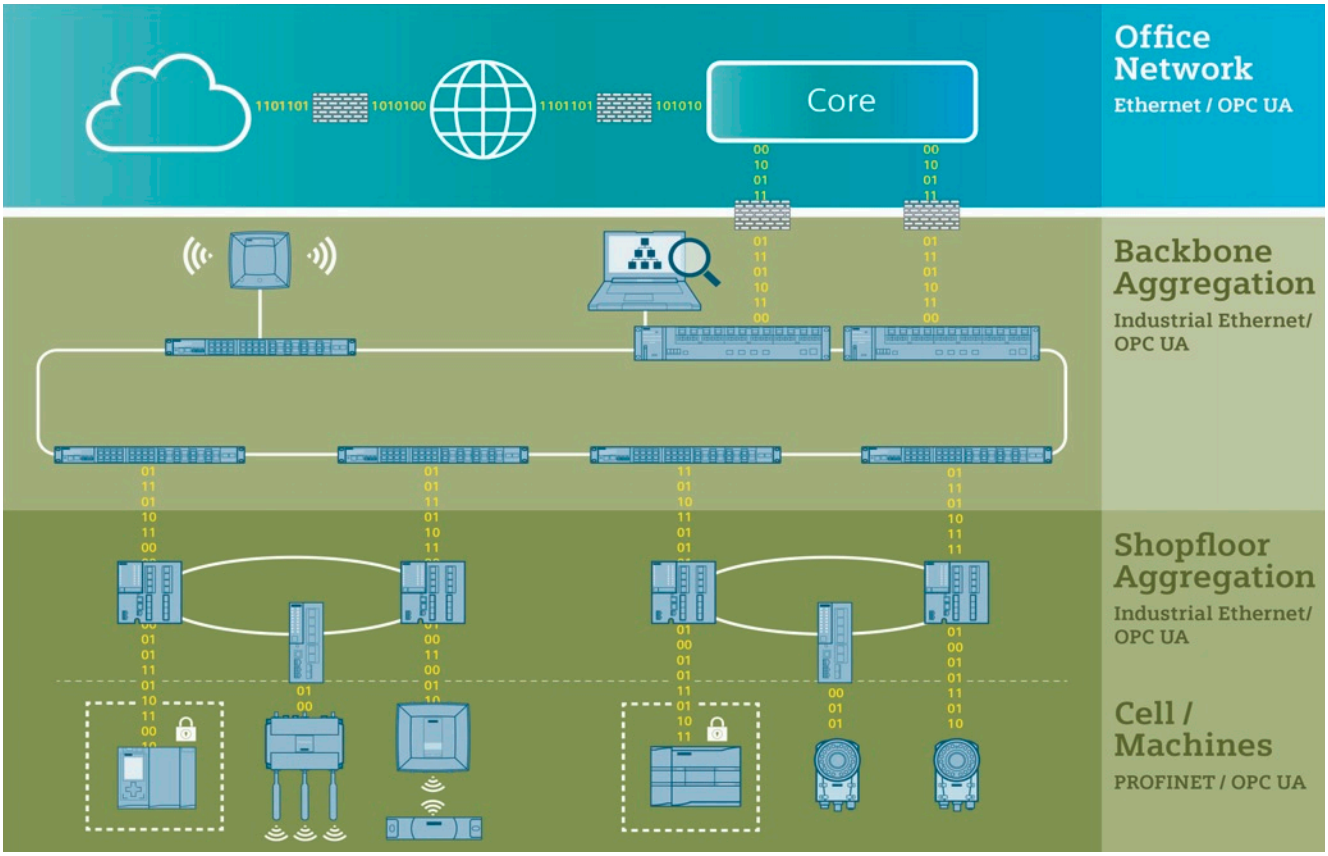
The digital factory, on the other hand, emphasizes the horizontal integration (that is, between components on the same level) and the vertical integration (communication between layers) of the communication levels. On the one hand, this breaks up the previously rigid cellular organization in the digital factory (for example, by means of freely mobile, autonomous robots); the machines therefore need an information infrastructure that is no longer organized on a strictly hierarchical basis, but takes into account the respective, dynamically changing environment.

The integration of data as a source of information for analytical, data-based services leads, on the other hand, to the breakup of the horizontal layers. Because in order, for example, to gain new insights for predictive maintenance, a high density of data is necessary at all levels, starting with design and engineering, through quality data in production, to sensors that deliver their measured values to the IT systems (cloud) when a machine is used. Under certain circumstances, this data is not relevant for the PLC that controls the production machine, or would misuse the resources of the controller for data routing exclusively. It is therefore reasonable that, although the sensors act on the one hand as a source of information, on the other hand they deliver their results directly to the data pool in the cloud in different cycles, resolutions or with different measured values.

Ultimately, such as digital factory may be imagined, not as an unchangeable system, but rather as an organism that continually adapts itself (autonomously or by means of engineering) to the new requirements. Accordingly, such an architecture must be flexible and easy to maintain, in order that the complexity can be intelligently mastered.

Demands on the data networks

The communications infrastructure that is necessary as a basis for the architecture outlined must therefore satisfy different requirements. On the one hand, properties such as the use of open standards, availability, quality of service and, above all, security are demanded that already characterize an Industrial Ethernet today. As on the other hand, however, the connection to IT systems for data-based services and an increased transparency across all levels are required, a link between office and production networks is necessary. Although this ensures the performance in the Industrial network by means of safeguarding mechanisms, it nevertheless permits access to all layers, devices and components. This points to the use of different aggregation stages and the introduction of a factory backbone as a network topology. On the one hand, this permits fast communication between the devices in the individual cells and, on the other hand, it ensures a high-performance link between office network and the various sub-areas.



Different aggregation levels and a factory backbone in a ring structure form the "Industrial Network Topology"

In order, however, to meet the aims and requirements of the digital factory, an end-to-end network topology is simply not enough. What is required is a communication protocol that is open and standardized, provides sufficient semantic information and translation options, is easy to expand and maintain, offers maximum security in various different versions, and also has memory and processing requirements that are low enough to be implemented on small devices.

Communication architecture for the digital factory

The answer to these demands is the Unified Architecture protocol of the Open Platform Communications Foundation (OPC UA). The most important thing about OPC UA is that it is not only a protocol, but also a complete architecture that provides software stacks suitable for the transmission definition for device and software suppliers, as well as engineering tools for the system integrators. In this way, OPC UA offers major advantages. Firstly, the information model ensures that all data is transmitted on a type-safe basis. Even complex data types (structures) are possible. Apart from the exclusively data values, OPC UA also transmits semantic information between the communication partners.

As the architecture functions on an object-oriented basis, the semantics are woven into an object context – thus comprising more than just a "speaking" identifier, but always referring to the overall object with its properties and methods. Function calls via the network permit a certain amount of control over the communication partner. Finally, events are supported as ad-hoc communication or message brokers for the connection to the cloud.

The fail-safe nature of the implementation is enhanced by interfaces that introduce their specification to the engineering environment (browseable interfaces). For each device, a description file can be imported into the engineering or read from the device available online that offers a detailed specification of the interface. The correct use of the interface in the user program is ensured by the development tools. Another key point is the protection against unauthorized access. As a defense mechanism, for example, OPC UA uses X.509 certificates and corresponding security protocols.

For actual use in different applications, industrial associations collaborate with the OPC Foundation on "Companion Specifications" that supplement the standards of OPC UA for a specific domain. One example is the collaboration with PLCopen, in which the shared block and access procedure for data has been defined in a programmable logic controller (PLC). Suppliers such as Siemens integrate these mechanisms to enable the integration – based on OPC UA – of the controller, for example, with devices from other manufacturers or with PC/IT systems. For example, the CP 443-1, which is used as a connection module in the SIMATIC S7-400 system, supports the client and server functionality of OPC UA. In this way, other systems can access the data areas of the SIMATIC S7-400 CPU, previously released in the engineering phase, via the standardized interface. Thanks to this module, existing plants can be retrofitted with OPC UA communication options.

Until OPC UA can be used as an integrated communication architecture, however, further standardized tasks must be completed, as some areas of industrial communication are not yet fully covered. For example, on the level of the sensors, only a few series of devices, or technologies such as radio frequency identification (RFID) systems, are specified for OPC UA. In addition, definitions are required at a higher level if it is no longer to be a matter of technical parameters, such as the transmission power of an RFID reader, or the access to process data exclusively. Instead it will be necessary, to standardize functional characteristics according to industry and application which correspond more with the engineering context of the plant engineer and less with that of the software designer.

Yet, apart from these future tasks, OPC UA today is a unique communication architecture in terms of its scope and is indispensable for the vertical and horizontal integration within the digital factory.

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 **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-407-2016-PD-PA
BR 092016 En
Produced in Germany

siemens.com/industrial-communication