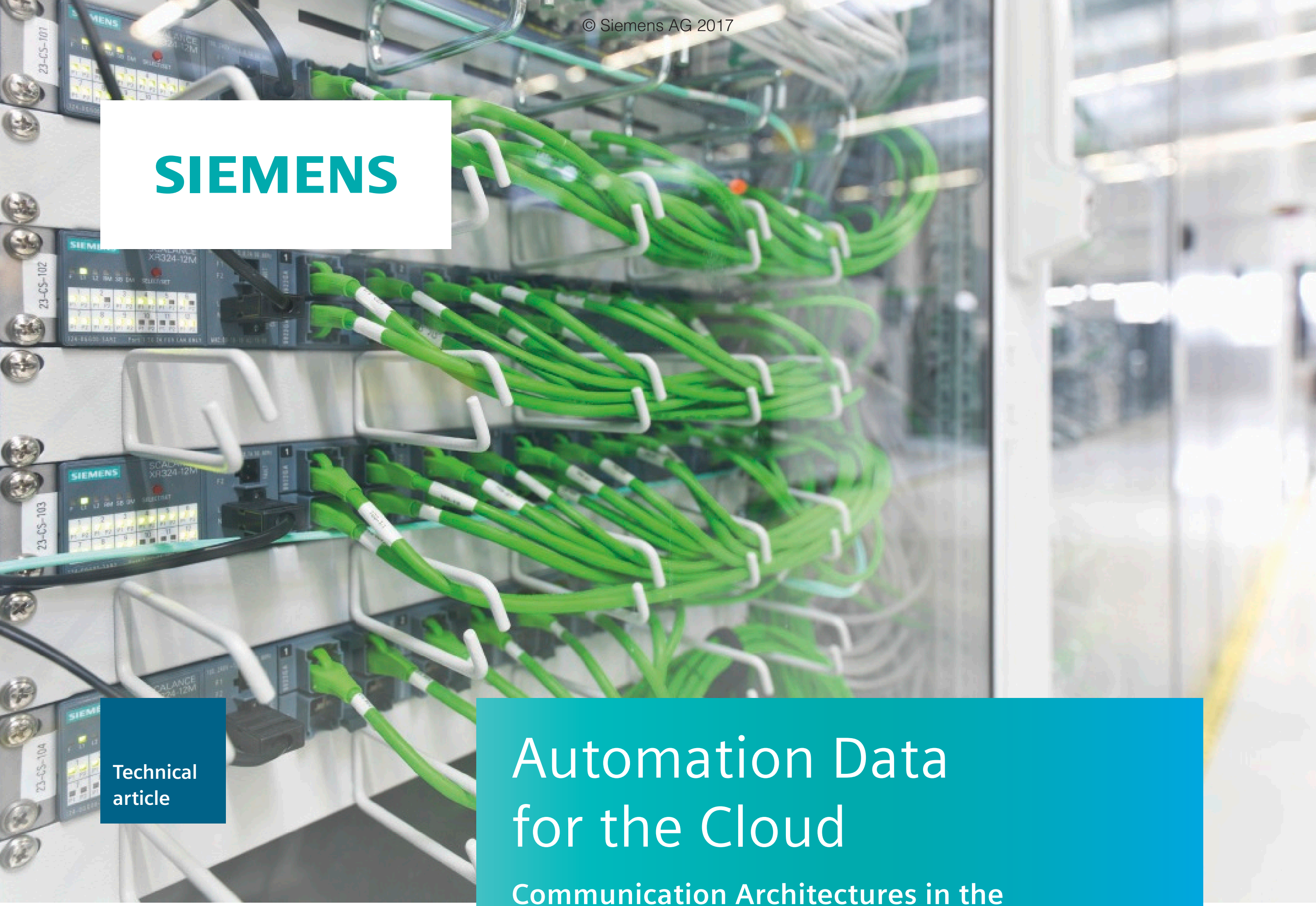
SIEMENS



Technical article

Automation Data for the Cloud

Communication Architectures in the Industrial Internet of Things

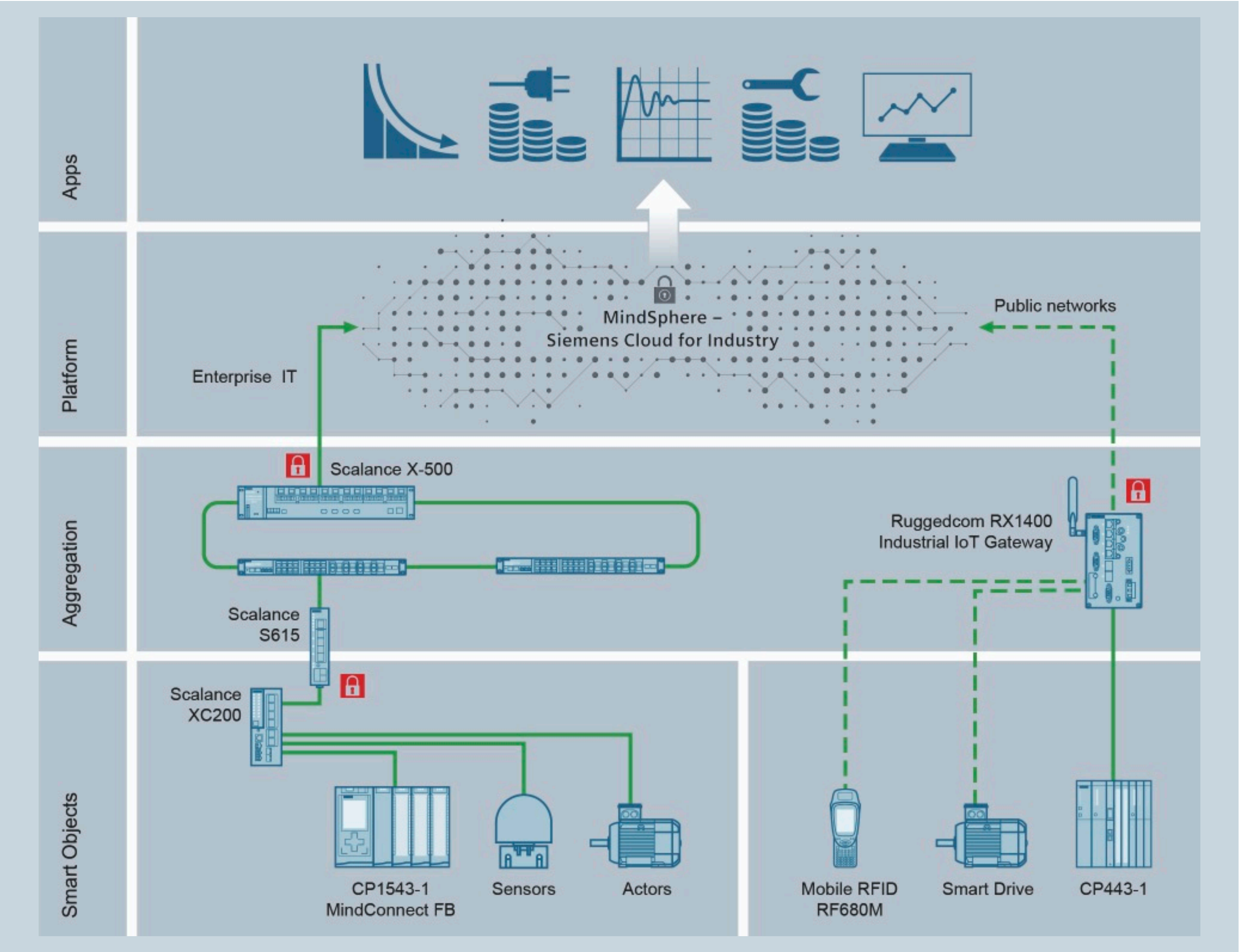
Cloud computing and the Internet of Things promise interesting possibilities – from process design to new business models – also for industrial companies. Prerequisite is a sufficiently wide database, which is transmitted from the field level to the cloud. This, however, requires a powerful, secure and flexible communication architecture.

So the idea is to transmit the sensors of the field level – which, e.g., monitor temperature curves, vibrations and power consumption of a machine – to the virtual evaluation platform, the cloud, as basis for big data algorithms. A direct connectivity of the sensors to the cloud via the Intranet and Internet, though, seems rather difficult in practice. Many sensors today are not even Ethernet-enabled, instead they transport the measured values to a programmable logic controller (PLC) via a current interface (4 ... 20 mA). Modern sensors may offer an IO-Link interface, which is also not cloud-capable, and therefore must first be compiled into the corresponding protocols – including the routing capability – by means of a master module and a gateway. Even if the sensor system came with the necessary Ethernet interfaces and protocols, several thousand Internet connections from the field to the cloud would be very difficult for IT administrators to control – not to mention the vast amounts of data without a clear business case that would have to be processed in the cloud.

It therefore makes more sense to provide an aggregation unit on the control level that compresses the data and bundles the information from the large number of sensors. From the automation point of view, this task can optimally be carried out by the PLC, since most of the sensor data accrues there anyway, e.g., for machine monitoring. In addition, the PLC already performs its own compression, e.g., through logical or arithmetical linking of the data.

In order to realize the communication from the PLC to the cloud, there are basically two approaches with specific advantages. On the one hand, IoT gateways can be used. These devices possess two logical units for data acquisition and communication to the cloud. The acquisition part is used to cyclically query the data to be transmitted from the field level, primarily from the PLC. The Ruggedcom RX1400 industrial IoT gateway from Siemens, for example, offers the Simatic S7 protocol, which allows the query of data without prior adaptation of the automation program – the ideal solution for existing plants. For other device types, the RX1400 also supports OPC UA on the field level; besides Ethernet, the data can also be transported via WLAN.
For the transmission to the cloud, the gateways support various communication protocols, e.g., for the connection to MindSphere. Furthermore, gateways are useful with regard to the security of the communication networks, since the cloud connection can take place via a separate network path.

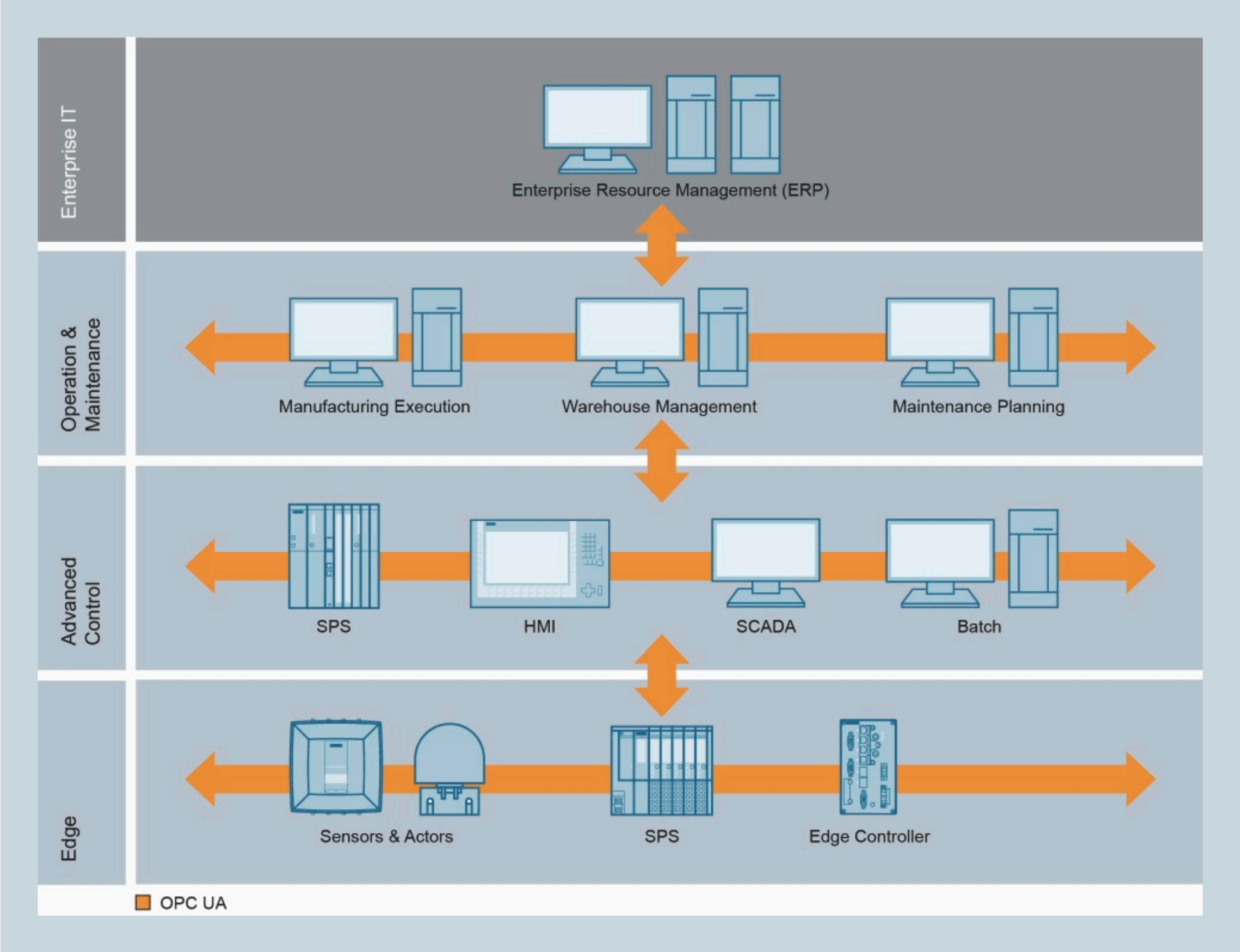
As an alternative, controllers can also offer intrinsic cloud connectivity. Although the automation project has to be adapted in the process, the possibilities are much more diverse. For instance, information about the context of the cloud data is available in the PLC, e.g., whether a machine is starting up, is operating normally or is in standby. Derived from this, different data can then be transmitted, or the cycle time for the transmission be dynamically adjusted – tight time periods during startup, rather sporadic status reporting in standby mode. This helps reduce the communication load and avoids flooding the cloud with irrelevant information noise. For these reasons, MindConnect FB provides the corresponding communication blocks for the SIMATIC S7-1500 PLC and the MindSphere operating system, which are configured and programmed in the TIA Portal. This also means that the engineering data for the cloud connection is automatically contained in the project backup and can be duplicated on other controllers – an important advantage for manufacturers of standardized machines.



Possible variations for the cloud connection: With MindConnect FB and CP 1543-1 (left) or an industrial IoT gateway such as RX1400 (right)

Security against attacks remains of utmost importance when it comes to intrinsic communication. Although the MindConnect FB library already features an encrypted transmission of data, the use of a separate communication module is recommended for maximum security, e.g., the CP 1543-1. This plug-in module for the SIMATIC S7-1500 decouples the cloud communication from the automation network as it provides a separate Ethernet interface.
To fend off attacks on the CP, a firewall is integrated into the module. Denial of service attacks (DoS attacks) on the automation network can thus be averted.

In addition to the actual communication architecture, the information design has to be considered as well, put simply, this means the protocols to the cloud. From the perspective of a data analyst, proprietary data formats for devices or manufacturers are to be avoided at all costs to avoid complex normalizations in the cloud. Furthermore, it is important to also transport the semantic context of the PLC data to the cloud, i.e., the identifier, the data type and the location in the object model – only in this way can the connection be realized failsafe and with little effort. To this end, a common language in the IIoT is required, which preferably is supported by all devices in the same way. The Unified Architecture of the OPC Foundation (OPC UA) offers the best conditions for it. OPC UA is non-proprietary, can be deployed on a variety of hardware platforms and operating systems, offers comprehensive services ranging from the dynamic exploration of a device interface to powerful security functions, and above all is supported by a broad alliance of manufacturers.



As a common language, OPC UA can integrate all levels of the IIoT

Decisive for the success of OPC UA, though, are industry-specific and application-specific supplementary standards, so-called companion specifications. This is where manufacturer consortia or industrial associations together with the OPC Foundation formulate specific versions of OPC UA – to really make the different devices or applications interoperable.

An example: The manufacturer of a temperature probe can of course integrate its own object model into the sensor. But what is the symbolic name – “Temp”, “Temperature”, or just “t”? Is the value output in degrees Celsius, degrees Fahrenheit, or Kelvin? Is it an integer or a floating point value? Determinations of this kind are made in the companion specifications; only then does OPC UA become truly IoT-capable.

One such companion specification was developed for AutoID devices (RFID or optical codes) by manufacturers such as Siemens and Harting together with the OPC Foundation. At the Hanover Messe in 2017, the OPC Foundation convincingly demonstrated the interoperability between the Simatic RF600 RFID reader from Siemens and a device from another manufacturer.

The development of these supplementary standards, though, is relatively complex and requires a group of manufacturers that jointly pushes forward the work. It will therefore still take some time until a comprehensive OPC UA modeling for all devices and objects of a factory becomes available.

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
Germany

© Siemens AG 2017
Subject to change without prior notice
PDF
Technical article
FAV-295-2017-PD-PA-V01
BR 1017 / 4 En
Produced in Germany

The information provided in this catalog 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. Availability and technical specifications are subject to change without notice.

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