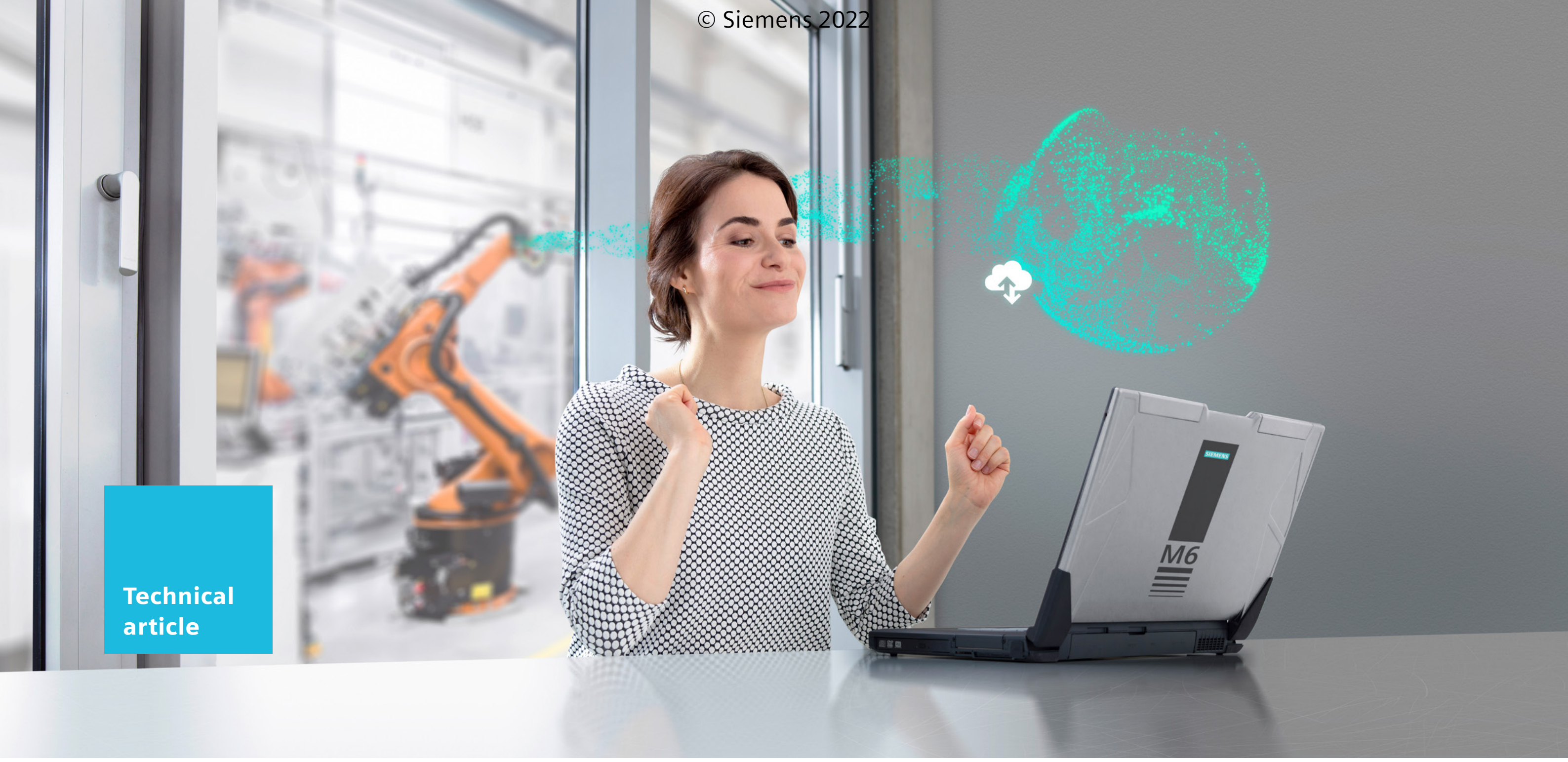


Many roads lead to the cloud

Proverbially, many roads lead to Rome. It is similar when it comes to the data transfer to cloud solutions. In order to generate added value from data, it must first be collected and transferred. The possible solutions involved are as diverse as the requirements of the various automation systems. And data security always plays a pivotal role.

IIoT and the cloud

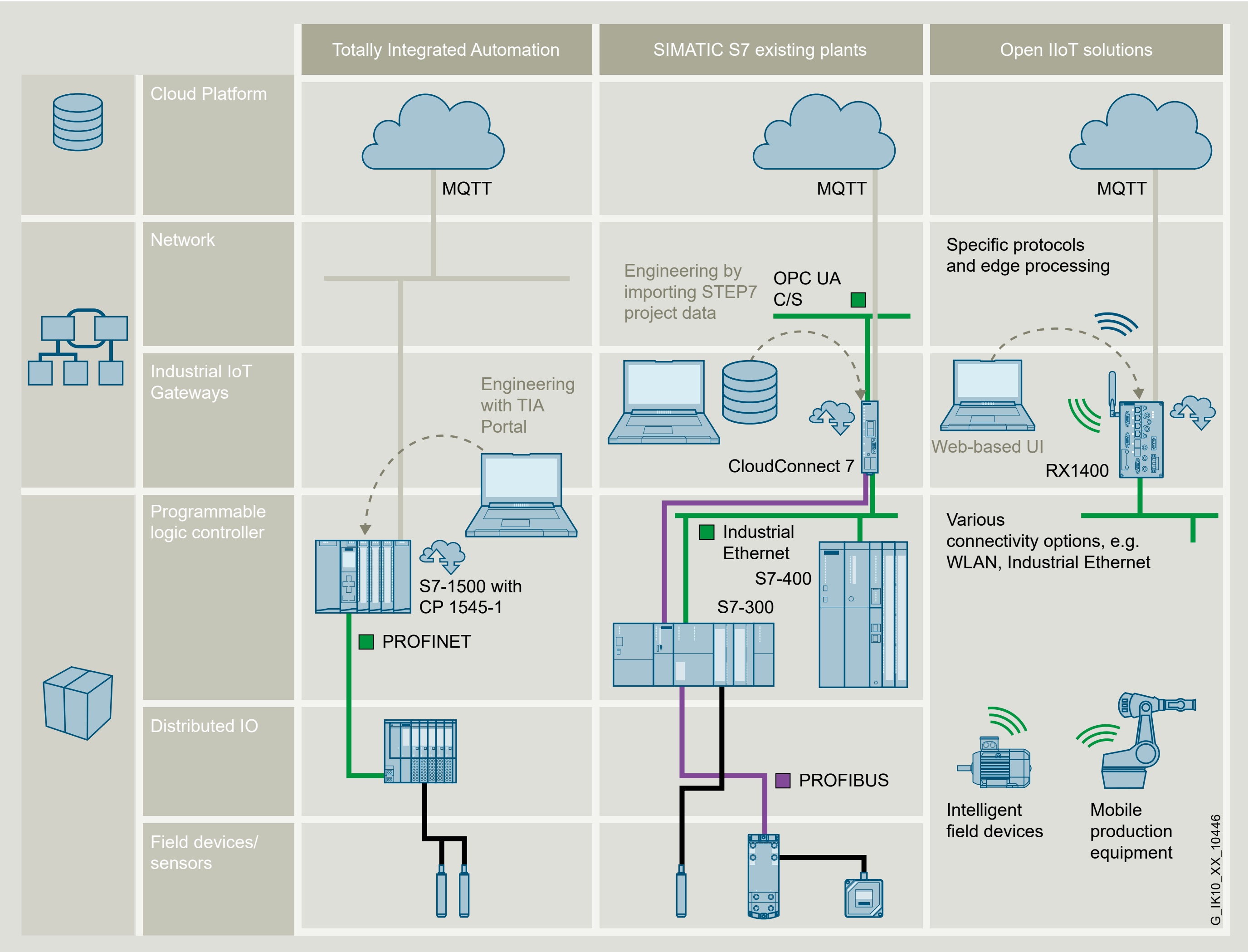
Two essential characteristics of digitalization are an increasing degree of networking of industrial plants as well as a rise in decentralized intelligence: in an industrial plant, more devices are capable of delivering data apart from their intended purpose. At the same time, this extra amount of data can be transferred faster.

In order to harness these data generated in the “Industrial Internet of Things” (IIoT), i.e., to create knowledge and economic benefits from the data, flexible and scalable storage and computing capacities are required. Providing these properties are cloud-based systems – such as the open MindSphere IoT operating system from Siemens.

Should all available information be directly transferred to the cloud? This is only partially recommended. Where previously the question was "how to even generate the required data", the question one should increasingly ask now is "where does a precompression of data make sense". Although the bandwidth made available by the infrastructure often increases, it is not necessarily by as much as the increase in the amount of data. Forward-looking planning can help avoid future bottlenecks. In this regard, a solution integrated into the plant controller offers advantages. For instance, data can be preprocessed here – the controller acts as a data concentrator, thus helping to avoid unnecessary network loads. In addition, a communication processor with security features can complement the concept, as presented below.

On the other hand, in some cases, most likely existing facilities, you might not want or are not able to change the actual controller program. In this case, a separate device can offer the needed connectivity options while leaving the engineering system untouched.

So, data are generated and a platform for the analysis, e.g., MindSphere, is identified. But how does the actual, secured data transfer to the cloud take place? In general, two methods of cloud connection can be distinguished: either via external hardware or as an integrated solution, e.g., as a communication processor for the controller. Let's go into detail ...


Totally Integrated Automation
SIMATIC S7 existing plants
Open IIoT solutions
Cloud Platform
Network
Industrial IoT Gateways
Programmable logic controller
Distributed IO
Field devices/ sensors
MQTT
MQTT
MQTT
Engineering with TIA Portal
S7-1500 with CP 1545-1
🟩 PROFINET
Engineering by importing STEP7 project data
OPC UA C/S 🟩
CloudConnect 7
🟩 Industrial Ethernet
S7-400
S7-300
🟪 PROFIBUS
Specific protocols and edge processing
Web-based UI
RX1400
Various connectivity options, e.g. WLAN, Industrial Ethernet
Intelligent field devices
Mobile production equipment
G_IK10_XX_10446

Various ways to an easy cloud connection – depending on the installed equipment and the actual use case

Enhance your controller with cloud connectivity

An integrated solution like the new communications processor SIMATIC CP 1545-1 enhances the existing SIMATIC S7-1500 hardware, e.g., the plant controller, with the possibility of securely sending data to the cloud. This approach offers several advantages:

On the one hand, the controller as an already present data aggregator can be used for the pre-processing mentioned earlier. Plant manufacturers already possess the process know-how required for this. The aspect of the cloud connection can thus be directly incorporated during the creation of the control program.

On the other hand, existing or hardware required anyway can be used to compute values, while the communication processor provides the needed cloud protocols like Message Queuing Telemetry Transport (MQTT).

Ultimately, however, it is not always possible to directly access all measured values available in a plant. Even though the degree of networking and especially the proliferation of the Ethernet infrastructure continue to increase, it is not always sensible to run this networking down to the lowest sensor level. For economic reasons, the sensor level is often still connected via bus systems or analog signals. Having said that, information from sensors connected in this way is available in the plant controller and can be utilized for higher-level analyses by means of an integrated cloud connection.

Easy-to-use cloud connectivity even for existing facilities

With the external variant, information from the plant is collected by a separate device and then sent to the cloud by means of secure communication. Such a solution is always advisable whenever the actual machine or plant controller is to remain untouched, and the automation side must not be affected by security updates.

Apart from the already available RUGGEDCOM RX1400, there are two ways to connect existing systems with the Industrial IoT Gateway SIMATIC CloudConnect 7:

SIMATIC CC712 facilitates the connection of a SIMATIC S7-300 or S7-400 via Industrial Ethernet by means of the S7 protocol. With SIMATIC CC716, on the other hand, up to seven SIMATIC S7 controllers can be connected via Industrial Ethernet or Profibus/MPI interfaces.

With the new SIMATIC CP 1545-1, cloud communication capabilities can easily be added to the SIMATIC S7-1500 controller.

SIMATIC CloudConnect 7 offers an easy way to connect existing facilities.

With the latter solution, the existing automation program does not have to be changed in order to select and transfer the essential information. In addition, the data read by CloudConnect 7 from lower-level SIMATIC S7 stations can be made available as OPC UA variables (server). This enables standardized data exchange, for example with MES systems or HMI and third-party controllers.

The open Message Queuing Telemetry Transport (MQTT) cloud protocol is used in all cases. This established standard also makes it possible to transfer data to MindSphere, the IoT operating system from Siemens. Direct connection to platforms such as Microsoft Azure, IBM Cloud or Amazon Web Services (AWS) can also be implemented.

Security as elementary component

Whenever cloud-based systems are talked about, data are transmitted over enterprise or even public networks. Data security should therefore always be part of the overall concept, as is the case with the "Security-in-Depth" concept from Siemens. Consequently, the data transfer to MindSphere is always encrypted based on certificates.

Special attention, however, should also be paid to the actual connection of the automation cell or plant. Since a connection to the higher-level network is necessary for the cloud connection, there is always a potential access point for attackers. The severity of the potential threat strongly depends on the higher-level network and its protective measures. In many cases, though, an additional protective mechanism in the cell makes sense, also because the access authorization can then be controlled independent of any higher-level mechanisms.

Two different protective concepts suggest themselves: one with separate hardware, such as a SCALANCE SC632-2C Industrial Security Appliance for connection via the existing company network or a WAN router for wired or mobile network communication (e.g., a SCALANCE M874-4 over LTE).

In each case, SCALANCE functions as a configurable firewall, among other things. If correspondingly set up, all devices in the subordinate network can be accessed IP-based.

For the integrated solution with SIMATIC S7-1500, the communication processor SIMATIC CP 1545-1 offers not only a separate network connection but also a built-in firewall. The operating status of the CP has no effect on the actual controller. Even in the case of a denial-of-service attack from outside that impairs the functioning of the CP, the actual controller can continue working unaffected. With this solution, a network separation is always realized: the controller can be reached from the higher-level network, but access to subordinate devices is blocked because no IP routing takes place.

In summary: with the CP 1545-1, a cloud connection tailored to the individual requirements of the plant can be implemented. For the processing of the data, all programming means familiar from the SIMATIC S7-1500 are available. An individual protection of the controller or the automation system makes sense and is already provided by the communication processor. For external devices like the CloudConnect 7, additional security options are available.

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Technical article
PD-FA-18/19-6
PDF 0522 5 En
Produced in Germany

siemens.com/cloudconnect