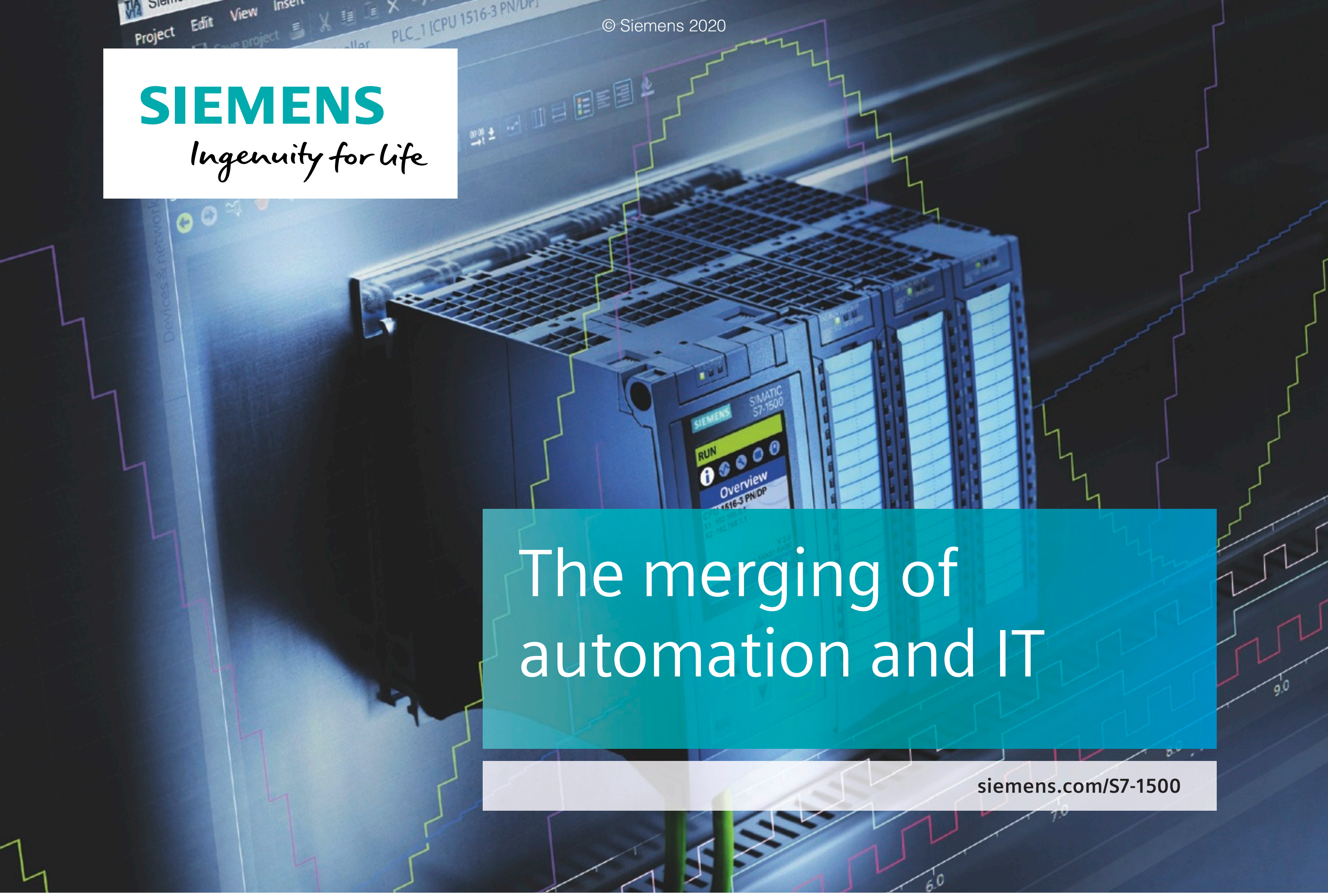
SIEMENS
Ingenuity for life



The merging of automation and IT

siemens.com/S7-1500

Author

Andrea Rauscher
Product manager SIMATIC
Siemens AG, Nuremberg
Germany

Andreas Czech
Marketing manager SIMATIC
Siemens AG, Nuremberg
Germany

The increasing digitalization of processes is being accompanied by growing demands for the provision and processing of data at the automation level:
Automation not only has to collaborate more closely with MES, ERP and Cloud systems, but must also assume tasks in the fields of data processing and analysis. The once distinct boundaries between automation and IT are becoming increasingly blurred, so that the PLC must also be capable of supporting secure and transparent administration of devices from the IT viewpoint as well as the simple integration of production data in an IT environment.

It is only at first glance that the networking of operational technology (OT) and IT seems to be a departure from the previously standard architectures in automation technology. For some time now, automation components have included functions based on the same mechanisms and protocols that IT systems also use.

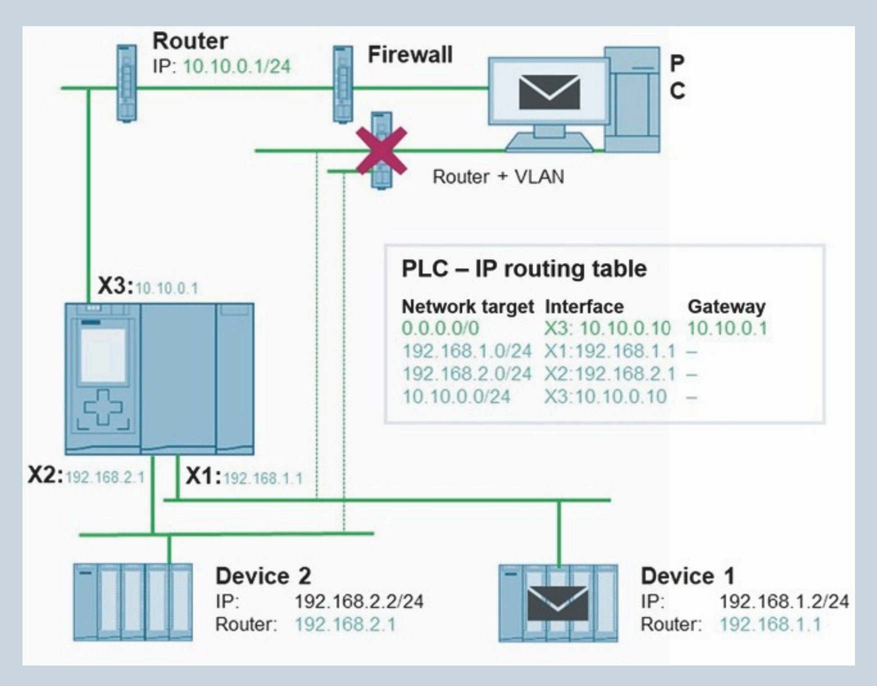
One example of this is communication via Profinet, which uses TCP/IP and IT standards. Components that communicate via Profinet have an IP address by which they are identified in the network. In addition, many components can provide information on the device or system status via an integrated web server – for example, for some years now users have able to access diagnostic data and process data from the CPU via the integrated web server in the Simatic S7-1500 CPU and ET 200SP or ET 200pro CPU through the network and a browser. What is new, however, is that in the course of digitalization, there has been a significant increase in the degree of system networking and the spread of IT functions within the automation level. In addition, industrial systems no longer communicate only with each other, but increasingly also with higher-level systems, for example in the field of inventory control, as well as with Cloud-based applications.

Accordingly, there is also a growing demand for standardization and efficient, secure administration and maintenance of network-compatible components at the automation level.

Transparent view of the network

One of these requirements is the desire to gain simple access to all participants in a network using the IP addresses that users are familiar with from other areas. Until recently, this possibility was severely limited in the field of automation, since networks are typically divided into several subnets, whereby direct access via the IP address is only possible within one network. For example, the central controller of a machine can be reached from the production network, but not the subordinate automation components, although they are also connected to this PLC via Profinet. For this purpose a separate connection from the router had to be set up, making it a relatively complex task to integrate all network-compatible automation components in a common device management system. One effect of this was to complicate central diagnostics or centrally controlled updates for the automation components. The configuration and parameterization of devices was previously also limited to one (sub)network.

Such functions will be familiar to users from the IT world, but if they are to be supported at control level, components such as controllers must support IP forwarding (routing of IP telegrams).



PLC – IP routing table

Network target	Interface	Gateway
0.0.0.0/0	X3: 10.10.0.10	10.10.0.1
192.168.1.0/24	X1:192.168.1.1	–
192.168.2.0/24	X2:192.168.2.1	–
10.10.0.0/24	X3:10.10.0.10	–

By means of IP forwarding, the controller can forward received IP frames to directly accessible IP subnets

This is now possible with the current Simatic S7-1500 controllers. As from firmware version 2.8, the controllers can forward IP telegrams from one integrated CPU Profinet interface to another integrated Profinet interface. This enables a connection to lower-level devices to be established without additional hardware expenditure, for diagnostics and commissioning purposes for example.

The new features of firmware version 2.8 are available for all CPU variants of the Simatic S7-1500, including the new CPU 1513pro-2 PN which, thanks to its IP65/67 degree of protection, can also be used on the machine itself without a control cabinet

Furthermore, in the case Simatic S7-1500 CPUs, this function can also be combined with IP accessibility via a communication module such as the Simatic CP 1543-1, so that the OPC UA server of the CPU can also be reached via the communication module, or can act as an OPC UA client to send data via the CP 1543-1. This means, for example, that production data can be read out and forwarded via OPC UA standard communication to integrate machines into an existing automation and communication infrastructure, including a connection to SCADA and MES systems or Cloud solutions.

Extended options for web-based diagnostics

Another widespread option for data access to the controller also comes from the IT world. Modern automation components often already have an integrated web server, which is used to provide a wealth of data for system diagnostics and maintenance: diagnostic buffers, alarm lists, actual/target topologies, module states and network information, especially from the different bus systems. The Simatic S7-1500 controller's web server also supports a wide range of maintenance functions, such as creating and restoring backups, loading new firmware versions and performing wiring tests.

Defense-in-depth for networked systems

The increasing networking of OT and IT ensures greater data transparency – but also has a downside: There is also the risk that unauthorized persons can gain access to valuable data. In order to protect systems and plants against attacks and unauthorized access, manufacturers such as Siemens recommend a “defense-in-depth” concept based on plant security, network security and system integrity as recommended by ISA 99/IEC 62443.

In addition to technical measures, organizational measures such as guidelines and processes as well as the monitoring of automation systems for anomalies are incorporated as protection for the overall system, ensuring that any attack is discovered as quickly as possible and major losses can be avoided. Network security includes all measures to inhibit unauthorized access to automation networks and eavesdropping or falsification of industrial communication. One part of this involves a password-protected CPU, authentication of communication partners and secured communication. The current firmware version 2.8 of Simatic S7-1500 now additionally supports secure email transmission with attachments. System integrity ultimately includes all security measures that serve to protect automation systems and terminal devices.

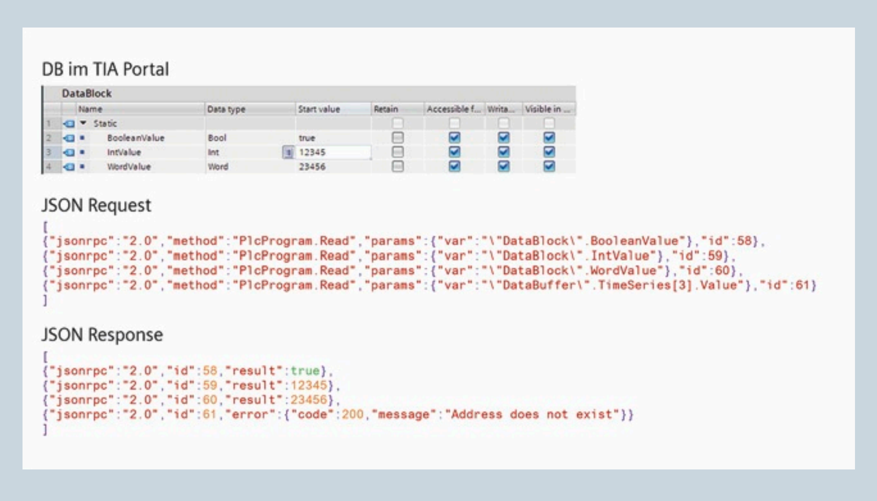
On the one hand, the defense-in-depth concept makes things harder for attackers as several coordinated security levels must be overcome. And even if one single vulnerability can be exploited, the attack remains without consequence or is limited in its impact as other security measures then kick in.

More on defense-in-depth:

siemens.com/industrial-security

The corresponding functions and information can be easily displayed using a web browser.

Here too, some requirements in this respect have changed considerably in recent years. Not only has the amount of data provided via the web server increased, but the type and utilization of the data, including visualization, has also become more diverse. The data should, for example, also be displayed on mobile devices, or the contents of a page should be dynamically reloaded, for example if the current operating or status data from several devices or machines is on one single page. One way to transfer such data between the web client and the automation level is JavaScript Object Notation (JSON). Data is exchanged between the applications in an easy-to-read text form so that developers can implement their own website content and evaluations without the need for special automation knowledge. Since data transmission via the JSON interface only supports secure communication via HTTPs, users also gain a certain amount of security during data transfer (see inset box). In addition to the usual browser frameworks, the JSON interface is also compatible with other frameworks such as Microsoft .Net, Java, GNU Wget or cURL. In this way, users can utilize automation data in many other applications based on web technologies. This applies, among other things, to data analysis and visualization in MES or SCADA systems, but also to applications in the context of the Industrial Internet of Things (IIoT).



DB im TIA Portal

DataBlock

	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...
1	Static			□	□	□	□
2	BooleanValue	Bool	true	□	☑	☑	☑
3	IntValue	Int	12345	□	☑	☑	☑
4	WordValue	Word	23456	□	☑	☑	☑

JSON Request

```
[
{"jsonrpc":"2.0","method":"PlcProgram.Read","params":{"var":"\"DataBlock\".BooleanValue"},"id":58},
{"jsonrpc":"2.0","method":"PlcProgram.Read","params":{"var":"\"DataBlock\".IntValue"},"id":59},
{"jsonrpc":"2.0","method":"PlcProgram.Read","params":{"var":"\"DataBlock\".WordValue"},"id":60},
{"jsonrpc":"2.0","method":"PlcProgram.Read","params":{"var":"\"DataBuffer\".TimeSeries[3].Value"},"id":61}
]
```

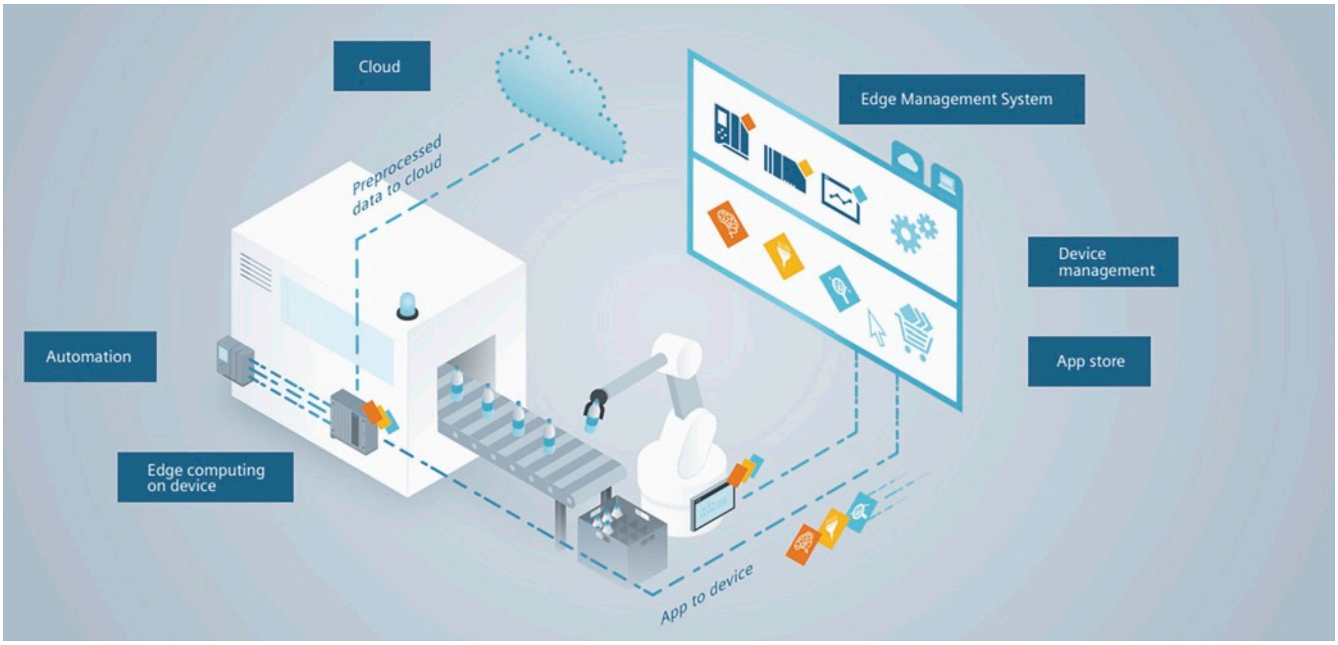
JSON Response

```
[
{"jsonrpc":"2.0","id":58,"result":true},
{"jsonrpc":"2.0","id":59,"result":12345},
{"jsonrpc":"2.0","id":60,"result":23456},
{"jsonrpc":"2.0","id":61,"error":{"code":200,"message":"Address does not exist"}}
]
```

A JSON RPC2.0 interface facilitates the use of current process values from the automation system in user-defined web pages

The IIoT migrates to the controller

The next stage in development is already on the horizon: As the core component of automation, controllers will also assume the task of a data aggregator and supplier. This immediately creates points of contact to Industrial Edge Computing, which relocates data processing from the Cloud closer to the source of data and thus reduces latency and costs of data transmission, improves



The Siemens ecosystem for Industrial Edge Computing supports users in the development, implementation and maintenance of Edge Computing applications and devices.

the protection of sensitive data and simplifies efficient administration of the networked systems.

Usually, Edge applications run on separate PC-based systems. Ideally this intelligence should be relocated directly to the automation level so that data can be processed where it is created. Siemens is currently preparing a technology module for Simatic S7-1500, which is just one example of how the company is using Industrial Edge. Thanks to Edge Runtime, this module facilitates easy implementation of Siemens Industrial Edge applications at control system level or realization of users' own applications in high-level languages such as C/C++.

This not only means that numerous applications in the field of data analysis and process optimization can be implemented but also that very specific tasks can be performed in automation projects. Among other things, this means that information from different bus systems can easily be read out and modified or that user-specific protocols can be integrated into the standard automation. In this way, the PLC assumes a further bridging function between OT and IT: As an Edge Device it enables users to combine the advantages of a Cloud with the strengths of a local solution and brings the IIoT directly into the automation system.

Editorial version is published at SPS-Magazin, edition 2-2020.

Published by
Siemens AG
Digital Industries
Factory Automation
P.O. Box 48 48
90026 Nürnberg
Germany

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Subject to change without prior notice
Produced in Germany
PDF 0320