

Mit neuen Funktionen übernehmen Steuerungen wie die Simatic S7-1500 eine Brückenfunktion zwischen Fertigungsebene und IT.

*Automatisierung und IT wachsen zusammen*

# Die SPS als Edge Device

*Mit der zunehmenden Digitalisierung von Prozessen steigen die Anforderungen an die Datenbereitstellung und -verarbeitung auf Automatisierungsebene: Die Automatisierung muss nicht nur immer enger mit MES-, ERP- und Cloud-Systemen zusammenarbeiten, sondern auch Aufgaben im Bereich der Datenaufbereitung und -analyse übernehmen. Die klaren Grenzen zwischen Automatisierung und IT verschwimmen zusehends, sodass die SPS auch in der Lage sein muss, eine sichere und transparente Administration von Geräten aus IT-Sicht und die einfache Integration von Produktionsdaten in einem IT-Umfeld zu unterstützen.*

Die Vernetzung von Automation und IT ist nur auf den ersten Blick eine Abkehr von den bisher üblichen Architekturen in der Automatisierungstechnik. Schon lange beinhalten Steuerungskomponenten Funktionen, die auf Mechanismen und Protokollen beruhen, die auch IT-Systeme nutzen. Ein Beispiel ist die Kommunikation über Profinet, die TCP/IP und IT-Stan-

dards nutzt. Komponenten, die über Profinet kommunizieren, besitzen eine IP-Adresse, über die sie im Netzwerk identifiziert werden. Darüber hinaus können viele Komponenten Informationen zum Geräte- oder Anlagenstatus über einen integrierten Webserver zur Verfügung stellen – z.B. können Anwender bereits seit einigen Jahren über den integrierten Webserver der Steuerungen Simatic S7-1500 und der

ET 200SP oder ET 200pro per Netzwerk und Browser auf Diagnosedaten und Prozessdaten der SPS zugreifen. Neu ist jedoch, dass im Zuge der Digitalisierung der Grad der Vernetzung der Systeme als auch die Verbreitung von IT-Funktionen innerhalb der Automatisierungsebene stark zugenommen hat. Industrielle Systeme kommunizieren zudem nicht mehr nur untereinander, sondern zunehmend auch



mit überlagerten Systemen sowie mit Cloud-basierten Anwendungen. Entsprechend steigt der Bedarf nach Standardisierung und einer effizienten, sicheren Administration und Instandhaltung netzwerkfähiger Komponenten auch auf der Automatisierungsebene.

## Transparente Sicht auf das Netzwerk

Eine dieser Anforderungen ist der Wunsch, einen einfachen Zugriff auf alle Teilnehmer eines Netzwerks anhand der IP-Adressen zu erhalten, wie es Anwender aus anderen Bereichen kennen. Diese Möglichkeit war bis vor kurzem im Bereich der Automatisierung stark eingeschränkt. Denn Netzwerke sind hier typischerweise in mehrere Subnetze unterteilt, ein direkter Zugriff über die IP-Adresse jedoch nur innerhalb eines Netzwerkes möglich ist. So ist zwar z.B. die SPS einer Maschine vom Produktionsnetzwerk erreichbar, nicht jedoch unterlagerte Automatisierungskomponenten, obwohl sie ebenfalls über Profinet angebunden sind. Dann muss eine eigene Verbindung vom Router aus eingerichtet werden, sodass es bisher relativ kompliziert war, alle netzwerkfähigen Automatisierungskomponenten in ein gemeinsames Gerätemanagement zu integrieren. Auch eine zentrale Diagnose oder zentral gesteuerte Updates für die Automatisierungskomponenten waren entsprechend aufwändig. Auch die Konfiguration und Parametrierung der Geräte war bisher auf ein (Sub-)Netzwerk beschränkt.

## IP-Telegramme durchleiten

Damit diese Funktionen, die Anwender aus der IT-Welt kennen, auch auf Steuerungsebene unterstützt werden, müssen Komponenten wie Steuerungen ein Durchleiten von IP-Telegrammen unterstützen, das sogenannte IP-Forwarding. Das ist mit den aktuellen Simatic S7-1500 Controllern jetzt möglich. Ab der Firmware-Version 2.8 können die Steuerungen IP-Telegramme von der integrierten Profinet-Schnittstelle zu einer anderen integrierten Profinet-Schnittstelle weiterleiten. Damit lässt sich ohne zusätzlichen Hardwareaufwand eine Verbindung zu unterlagerten Geräten aufbauen, z.B. für die Diagnose und Inbetriebnahme. Außerdem

kann diese Funktion bei SPSen der Simatic S7-1500-Reihe zusätzlich noch mit der IP-Erreichbarkeit über ein Kommunikationsmodul wie dem Modell Simatic CP 1543-1 kombiniert werden. So ist der OPC UA Server der SPS auch über das Kommunikationsmodul erreichbar bzw. die CPU kann als OPC UA Client Daten über das Kommunikationsmodul versenden. Dadurch können etwa Produktionsdaten über OPC-UA-Standardkommunikation ausgelesen und weitergegeben werden, um Maschinen in eine vorhandene Automatisierungs- und Kommunikationsinfrastruktur zu integrieren, inklusive einer Anbindung an Scada- und MES-Systeme oder Cloud-Lösungen.

## Erweiterte Möglichkeiten bei Web-basierter Diagnose

Auch eine weitere verbreitete Möglichkeit des Datenzugriffs auf die Steuerung kommt aus der IT-Welt: Moderne Automatisierungskomponenten besitzen oftmals bereits einen integrierten Webserver, über den eine Vielzahl von Daten für die Systemdiagnose und Instandhaltung bereitgestellt werden: Diagnose-Puffer, Alarmlisten, Ist/Soll-Topologien, Baugruppenzustände oder Netzwerkinformationen, insbesondere auch die der unterschiedlichen Bussysteme. Der Webserver der Simatic S7-1500 unterstützt zudem vielfältige Wartungsfunktionen, wie das Erstellen und Wiederherstellen von Backups, das Nachladen von Firmware-Versionen und die Durchführung von Verdrahtungstests. Die entsprechenden Funktionen und Informationen lassen sich einfach über einen Webbrowser darstellen. In den letzten Jahren haben sich auch hier die Anforderungen teilweise erheblich gewandelt: So ist nicht nur die Datenmenge gestiegen, die über den Webserver bereitgestellt wird, auch die Art und Nutzung der Daten inklusive Visualisierung ist vielfältiger geworden. Daten sollen unter anderem auf mobilen Geräten angezeigt oder Inhalte einer Seite dynamisch nachgeladen werden, wenn es z.B. um aktuelle Betriebs- oder

Statusdaten von mehreren Geräten oder Maschinen auf einer Seite geht. Eine Möglichkeit, um solche Daten zwischen dem Webclient und der Automatisierungsebene zu übertragen, ist die JavaScript Object Notation (JSON). Die Daten werden dabei in einer einfach



Die neuen Features der Firmware Version 2.8 gibt es für alle Varianten der Simatic S7-1500, auch für die neue IP65/67-Ausführung der CPU 1513, die ohne Schaltschrank direkt an der Maschine installiert werden kann.

lesbaren Textform zwischen den Anwendungen ausgetauscht, sodass Entwickler ohne spezielle Automatisierungskennnisse eigene Webseiteninhalte und Auswertungen realisieren können. Da die Datenübertragung über die JSON-Schnittstelle nur noch die sichere Kommunikation via HTTPs unterstützt, gewinnen Anwender damit auch ein Stück Sicherheit beim Datentransfer. Zudem ist die JSON-Schnittstelle neben den üblichen Browsern auch mit weiteren Frameworks wie Microsoft .Net, Java, GNU Wget oder cURL kompatibel. Anwender können über diesen Weg also Automatisierungsdaten in vielen weiteren Anwendungen nutzen, die auf Web-Technologien basieren. Das gilt unter anderem für die Datenanalyse und -visualisierung in MES- oder Scada-Systemen, aber auch für Anwendungen im Kontext des Industrial Internet of Things (IIoT).

## IIoT in der Steuerung

Die nächste Entwicklungsstufe zeichnet sich bereits deutlich ab: Als Kernkomponente der Automatisierung werden Steuerungen zusätzlich auch die Auf-



gabe eines Datenaggregators und -lieferanten übernehmen. Dabei ergeben sich unmittelbar Berührungspunkte zum Industrial-Edge-Computing, das die Informationsverarbeitung aus der Cloud näher an die Datenquelle verlagert und so Latenz und Kosten bei der Datenübertragung verringert, den Schutz sensibler Daten verbessert und eine effiziente Administration der vernetzten Systeme vereinfacht. Üblicherweise laufen Edge-Applikationen auf separaten PC-basierten Systemen. Idealerweise sollte diese Intelligenz aber unmittelbar in die Automatisierungsebene verlagert werden, um die Daten direkt am Ort ihrer Entstehung zu verarbeiten. Siemens will Industrial Edge unter anderem mit einem Technologiemodul für die Simatic S7-1500 bieten, das aktuell in Vorbereitung ist. Damit können Anwender industrielle Edge-Anwendungen unkompliziert auf der Steuerungsebene implementieren oder auch eigene Applikationen in Hochsprachen wie C/C++ umsetzen. Auf diese Weise lassen sich nicht nur zahlreiche Applikationen im Bereich der Datenanalyse und Prozessoptimierung realisieren, sondern auch sehr spezifische Aufgaben in Automatisierungsprojekten lösen. So können unter anderem Informationen aus unterschiedlichen Bussystemen

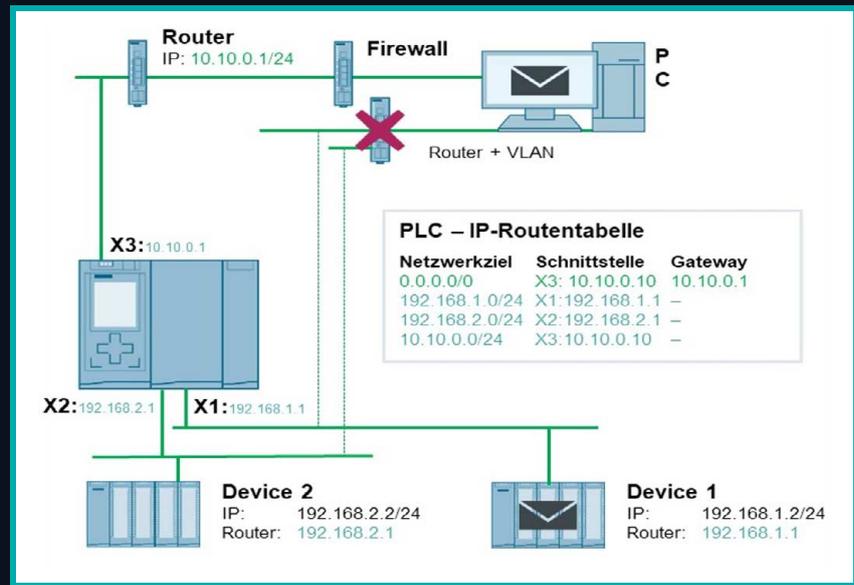


Bild: Siemens AG

► Über IP-Forwarding kann die Steuerung empfangene IP-Frames an direkt erreichbare IP-Subnetze weiterleiten.

einfach ausgelesen und modifiziert bzw. anwenderspezifische Protokolle in die Standardautomatisierung integriert werden. Damit übernimmt die SPS eine wichtige Brückenfunktion zwischen Automatisierung und IT: Als Edge Device ermöglicht sie es, die Vorteile einer Cloud mit den Stärken einer lokalen Lösung zu kombinieren und bringt das IIoT direkt in die Automatisierung. ■

Direkt zur Übersicht auf  
**i-need.de**  
[www.i-need.de/ff/9595](http://www.i-need.de/ff/9595)



**Andrea Rauscher,**  
Product Manager SIMATIC  
Siemens AG  
[www.siemens.com](http://www.siemens.com)



**Andreas Czech,**  
Marketing Manager SIMATIC  
Siemens AG  
[www.siemens.com](http://www.siemens.com)

## Tiefengestaffelte Cyber-Sicherheit für vernetzte Systeme

Die zunehmende Vernetzung von Automatisierung und IT sorgt für mehr Datentransparenz – hat aber auch eine Kehrseite: Es wächst die Gefahr von Angriffen und unbefugten Zugriffen. Um Systeme und Anlagen zu schützen, empfiehlt Siemens ein sogenanntes Defense-in-Depth-Konzept, das auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität nach den Empfehlungen der ISA99 bzw. IEC62443 basiert. Dabei gehören zur Sicherheit der Gesamtanlage neben technischen auch organisatorische Maßnahmen wie Richtlinien und Prozesse sowie die Überwachung der Automatisierungsanlagen auf Anomalien, um Angriffe möglichst frühzeitig entdecken zu können. Die Netzwerksicherheit umfasst alle Maßnahmen, um unbefugte Zugriffe auf Automatisierungsnetze und das Mitlesen oder Verfälschen in-

dustrieller Kommunikation zu unterbinden. Zur Systemintegrität zählen schließlich alle Security-Maßnahmen, die dem Schutz der Automatisierungssysteme und Endgeräte dienen. Ein Teil davon ist eine passwortgeschützte SPS, die Authentifizierung der Kommunikationspartner und eine abgesicherte Kommunikation. Die aktuelle Firmware 2.8 der Simatic S7-1500 unterstützt zusätzlich den sicheren E-Mail-Versand mit Anhang. Das Defense-in-Depth-Konzept steigert einerseits den Aufwand für Angreifer, da mehrere abgestimmte Sicherheitsebenen überwunden werden müssen. Und selbst wenn eine einzelne Schwachstelle ausgenutzt werden kann, bleibt der Angriff entweder folgenlos oder wird in seinen Auswirkungen begrenzt, da dann andere Security-Maßnahmen greifen.