



© jpoppha - stock.adobe.com

Verbindung ins Feld

Wahl des richtigen industriellen Ethernet-Protokolls



Vibhoosh Gupta,
Emerson

In der industriellen Automatisierung setzt sich die Ethernet-Kommunikation immer mehr durch. Die Entscheidung, welches Industrieprotokoll für welche Architekturebene am besten geeignet ist, liegt jedoch immer noch beim Nutzer.

Eine der wichtigsten Voraussetzungen für eine erfolgreiche industrielle Automatisierung ist eine hohe Konnektivität von der niedrigsten bis zur höchsten Architekturebene. Die einfachsten Feldverbindungen sind fest verdrahtete E/A-Punkte. Diese wurden im Laufe der Jahre durch industrielle Feldbusse ergänzt bzw. nach und nach ersetzt. Für die Kommunikation zwischen den Geräten auf den höheren Architekturebenen sind andere Netzwerke und Protokolle besser geeignet.

Ein bedeutender Fortschritt, der in den letzten zehn Jahren erzielt werden konnte, ist die zunehmende Verwendung von Ethernet-Verbindungen für die industrielle Konnektivität. Doch auch wenn sich das Ethernet gegenüber vielen anderen Kommunikationsoptionen immer mehr durchsetzt, müssen Nutzer immer noch entscheiden, welche industriellen Ethernet-Protokolle in ihrem konkreten Anwendungsfall am besten geeignet sind.

Je nachdem, in welcher Anwendung und wo genau innerhalb des Automatisierungssystems

ein Protokoll zum Einsatz kommen soll, wird sich der Nutzer für das eine oder das andere Protokoll entscheiden. Einige industrielle Ethernet-Protokolle sind ziemlich ausgereift und eignen sich für alle Architekturebenen. Allerdings enthalten viele auch noch Technologien, die mittlerweile veraltet sind. Andere Protokolle wurden für bestimmte Anwendungen wie z.B. für Hochgeschwindigkeitsbewegungen optimiert. Auf den oberen Architekturebenen, d.h. der Netzwerkebene oberhalb der Betriebs- und der Steuerungsebene, gelten für die Auswahl des passenden Protokolls ganz andere Vorgaben als auf der Ebene der Feldgeräte und E/A-Punkte.

Auf der Produktionsebene interagieren viele verschiedene Systeme miteinander. Dies macht ein sicheres Netzwerkprotokoll mit zahlreichen kontextbezogenen Links erforderlich, da nur so sicherzustellen ist, dass aus den Rohdaten tatsächlich wertvolle Informationen gewonnen werden können. In diesem Artikel wird erörtert, warum das Netzwerkprotokoll OPC UA für

diese Aufgaben besonders geeignet ist. Das Protokoll wurde speziell für die umfassenden Aufgaben im Industriebereich ausgelegt.

Aufbau eines Betriebsnetzwerks

Industrielle Automatisierungssysteme bestehen aus zahlreichen Geräten und Komponenten, die alle miteinander verbunden bzw. vernetzt sind. Feldgeräte wie Sensoren, Aktuatoren und intelligente Elemente sind dabei mit Steuerungseinheiten verbunden. Diese speicherprogrammierbaren Steuerungen (SPS) und programmierbaren Automationssteuerungen (PAC) überwachen und steuern die Feldgeräte, kommunizieren miteinander, sind mit Mensch-Maschine-Schnittstellen (HMIs) sowie SCADA-Systemen zur Überwachung und Steuerung verschiedener Prozesse vernetzt und unterstützen verschiedene Aufgaben wie die Archivierung, Auswertung und weitere Verarbeitung von Daten (Abb. 1).

In der Industrie verfügen Netzwerkhierarchien über viele verschiedene Merkmale.

Nicht immer können letztere dabei genau definiert werden, da es auf einigen Ebenen zu einer Virtualisierung der IT-Ressourcen oder zu einer Zusammenlegung verschiedener Netzwerke kommen kann. Hier ist ein kurzer Überblick über die wichtigsten Ebenen, die innerhalb eines Industrieunternehmens miteinander zu vernetzen sind:

- Ebene 4: Fabrik- und Produktionsplanung & Logistik
- Ebene 3: MES-System zur Produktionsüberwachung
- Ebene 2: HMI und SCADA zur übergeordneten Steuerung und Vernetzung
- Ebene 1: prozessnah positionierte SPS- und PAC-Systeme
- Ebene 0: Feldsensoren, Geräte und Netzwerke

Über fest verdrahtete E/A-Punkte, Feldbussysteme und industrielles Ethernet sind alle Steuerungseinheiten mit den Feldgeräten und anderen Komponenten auf den Ebenen 0 und 1 vernetzt. Alle Verbindungen erfolgen prozessnah und bestehen in der Regel nur aus kleinen Datenpaketen. Denn die Daten müssen schnell übertragen werden, da die Geräte auf Feldebene in Echtzeit gesteuert werden müssen.

Für die industrielle Kommunikation auf den verschiedenen Ebenen gelten unterschiedliche Anforderungen.

Die industriellen Netzwerke auf Ebene 1 und darüber werden manchmal zusammenfassend als Netzwerke auf Anlagenebene bezeichnet. Im Gegensatz zu den Netzwerken auf den unteren Architekturebenen sind die Steuerungsprozesse in den Netzwerken auf Anlagenebene weniger zeitkritisch.

Im Vergleich zu den eher dezidierten Netzwerken auf den unteren Architekturebenen verbinden Netzwerke auf Anlagenebene sehr unterschiedliche Systeme miteinander. Dadurch steht die moderne industrielle Kommunikation auf Anlagenebene vor ganz neuen Herausforderungen. Sie sollte sich durch folgende Merkmale auszeichnen:

- Sicher: Es werden integrierte Sicherheitsfunktionen bereitgestellt.
- Kontextbezogen und objektorientiert: Die übermittelten Daten werden definiert und organisiert.
- Plattformunabhängig: In verteilten Anwendungen wird eine nahtlose Kommunikation ermöglicht.

Wie bereits erwähnt, gehört dem Ethernet die Zukunft. Dies gilt sowohl für die Informationstechnologie auf Unternehmens- und Produktionsebene (IT) als auch für die Operativen Technologien auf der unteren Produktions- bzw. Anlagen und Maschinenebene (OT). Aus physikalischer Sicht kann die Datenübertragung

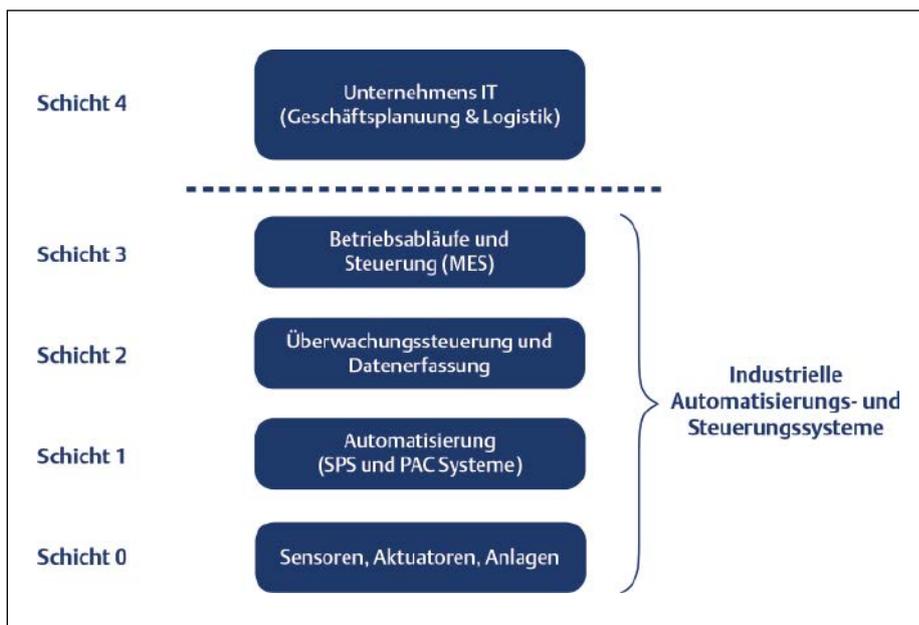


Abb. 1: Industrielle Automatisierungs- und Steuerungssysteme bestehen aus unterschiedlichen Ebenen, in denen zahlreiche Geräte zu einem Netzwerk verbunden sind.

im Ethernet über Kupferdrähte, Glasfaserkabel und sogar über drahtlose Technologien erfolgen. Je nachdem, ob das Ethernet in IT- oder OT-Umgebungen genutzt wird, kommen jedoch verschiedene Ethernet-Kommunikationsprotokolle zum Einsatz.

Protokolle

Die Anpassung des für die höheren Unternehmensebenen entwickelten IT-Ethernets an die auf die Automatisierung von Maschinen und Anlagen ausgerichtete OT-Anwendungen ist nicht einfach. Wenn gute Protokolle wie Profinet, Ethernet/IP und andere zur Verfügung stehen, kann das Ethernet jedoch auch für OT-Netzwerke auf der Feldebene an Bedeutung interessant sein.

Bedingt durch das dahinterstehende OT-Konzept sind Netzwerkprotokolle, die auf der Feldebene zum Einsatz kommen, in der Regel anwendungsspezifisch. Durch diese Spezialisierung und Konzentrierung auf die Maschinen- und Anlagenebene sind sie für einen Einsatz auf höheren Architekturebenen weniger geeignet. Hier werden flexiblere und leistungsfähigere Protokolle benötigt, die eine Interaktion mit vielen verschiedenen Systemtypen ermöglichen. Daher kommen vermehrt offene Lösungen zum Einsatz, die über bestimmte, für internetfähige Geschäftsverbindungen erforderliche Sicherheitsvorkehrungen verfügen müssen.

Im Laufe der Jahre hat das Industriekonsortium OPC Foundation einige Standards erarbeitet und weiterentwickelt, die eine sichere und zuverlässige Interoperabilität verschiedener Betriebs- und Automatisierungssysteme sicherstellen sollen. Der neueste Standard, der

2008 erstmals veröffentlicht wurde, ist OPC Unified Architecture (OPC UA). Dieser steht für eine plattformunabhängige, serviceorientierte Kommunikationsstruktur (Abb. 2).

Auf der Ebene 1 und darüber wird durch das Kommunikationsprotokoll OPC UA genau festgelegt, welche Maßstäbe in Bezug auf die Sicherheit sowie die kontextbezogene und objektorientierte Erfassung und Verarbeitung von Daten gelten. Dadurch ist der Standard für die meisten industriellen Anwendungen interessant. Dank des umfassenden, modularen und skalierbaren Ansatzes von OPC UA können die Nutzer selbst ein „System von Systemen“ erstellen. Das heißt, sie können zahlreiche Subsysteme beliebiger Größe zu einem integrierten industriellen Gesamtautomatisierungssystem zusammenfügen, so dass alle Untereinheiten nahtlos miteinander interagieren können. Dabei werden sowohl Clients als auch Server als interagierende Partner definiert.

Sicherheit

Mit dem Ausbau der Kommunikationsfähigkeit digitaler Systeme über Ethernet und Internet gehen auch gewisse Sicherheitsrisiken einher. Im Allgemeinen gelten für die Informationstechnik und deren Sicherheit die drei CIA-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity und Availability). Herkömmliche Feldbusnetzwerke und klassische industrielle Ethernet-Protokolle konzentrierten sich üblicherweise auf die beiden Schutzziele Verfügbarkeit und Integrität. Das Ziel der Vertraulichkeit wurde kaum oder gar nicht berücksichtigt. Man könnte also sagen, dass die drei oben genannten Schutzziele eine genau umgekehrte Priorisierung erfahren haben und folglich

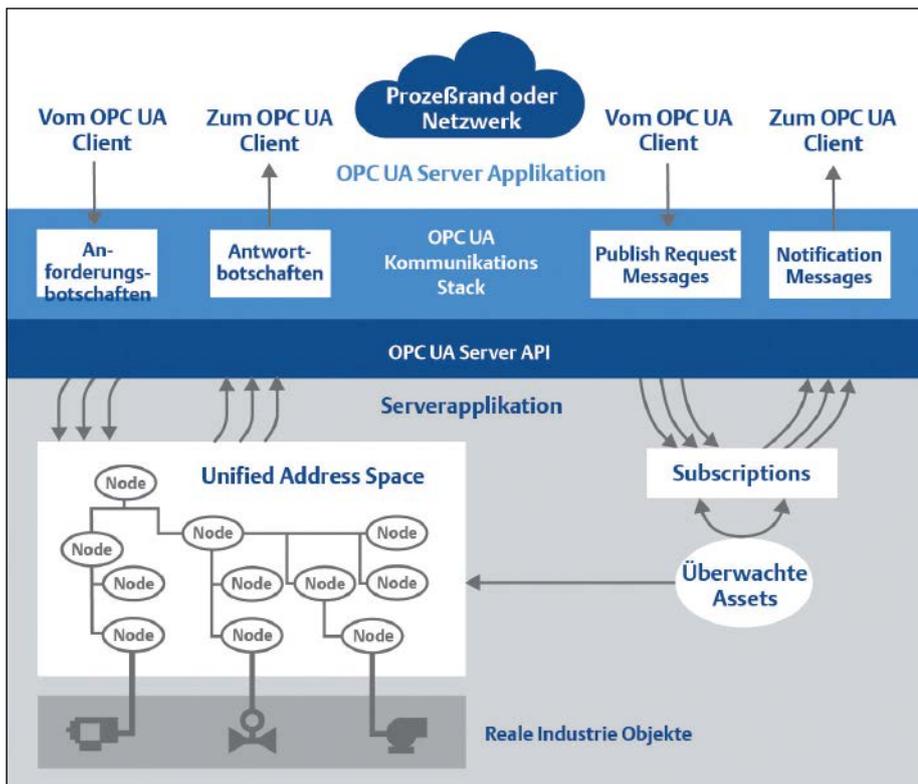


Abb. 2: Das industrielle Kommunikationsprotokoll OPC UA basiert auf einer plattformunabhängigen Architektur. Dies führt zu einer sicheren und kontextbezogenen Erfassung und Verarbeitung der Daten.

nicht mehr von der CIA-Triade, sondern vielmehr der AIC-Triade gesprochen werden muss. Übergeordnete Netzwerke erfordern jedoch einen ausgewogeneren Ansatz, bei dem alle Schutzziele gleichermaßen berücksichtigt werden.

Um die Sicherheit zu erhöhen, können einige Protokolle um Funktionen wie VPN's (Virtual Private Networks) oder TLS (Transport Layer Security) erweitert werden. Doch auch damit lassen sich nicht alle Risiken ausschließen. Wesentlich zielführender ist es, die Sicherheitselemente fest im Protokoll zu integrieren. In das Kommunikationsprotokoll OPC UA sind verschiedene Dienste integriert, durch die sich Sicherheitszertifikate verwalten und sichere Client/Server-Sitzungen auf Anwendungsebene aufbauen lassen. Als Beispiele seien hier nur VPN-Tunnel oder SSL-Verbindungen genannt.

Zudem bietet das Protokoll OPC UA native Sicherheitsmechanismen, damit auf der Client-Ebene verfügbare Server ermittelt, Zertifikate und Vertrauenslisten verwaltet und verteilt werden können und ein Austausch mit der Zertifizierungsstelle möglich ist. OPC UA ist somit ein modernes Ethernet-Protokoll, das für eine sichere industrielle Kommunikation auf allen Architekturebenen bestens geeignet ist.

Kontextbezogene und objektorientierte Erfassung und Verarbeitung von Daten

Klassische Industrieprotokolle konzentrierten sich vor allem auf die zuverlässige Übertragung von Rohdaten. Um die Rohdaten anschließend in nützliche Informationen umwandeln zu können, mussten alle eingehenden Datensignale erfasst und verarbeitet werden, bevor sie an die entsprechenden Schnittstellen weitergeleitet werden konnten. Unter anderem mussten die Daten also genau definiert und die erhaltenen Werte in technische Einheiten übertragen werden. Dies war ein sehr aufwendiges Verfahren, da das industrielle Kommunikationssystem sehr komplex ist. Nötig waren die genannten Operationen z.B. zwischen E/A-Signal und Controller, zwischen Controller, HMI und SCADA, zwischen SCADA und MES oder zwischen SCADA oder Controller und Archiv.

Eine bessere Methode ist die kontextbezogene Erfassung und -verarbeitung der Daten. Das Prinzip besteht darin, dass die Daten über eine inhärente Semantik verfügen. Dadurch können sie unabhängig voneinander sowohl von der SPS als auch von der HMI ausgewertet werden. Dies bedeutet wiederum, dass keine Informationen mehr verloren gehen können. Zudem stehen in diesem System allen Nutzern dieselben Ausgangsdaten zur Verfügung. Durch die umfassenden, im OPC UA vorgegebenen Analysefunktionen kann eine HMI-Konfiguration mühelos in eine SPS-Konfiguration umgewandelt werden. Dabei bleiben alle Skalierungen und Eigenschaften in jedem Standardformat erhalten. Das Protokoll OPC UA unterstützt auch die Bildung von Datenhierarchien. Geübte Anwender können also die Daten in komplexen Baumstrukturen anordnen, wie sie es von ihrem PC gewohnt sind.

Dank der kontextbezogenen Erfassung und -verarbeitung können alle Daten aus einem bestimmten Betriebsbereich oder mehreren Betriebsbereichen zentral auf einem OPC UA-Aggregationsserver abgelegt werden. Über verschiedene Funktionen wie die Visualisierung, die Analyse oder das Archiv stehen sie hier den verschiedenen

Clients zur Verfügung. Dazu müssen diese nur zum jeweiligen Knoten gehen, denn alle Zusatzdaten sind hier in einem strukturierten Format hinterlegt. Etwaige Datenvariablen und besondere Eigenschaften sind so klar definiert, dass sie leicht in Beziehung zu den anderen Daten gesetzt werden können. Dadurch wird die Automatisierungshierarchie flacher und allen Entscheidungsträgern stehen unmittelbar sämtliche Daten zur Verfügung.

Die Objektorientierte Programmierung umfasst Methoden, mit deren Hilfe Informationsmodelle erstellt und vermittelt werden können. So könnten beispielsweise die in einer Pumpe herrschenden Ein- und Auslasstemperaturen sowie der dort gemessene Druck in einem solchen Modell dargestellt werden.

Durch die Anwendung von objektorientierten Techniken lassen sich viele Abläufe effizienter und einheitlicher gestalten, da Konstrukteure verschiedene Modelle erstellen, wiederverwenden und miteinander kombinieren können.

Dank der objektorientierten Programmierung können Best-Practice-Konfigurationen entwickelt und wiederverwendet werden. Ein weiterer Vorteil besteht darin, dass alle Objekte auch auf andere verweisen oder aus anderen zusammengesetzt werden können. Somit trägt die objektorientierte Programmierung dazu bei, viele Vorgänge effizienter zu gestalten und zu vereinheitlichen.

Doch ein OPC UA-Server ist viel mehr als eine einfache Datenbank. Darüber hinaus definiert er einige Dienste, die in sogenannten Service Sets organisiert werden. Dazu zählen das Discovery Service Set zum Auffinden OPC UA-fähiger Teilnehmer und Eigenschaften, das Subscription Service Set zur Erzeugung, Veränderung und Löschung von Mitteilungen, das Query Service Set zum Auswählen bestimmter Filterkriterien und das NodeManagement Service Set zum Hinzufügen, Ändern und Löschen von Knoten.

Auf diese Weise können Nutzer Objektmodelle erstellen, die von jeder Client-Anwendung problemlos genutzt werden können.

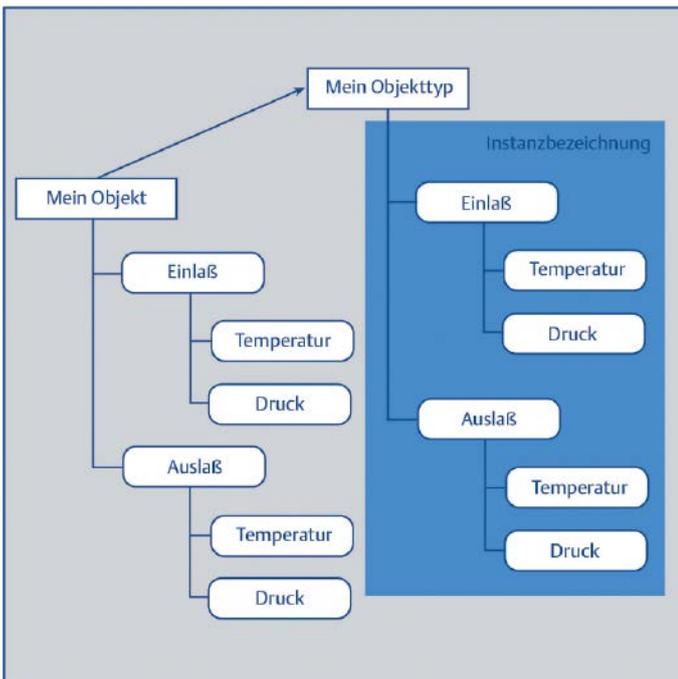


Abb. 3: Beispiel für ein mit Hilfe der objektorientierten Programmierung erstelltes Modell

Plattformunabhängigkeit

Das frühere Konzept Classic OPC unterlag bestimmten Beschränkungen. So unterstützte es nur die Microsoft-Technologie. Der neue Standard OPC UA wurde auch deshalb geschaffen, um diese Abhängigkeiten zu überwinden, den gestiegenen Sicherheitsanforderungen gerecht zu werden, eine Kommunikation über Firewalls hinweg zu ermöglichen und komplexe Datenstrukturen zu unterstützen.

Dadurch können verteilte Anwendungen, die auf verschiedenen Plattformen laufen, nahtlos mit Systemen auf Ebene 2 kommunizieren. Als Beispiele seien hier die Echtzeitbetriebssysteme VxWorks oder QNX genannt, die auf Ebene 1 häufig zur deterministischen Leistung der Hochgeschwindigkeits-SPS/PACs beitragen.

TSN als nächster Schritt

Time sensitive Networking (TSN) ist eine Entwicklung, die das Standard-Ethernet im Bereich Quality of Service (QoS) ergänzt, also eine Priorisierung des Datenverkehrs fördert. So soll es möglich sein, bestimmte Datenbandbreiten für Datenverkehr mit hoher Priorität zu reservieren und den Datentransfer zu synchronisieren. TSN zielt also darauf ab, den Determinismus und die Sicherheit von Ethernet-basierten Netzwerken zu verbessern und genügend Bandbreite zu reservieren, um der steigenden Datenverfügbarkeit in anspruchsvollen industriellen Anwendungen gerecht zu werden. Zudem sollen verschiedene Standard- und Echtzeitprotokolle in einem einzigen Netzwerk zusammengeführt werden. Die Kombination von OPC UA und TSN trägt ohne Zweifel zu einer Weiterentwicklung der industriellen Automatisierung bei, da ein Unternehmen so in den Genuss der Vorteile beider Systeme kommt: die kontextbezogene Erfassung und Verarbeitung von Daten, eine verbesserte Sicherheit und eine garantierte Bandbreite.

OPC UA als Standard für die Industrie

Obwohl das physikalische Ethernet heute weit verbreitet ist, haben Systementwickler und Konstrukteure in der industriellen Automatisierung immer noch die Qual der Wahl, wenn es darum geht, sich für ein bestimmtes Kommunikationsprotokoll zu entscheiden. Welches Protokoll in Frage kommt, hängt auch davon ab, welches physikalische Netzwerk

bereits besteht und ob das Protokoll mit den vorhandenen Geräten in der Produktion kompatibel ist. In jedem Fall muss durch die Architektur sichergestellt sein, dass die Kommunikation über die Netzwerke auf Anlagenebene sicher, kontextbezogen und objektorientiert ist.

Und genau dies wird durch das Protokoll OPC UA gewährleistet. Das Sicherheitskonzept des Protokolls folgt bewährten, für die IT-Branche geltenden Vorgaben. Die kontextbasierte Erfassung und Verarbeitung von Daten garantiert die Übertragung der OT-Rohdaten sowie weiterer Zusatzinformationen zu verschiedenen übergeordneten IT/OT-Systemen. Durch die Objektorientierung sind die gewünschte Einheitlichkeit und Effizienz sowie die Kompatibilität mit den neuesten Programmiersprachen gegeben. Alle diese Vorteile machen das OPC UA in der industriellen Automatisierung zum Kommunikationsprotokoll der Wahl.

Der Autor

Vibhoosh Gupta, Leiter Geschäftsbereich
Maschinenautomationslösungen, Emerson

Diesen Beitrag können Sie auch in der Wiley Online Library als pdf lesen und abspeichern:
<https://dx.doi.org/10.1002/citp.202101114>

Kontakt

Emerson, Augsburg
Vibhoosh Gupta
Tel.: +49 821 50 340
mas.infoEurope@emerson.com
www.emerson.com/PACSystems

Bilder © Emerson

Einfach digital

- Individuell anpassbares Gerätemenü für eine benutzerfreundliche Integration in unterschiedlichste Applikationen
- SPS-Funktion mit Programmierung über ST-Code inklusive Echtzeituhr und direktem Zugriff auf Bedienung und Display
- Planungssicherheit durch skalierbare Hardware mit Plug and Play
- Kommunikation via USB, Bluetooth, PROFINET, Ethernet und RS-485 (Modbus-Master/Slave TCP/RTU)
- Kalibrierung der Analogeingänge nach CQI-9 und AMS2750

More than sensors + automation

Modularer Ein-/Zweikanalregler mit SPS-Funktion

JUMO meroTRON

Willkommen bei JUMO. www.jumo.net