IoT und SPS als Systemverbund

Um eine speicherprogrammierbare Steuerung (SPS) in die IoT-Welt mitzunehmen, muss man sie nicht unbedingt mit der Cloud verbinden.

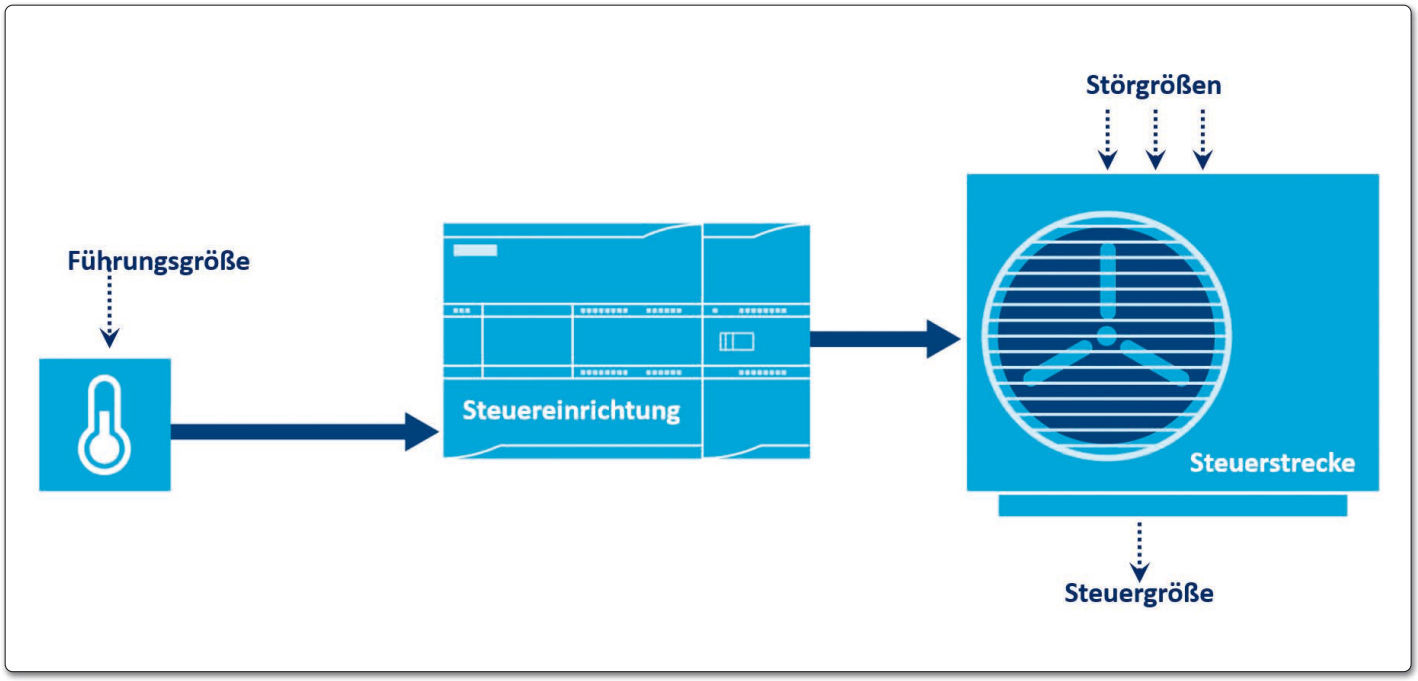

Bild 1: Viele Steuerungsanwendungen in der Gebäudeautomatisierung haben sich trotz des Internets der Dinge kaum verändert. Ein einzelner Sensor erzeugt nach wie vor die Führungsgröße. Störgrößen werden überhaupt nicht berücksichtigt. Die Steuergröße wird lediglich nach einem in der Steuerungssoftware abgelegten Regelwerk beeinflusst. Schutzmaßnahmen gegen Cyberangriffe sucht man vergeblich, weil die Betreiber davon ausgehen, dass wegen der nicht vorhanden Internetanbindung ja auch nichts passieren kann

Sehr viel sinnvoller ist es nämlich, die Führungsgröße der SPS-Anwendung durch IoT-Sensorik zu erzeugen. Dadurch entsteht ein intelligentes System, das sich an seine Umgebung anpasst.

Die Problematik

Das Internet der Dinge hat zu einer bisher einzigartigen Vielfalt an preiswerten Halbleitersensoren geführt, mit welchen sich Messdaten erzeugen lassen, die vor nicht allzu langer Zeit nur mit teurem Laboraufbauten möglich waren. Im Konsumerbereich sind dadurch beispielsweise Anwendungen entstanden, die vorher nur dem Militär oder ähnlichen Spezialbereichen möglich waren. Eine Smartwatch mit GPS- und Beschleunigungs-Sensor, die darüber hinaus auch die Vitaldaten, wie Blutdruck und Herzfrequenz des Trägers, messen kann, wäre ein Beispiel. IR-Sensoren messen zweidimensionale Objekttemperaturen aus der Ferne. Mit Ultraschallsensoren lassen sich sowohl beliebige Füllstände messen, als auch die Personen in einem Raum zählen. Bildsensoren erkennen Objekte und sogar Gesichter, Radarsensoren erfassen einen 3D-Raum und ermöglichen Gestensteuerungen usw.

Manche IoT-Anwendungen benutzen sogar eine Vielzahl unterschiedlicher Sensoren, um ihre Aufgaben zu erfüllen. Die Sensorenanzahl ist in diesem Anwendungssegment der Gegenentwurf zu den Big-Data-Konzepten in der Business-IT. Mit anderen Worten: Sensorfusionsdaten ermöglichen im Internet der Dinge überhaupt erst den Einblick in komplexe Zusammenhänge. Sie sind auch ein wichtiger Funktionsblock für völlig neue Anwendungen, beispielsweise autonome Systeme.

An einem Anwendungsbereich sind diese IoT-Sensorinnovationen bisher nahezu spurlos vorbeigezogen: den SPS-basierten Steuerungsanwendungen in der Automatisierungstechnik. Steuerungen werden zwar inzwischen durch IoT Connectivity Gateways ergänzt, um die zur Verfügung stehen Daten durch Edge- und Cloud-Applikationen weiterzuverarbeiten. Ein solcher IoT-Retrofit ändert aber nichts daran, dass die eigentliche SPS-Software nach wie vor ohne IoT-Sensorik auskommen muss. Bild 1 illustriert den skizzierte Zustand.

Grundkonzept einer Steuerungsanwendung

Schaut man sich beispielsweise das Grundkonzept einer typischen Lüftungs-, Klima- und Kältetechniksteuerung (LüKK-System) an, gewinnt man den Eindruck, es hier mit dem Gegenentwurf zum Internet der Dinge zu tun zu haben: Es wird vielfach versucht, mit einem einzigen Sensor zurechtzukommen. Die meisten LüKK-Anlagen sind zunächst einmal einfache Steuerungsanwendungen gemäß Lehrbuch mit einer Regel- bzw. Steuergröße x, einer Führungsgröße w, der Stellgröße y, sowie möglichen Störgrößen z. Das Ziel einer diesem Grundkonzept folgenden simplen Heizungssteuerung in einer Wohnung ist die Raumtemperatur innerhalb eines bestimmten Bereichs zu halten, welchen die Bewohner insgesamt als angenehm empfinden und der Gebäude- und Anlagenschäden durch extreme Temperaturen verhindert (z.B. Frost).

Die Raumtemperatur ist in diesem Fall die Steuergröße, also die Ausgangsvariable der Steuerstrecke. Als Führungsgröße wird die jeweilige Außentemperatur vor Ort genutzt, die von der Steuereinrichtung mit einem Sensor (Außenfühler) gemessen wird.

Zur Beeinflussung der Steuerstrecke kann die Steuereinrichtung beispielsweise über die Stellgröße eine elektrische Heizspirale ein- und aus-

Autor:
Klaus-Dieter Walter, CEO
SSV Software Systems
www.ssv-embedded.de

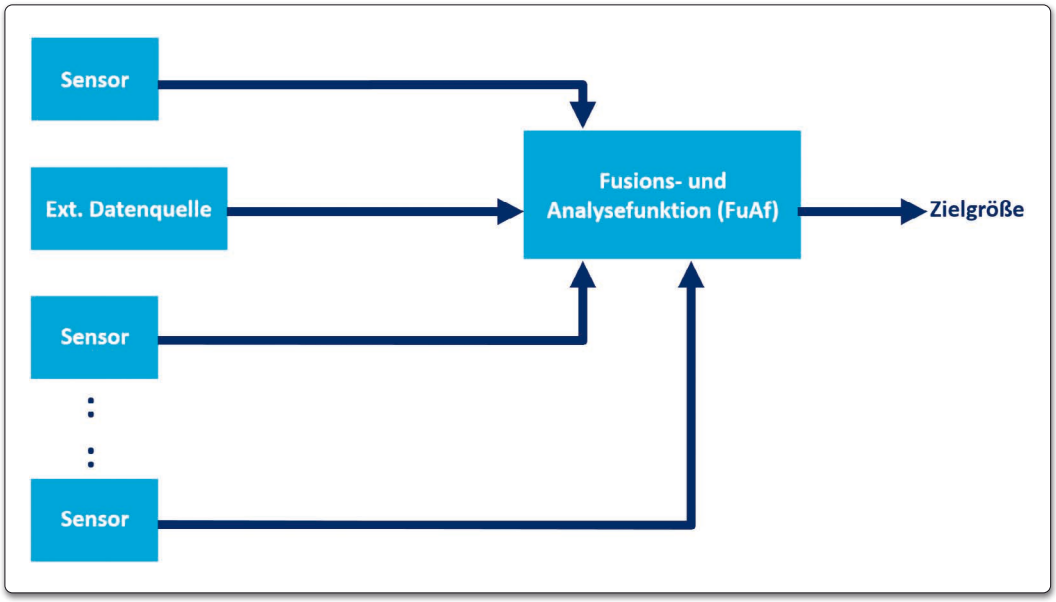

Bild 2: Die Führungsgröße einer SPS lässt sich auch durch einen virtuellen Sensor erzeugen, der unter Zuhilfenahme von IoT-Funktionsbausteinen aufgebaut wird. In einer Fusions- und Analysefunktion werden verschiedene Sensordaten und externe Datenquellen (z.B. eine Wetterberichtsabfrage im Internet) zusammengeführt und ausgewertet. Dadurch entsteht eine aufgabenbezogene Zielgröße, die sich als erweitere Führungsgröße in einer Steuerungsanwendung verwenden lässt

schalten sowie die Lüftergeschwindigkeit beeinflussen.

Bei einer hohen Außentemperatur sind nur relativ wenig Heizzyklen und eine geringe Lüftergeschwindigkeit pro Zeiteinheit erforderlich. Eine sinkende Außentemperatur wird durch die Steigerung der Zyklenzahl und die Einschaltdauer der Heizspirale sowie eine erhöhte Lüftergeschwindigkeit ausgeglichen. Mögliche Störgrößen könnten in diesem Beispiel geöffnete Fenster sowie ein Lagerschaden am Lüfter sein. Der Zusammenhang zwischen Führungsgröße und Stell- bzw. Regelgröße ist als Heizkurve in der Steuerungssoftware abgelegt. Insofern ist prinzipiell auch nur ein einziger Sensor erforderlich.

Intelligenz-Upgrade durch IoT-Sensorik

Das zuvor beschriebene Steuerungskonzept hat üblicherweise keinerlei intelligentes Anlagenverhalten zur Folge. Aber wenn es draußen kalt ist und keine gravierenden Störgrößen vorliegen, wird die vorgestellte Heizung den Raum auf angenehme Innentemperaturen erwärmen. Ob überhaupt jemand zuhause ist, spielt dabei keine Rolle.

Das gesamte Anlagenverhalten lässt sich grundlegend ändern, wenn die Führungsgröße der Steuerung nicht durch einen einfachen Außenfühler, sondern durch einen an die Aufgabenstellung angepassten virtuellen Sensor erzeugt wird, der mit IoT-Technik aufgebaut wurde. Ein virtueller Sensor ist ein softwarebasierter Sensor (Softsensor), der eine ausgangsseitige Zielgröße durch Verknüpfung geeigneter Datenquellen nachbildet. Mit anderen Worten: Die jeweilige Zielgröße wird nicht direkt aus realen Messwerten gewonnen, sondern mit Hilfe von Algorithmen berechnet.

Eingangsseitig lassen sich verschiedene Sensorelemente, aber auch per Netzwerkschnittstellen erreichbare Datenquellen (externe Datenbanken, Cloud-Services usw.) in einen virtuellen Sensor einbinden. Für die hier vorgestellte LüKK-Steuerung könnte man folgende Datenquellen in die Zielgröße eines virtuellen Sensors einbeziehen:

• Wetterbericht

Die für den Steuerungsbetrieb erforderliche Außentemperatur wird nicht mehr direkt gemessen, sondern per Internet über das Application Programming Interface (API) eines Online-Wetterberichts für den jeweiligen Standort abgefragt.

• Ist-Wert

Der tatsächliche Wert der Steuergröße, also die aktuelle Raumtemperatur, wird über einen einfachen Funksensor gemessen. Die Steuerung kann sehr viel genauer auf Störgrößen reagieren.

• Fenstersensor

Das Öffnen eines Fensters zum Lüften des Wohnraums wird erkannt und von einem Funksensor weiter gemeldet.

• Anwesenheitssensor

Es wird ermittelt, ob sich überhaupt eine Person in der Wohnung befindet. Dafür können z.B. ein Ultraschallsensor oder der Standort einer Smartphone-App verwendet werden.

• Tag/Nacht-Betrieb

Für die Steuergröße lassen sich zwei unterschiedliche Zielbereiche definieren, wenn eine Steuerung zwischen Tag und Nacht unterscheiden kann.

• Condition Monitoring

Tritt während der Anlagenlebensdauer z.B. am Lüfter ein Lagerschaden auf, so kann man die daraus resultierende Unwucht erkennen und eine Störung anzeigen.

Die Zielgröße eines virtuellen Sensors kann als (erweiterte) Führungsgröße für eine Steuerung dienen. Man erkennt, dass sich durch das Einbeziehen der Umgebungsdaten, wie zum Beispiel Fensterzustand, Anwesenheit, usw. die Anlageneffizienz verbessern wird, CO_2-Emmisionen reduziert werden und dass sich insgesamt Betriebskosteneinsparungen ergeben dürften. Das integrierte Condition Monitoring erhöht darüber hinaus die Anlagenzulässigkeit.

Viele Daten

Bild 2 visualisiert das Funktionsprinzip eines virtuellen Sensors, der einer LüKK-Steuerung eine erweitere Führungsgröße liefert: verschiedene Eingangsdatenquellen sind mit einer Fusions- und Analysefunktion (FuAf) verbunden. Dort werden die einzelnen Daten zusammengeführt und beispielsweise mithilfe von Supervised-Machine-Learning-Algorithmen (also per überwachtem maschinellen Lernen) bearbeitet, um die jeweilige Zielgröße zu erzeugen. Für die FuAf wird eine externe Kommunikationsschnittstelle benötigt, die sich in IP-Netzwerke (LAN, WiFi, Mobilfunk) einbinden lässt. Sie ermöglicht zum einen den Zugriff auf externe Datenquellen, wie einem Wetterbericht-Service-API und zum anderen den Download und ggf. erforderlichen Remote Updates des Machine-Learning-Modells. Für den Condition-Monitoring-Teil der Aufgabenstellung eignet sich besonders ein kapazitiver MEMS-Inertialsensor. MEMS steht für mikro-elektromechanisches System. Gemeint sind damit kleine Halbleitersensoren, die mit einem speziellen Herstellungsverfahren angefertigt werden und beispielsweise kleinste Lage- und Beschleunigungsänderungen erkennen können. Dafür wird auf einem Siliziumchip ein mikroskopisch kleines Feder-Masse-System realisiert. Durch eine Beschleunigungsänderung wird die Miniaturmasse für wenige Mikrometer ausgelenkt und dadurch eine messbare Kapazitätsveränderung verursacht, aus der letztendlich der Ausgangsmesswert des Sensors entsteht. Damit lässt sich ein Lagerschaden des Lüfters frühzeitig diagnostizieren.

IoT Security beachten

Wenn man sich mit der IoT-Fähigkeit einer Steuerung auseinandersetzt, darf auf keinen Fall die Security auf der Agenda fehlen. Bisher

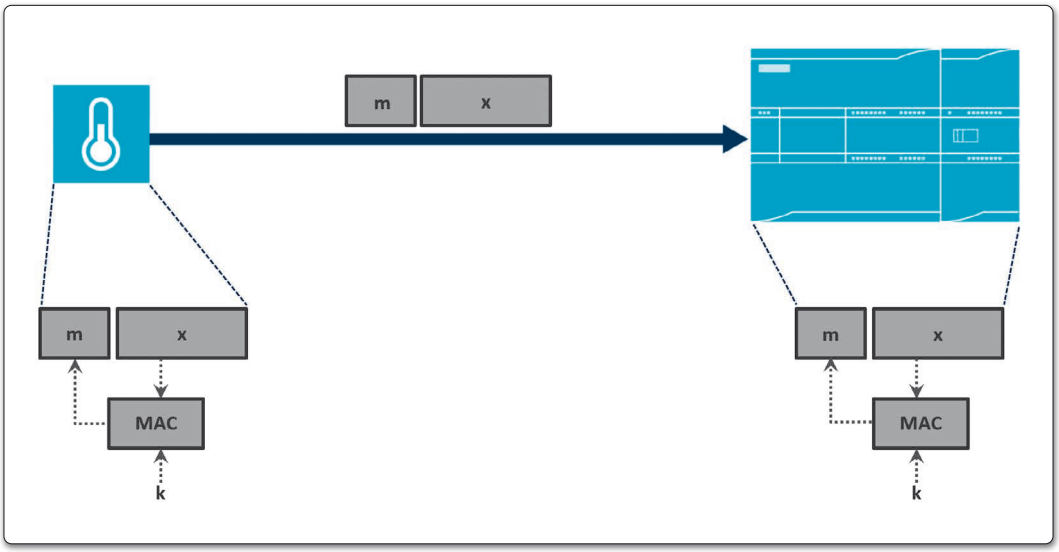

Bild 3: Sender (Sensor) und Empfänger (Steuerung) besitzen einen geheimen Schlüssel k. Mit Hilfe dieses Schlüssels wird für die Sensordaten x vor dem Versand an die Steuerung eine Prüfsumme m als Message Authentication Code (MAC) errechnet, die zusammen mit x an den Empfänger geschickt wird. Der Empfänger kann für die erhaltenen Daten eine eigene Prüfsumme errechnen und mit der empfangenen Prüfsumme vergleichen, um die Integrität und Authentizität der Sensordaten zu überprüfen

ist dieser Themenbereich praktisch spurlos an der SPS-Welt vorbeigezogen. Den meisten Steuerungen fehlen die elementaren kryptographischen Primitiven, wie Blockchiffren, Hash-Funktionen, Stromchiffren und sichere Zufallszahlengeneratoren. Daher ist schon das Grundkonzept mit Führungsgröße, Steuereinrichtung und Steuerstrecke hochgradig gefährdet das Ziel eines Cyberangriffs zu werden. Es ist z.B. relativ einfach, die Messdatenübertragung zwischen Sensoren und SPS anzugreifen und eine LüKK-Anlage zu manipulieren. Insofern gehört zu einer IoT-Sensorik auch geeignete Sicherheitsfunktionen, die Sensordaten mit einem Message Authentication Code (MAC) absichern (s. Bild 3).

Der Autor

Klaus-Dieter Walter, kdw@ssv-embedded.de, ist als CEO für die SSV Software Systems GmbH in Hannover tätig und durch zahlreiche Vorträge auf internationalen Veranstaltungen, Seminare, Workshops sowie Beiträge in Fachzeitschriften bekannt. Er hat als Autor und Coautor mehrere Fachbücher und Buchkapitel zu den Themenbereichen Embedded Linux, ARM-basierte Mikrocontroller sowie Internet der Dinge veröffentlicht. Neben seiner CEO-Tätigkeit engagiert sich Walter seit 2012 aktiv in der Expertengruppe Internet der Dinge innerhalb der Fokusgruppe Intelligente Vernetzung des Digital Gipfel der Bundesregierung. ◄