Mess- und Sensortechnik in der digitalen Transformation

Ulrich Kaiser[1], Klaus-Dieter Sommer[2]
[1]Endress+Hauser AG, Reinach, Schweiz
[2]TU Ilmenau, Ilmenau, Deutschland

Zusammenfassung

Die digitale Transformation ist über einige Ihrer Handlungsfelder unmittelbar mit der Mess- und Sensortechnik verbunden. Dafür müssen Sensoren „smart“ sein und können so Teilnehmer eines IoT-Ökosystems werden. „Smarte“ Sensoren unterstützen Diagnose und vorausschauende Wartung und können Ihren eigenen Kalibrierungsbedarf optimieren. Die IoT-Ökosysteme sind eine gute Plattform für die Fusion vieler diverser Sensoren zu Soft-Sensoren mit neuen Messgrössen. Hierfür bietet die recht neue Methodik des maschinellen Lernens neue Möglichkeiten. Der Schutz von Informationen ist bei „smarten“ Sensoren in IoT-Ökosystemen sehr viel anspruchsvoller. Da braucht es immer Massnahmen der OT-Security.

Keywords: Ökosystem für Internet of Things, Soft-Sensoren, maschinelles Lernen, OT-Security

Die DigitaleTransformation

Eine digitale Transformation geht weit über die eigentliche Digitalisierung hinaus. Digitalisierung ist die Optimierung bestehender Prozesse mit digitalen Mitteln, wobei diese Prozesse technische, aber auch Geschäftsprozesse sein können. Darüber steht die digitale Transformation, welche zusätzlich die Veränderung bestehender und/oder den Aufbau neuer (Geschäfts)-Prozesse mit den Möglichkeiten digitaler Technologien zum Inhalt hat. Nach Peters /1/ findet digitale Transformation in sieben Handlungsfeldern statt /1/, von denen drei, nämlich „Cloud and Data“, „New Technologies“ und „Process Engineering“ unmittelbar mit der Mess- und Sensortechnik verbunden sind.
Dabei sind im Besonderen die digitalen Technologien, Internetzugang, hoch leistungsfähige Embedded Systeme, Funkkommunikation und künstliche Intelligenz für die Mess- und Sensortechnik von Relevanz und erlauben dieser einen wesentlichen Beitrag zur digitalen Transformation zu leisten.

Was braucht es nun, damit ein Sensor oder ein Messsystem einen solchen Beitrag leisten kann? Diese Frage wurde von der NAMUR-Organisation in ihrer Technologie Roadmap „Prozesssensoren 4.0“ /2/ beantwortet. Sensoren müssen „smart“ sein, um so Teil des Internet of Things (IoT) werden zu können. Das bedeutet Sensoren müssen über Konnektivität und Kommunikationsfähigkeit verfügen. Sie müssen Instandhaltung und Betriebsfunktionen integrieren. Dazu gehört die Selbstdiagnose und – angestrebt – die eigene Wartung wie die Selbstkalibration. Sie müssen Fähigkeiten für Rückführbarkeit zum SI-System (Traceability) und Compliance aufweisen. Sie besitzen eine virtuelle Beschreibung von sich selbst – auch digitaler Zwilling genannt - und sind gegebenenfalls in der Lage, untereinander zu interagieren (Abbildung 1).

Abb. 1: Anforderungen an „smarte“ Sensoren (aus /2/)

Das IoT-Ökosystem für „smarte“ Sensoren

Um „smarte“ Sensoren wirksam werden zu lassen, braucht es natürlich eine angepasste Architektur des Steuerungssystems und eine Plattform für die Ausführung der Methoden: das IoT-Ökosystem. Dabei ist eine der Architekturrealisierungen die Ergänzung des klassischen geschlossenen Steuerungssystems in der Struktur der Automatisierungspyramide um ein offenes IoT-Ökosystem (Abbildung 2). In dieser Variante wird nur ein Teil der Sensordaten und Informationen im Ökosystem verarbeitet und zum Beispiel kritische Daten bleiben nach wie vor im klassischen Steuerungssystem. Eine übliche Anwendung ist die Erweiterung eines bestehenden Messsystems um Verwaltungsfunktionen zur Diagnose und Wartung der Sensoren über das Ökosystem, während die eigentliche Verarbeitung von Messdaten noch

dem vorhandenen Steuerungssystem verbleibt. Eine Realisierung einer solchen Architektur ist zum Beispiel die Namur Open Architecture (NOA /3/). Für neu zu erstellende Messsysteme übernimmt das IoT-Ökosystem auch die Aufgaben der Steuerung (Abbildung 3).

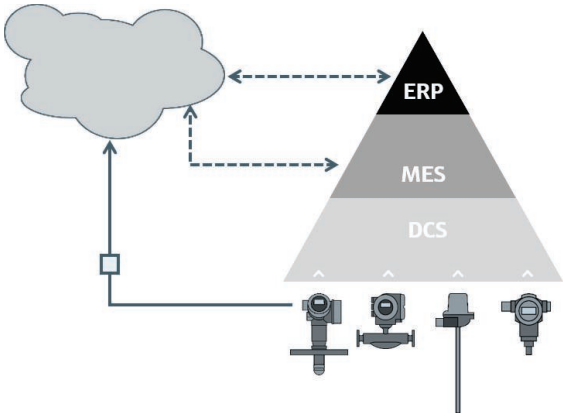

Abb. 2: Erweiterung der klassischen Automatisierungspyramide um ein IoT-Ökosystem

In einem IoT-Ökosystem werden alle Sensordaten und -Informationen in Echtzeit oder zeitnah in einer zentralen Datenbank abgebildet. Diese kann cloud-basiert oder lokal sein. Ein zentrales Rechnersystem, welches auch cloud-basiert sein kann, offeriert dann beliebige Dienste aus Daten und Informationen der Sensoren und anderen Quellen wie dem Internet. Auf diese Dienste kann dann über standardmässige Frontend-Technologien wie Mobile Apps zugegriffen werden.

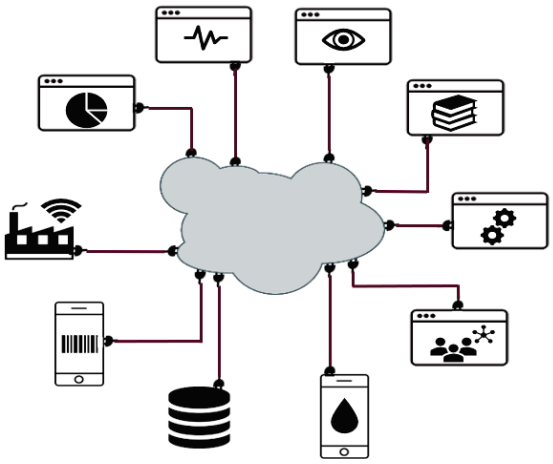

Abb. 3: Skizze eine IoT-Ökosystems

Diagnose und vorausschauende Wartung

Eine der am häufigsten diskutierten und schon oft realisierten Anwendungen auf IoT-Ökosystemen ist die Diagnose und die vorausschauende Wartung. Dabei sind Sensoren dafür erforderlich, um entweder Informationen zur Diagnose von anderen technischen Systemen oder Diagnose-Informationen für sich selbst liefern. Die Übermittlung von Diagnoseinformationen ist an sich nichts Neues; der besondere Nutzen besteht aber darin, dass in einem IoT-Ökosystem das Kollektiv aller Diagnose-informationen betrachtet werden kann, woraus dann übergreifende Informationen wie der Gesundheitszustand einer technischen Anlage und Trends ermittelt werden können.

Solche Trends können auch eine voraus-schauende Wartung ermöglichen, wenn sie behandlungsbedürftige Zustände vorhersagen können. Vorausschauende Wartung kann nach grundsätzlich zwei Prinzipien realisiert werden. Einmal über die direkte Messung eines Abnutzungsvorrats oder anderen Indikators für das Wartungsereignis. Oder aus einer längeren Beobachtungsphase heraus, wo dann reale Wartungsereignisse mit einer grossen Anzahl von Messdaten und anderen Informationen korreliert werden und so eventuell Indikatoren mittels statistischer Auswertung oder Methoden des maschinellen Lernens ermittelt werden können. Für Letzteres bietet unser IoT-Ökosystem eine geeignete Plattform. Als ein Beispiel für vorbeugende Wartung sei die frühzeitige Erkennung von Schaumbildung in Tanks genannt, die direkt über interne Messwerte von Radarfüllstandssensoren im Tank ermittelt werden kann.

Kalibrierung von Sensoren

Die Technik von Sensoren unterliegt zeitlichen Veränderungen, abhängig von der Belastung durch den Betrieb. Zur Sicherstellung der metrologischen Qualität ist daher eine regelmässige Kalibrierung und gegebenenfalls Justage der Sensoren notwendig. Die zeitliche Rate der notwendigen Kalibrierungen wird bestimmt durch das Driftverhalten des Sensors und die Kritikalität seines Einsatzes. Kalibrierungen dominieren häufig die Betriebskosten eines Sensors und deshalb ist eine Reduzierung der Rate von Kalibrierungen immer anzustreben. Ein erfolgreicher Ansatz dafür ist das regelmässige, explizite Über-prüfen von Komponenten, welche die zeitlichen Veränderungen bewirken. Diese Überprüfung passiert dabei gegen interne Referenznormalen wie zum Beispiel

(Quanten)-Normalen für die elektrische Spannung. Diese Sensorverifikation wird entweder mittels digitaler Technik im Sensor selbst oder über das IoT-Ökosystem realisiert. Über Letztere können dann auch die für eine Dokumentation notwendigen Zertifikate automatisch publiziert werden.
Die angestrebte Ideallösung ist, Referenznormale – möglichst mit direkter Rückführbarkeit auf das (aktuelle) SI – in Sensoren oder dem Messsystem zu integrieren. Dann könnte der Sensor ohne jegliche externe Infrastruktur und Aufwand sich selber kalibrieren. Das National Institute of Standards and Technology der USA (NIST) hat diese große technologische Herausforderung mit ihrem NIST-on-a-Chip-Projekt in Angriff genommen /4/. In diesem Projekt sollen Referenznormale mikrotechnisch konstruiert werden, die in Sensoren integriert werden können /5/.

Soft-Sensoren

Soft-Sensoren sind Messsysteme, wo schwierig zu messende Messgrössen aus einer Mehrzahl von einfach zu messenden Messgrössen errechnet werden /5/. Schwierig zu messende Messgrössen sind diejenigen, für die kein direktmessendes Messsystem zur Verfügung steht, zum Beispiel für bestimmte stoffliche Eigenschaften, wo der Ort der Messung nicht zugänglich ist oder wo eine Vorhersage eines zukünftigen Messwertes gefordert ist. Die Gesamtheit der Eingangs-Messgrössen muss natürlich die Ergebnis-Messgrösse repräsentieren können. In /6/ ist das Verfahren zur Entwicklung eines Soft-Sensors beschrieben, der aus den Informationen von 85 „einfachen“ Sensoren die Konzentration einer Substanz in einem chemischen verfahrenstechnischen Prozess berechnen kann. Als technische Plattform für solche Soft-Sensoren ist unser IoT-Ökosystem wieder sehr gut geeignet. Für die Berechnung der gewünschten Messgrösse aus den Eingangsdaten gibt es zwei grundsätzliche Verfahren, das modellgetriebene und das datengetriebene. Beim modellgetriebenen Verfahren muss der Zusammenhang zwischen den Eingangsgrössen und der Ausgangsgrösse - der gewünschte Messwert - bekannt und analytisch darstellbar sein. Bei den datengetriebenen Verfahren wird die Beziehung zwischen Eingangsgrösse und der gewünschten Messgrösse anhand von Trainingsdaten erlernt. Die Trainingsdaten der gewünschten Messgrösse müssen dann natürlich auf eine andere Art und Weise beschafft werden. In dem erwähnten Beispiel durch separate Labormessungen.

Für die datengetriebenen Verfahren gibt es eine grosse Anzahl von mathematischen Verfahren, von der einfachen Regressionsanalyse bis zum Deep Learning, Letzteres ist eine Methode des maschinellen Lernens, dieses wiederum eine Disziplin der künstlichen Intelligenz /7/. Moderne Cloud-Systeme von Amazon, Google, Microsoft, …, auf denen die IoT-Ökosysteme häufig aufgebaut sind, bieten eine Vielzahl von Tools für solche Berechnungen an.

Informationssicherheit für die Mess- und Sensortechnik

Werden Sensoren und Messsysteme Objekte des Internet of Things, so werden Sie auch verwundbar wie die anderen Objekte des Internets. Manipulationen von Sensordaten und Unterbrüche von Kommunikations-Verbindungen können gefährliche Auswirkungen haben. Ebenso kann das unautorisierte „Mithören“ von Sensordaten bei bestimmten Applikationen unerwünscht sein. Die OT-(Operational Technology)-Security befasst sich mit der Informationssicherheit von technischen Systemen /8/. Dabei finden die gleichen Methoden und Massnahmen der Informationssicherheit Anwendung wie Verschlüsselung, Authentifizierung, etc., um den für jede Kritikalität der Anwendungen benötigten Schutz zu gewährleisten.

Literaturnachweis

[1] Marc K. Peter (Hrsg.) KMU-Transformation: Als KMU die digitale Transformation erfolgreich umsetzen; *FHNW Hochschule für Wirtschaft*, Olten, Schweiz, (2017); https://kmu-transformation.ch/

[2] Technologie-Roadmap "Prozess-Sensoren 4.0", VDE/VDI, NAMUR, 2015

[3] NAMUR Open Architecture; *Interessengemein-schaft Automatisierungstechnik der Prozess-industrie e.V.;* https://www.namur.net/fokusthemen/namur-open-architecture.html

[4] NIST on a Chip; https://www.nist.gov/pml/productsservices/nist-chip-portal

[5] Th. Simmons, G. Gerlach, K.-D. Sommer: Linking Innovators in Sensors and Measurement Technology. NIST - Visitors' Seminar, Gaithersburg, 2019-04-10

[6] Marcin Budka et al. (2014) From Sensor Readings to Predictions: On the Process of Developing Practical Soft Sensors. In: Blockeel H., van Leeuwen M., Vinciotti V. (Hrsg) *Advances in Intelligent Data Analysis XIII. IDA 2014. Lecture Notes in Computer Science*, Band 8819. Springer,

[7] Wolfgang Ertel, Grundkurs Künstliche Intelligenz; Eine praxisorientierte Einführung; *Springer Vieweg*; 4. Auflage, (2013)

[8] IEC 62443-3 Security for industrial process measurement and control – Network and system security