Customized IoT Gateways in der Industrie

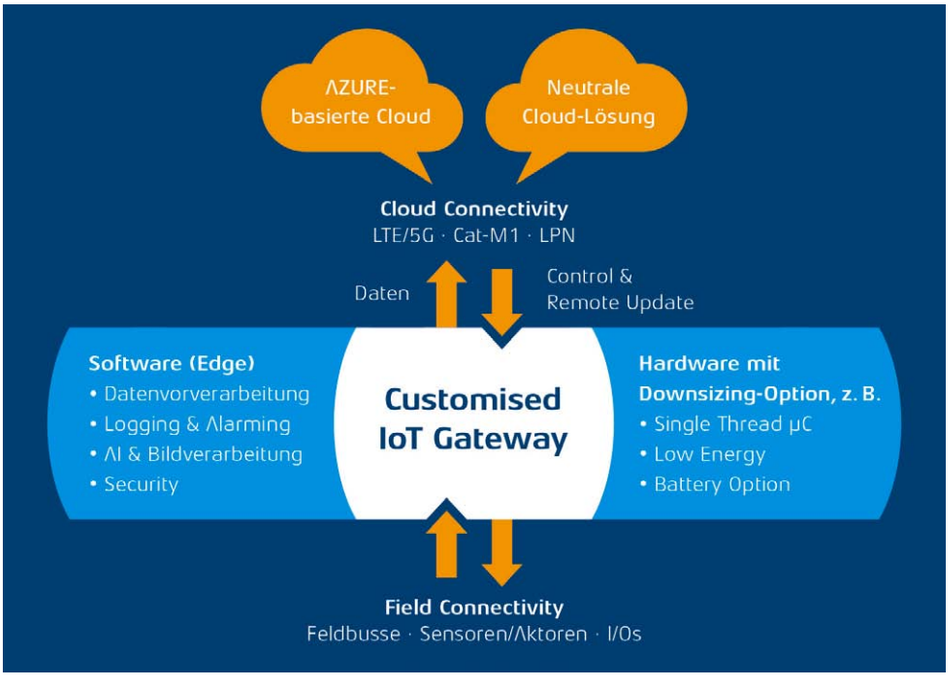
# Das IoT Gateway als Digitalisierungs-Agent

*Eine IoT-Anbindung gehört für immer mehr Maschinen und Anlagen zum Standard. Entsprechende Produkte müssen sicher und Support-arm sein, weltweit möglichst flächendeckend Internetverbindungen herstellen können und Betriebsdaten in Cloud-Umgebungen speichern können. Die Anforderungen an IIoT Gateways sind deshalb beträchtlich.*

Von Roger Hügli, Bereichsleiter Controls & Displays bei Grossenbacher Systeme

Ob Betriebsstundenzählung, Sammlung umfassender Nutzungs- und Maschinendaten für Predictive Maintenance, Remote Updates oder Fernsteuerung – die Einsatzbereiche und die sich daraus ergebenden Anforderungen an IoT Gateways sind so vielfältig wie die möglichen Wireless-Techniken zur Internet-Anbindung. Schon diese Tatsache verdeutlicht, dass die Entwicklung solcher Komponenten für die meisten Maschinenbauer jenseits ihrer Kernkompetenz liegt. Der Einkauf bei spezialisierten Anbietern wie etwa Grossenbacher Systeme liegt deshalb nahe. Doch selbst die Auswahl des passenden IoT Gateways ist alles andere als trivial.

Bild: Grossenbacher Systeme




**Customized IoT-Gateways stehen im Zentrum digitalisierter Automatisierungssysteme auf IoT-Basis.**

Die Komplexität, die für Entwicklung, Auswahl und Einsatz von IoT Gateways kennzeichnend ist, lässt sich an einer ganzen Reihe von Faktoren festmachen. Der erste betrifft Art und Umfang der zu sammelnden Daten sowie den gewünschten Steuerungsumfang. Die zweite Kernfrage ist die nach der Internet-Verbindungstechnik sowie ihrer regionalen Verfügbarkeit und erzielbaren Bandbreite. Allein die oft sinnvolle Integration unterschiedlicher Funktechniken und deren weltweiter Einsatz – Stichwort Roaming – kann eine Herausforderung technischer und administrativer Art darstellen. Aus Datenmenge und Bandbreite leitet sich die Frage ab, ob das Gateway über eine Edge-Funktion zur Vorverarbeitung der Daten verfügen sollte. Ist das der Fall, können künstliche Intelligenz und Machine Learning auch in modernen Embedded-Systemen zum Thema werden. Das Maß an Intelligenz entscheidet gemeinsam mit der Schnittstellen-/Sensorik-Ausstattung und der gewählten Funktechnik darüber, ob Batteriebetrieb zumindest möglich wäre.

Mit energieeffizienter Embedded Hardware und bei Nutzung von Low-Power-Netzwerken für die Kommunikation wären derartige batteriebetriebene Produkte durchaus eine Option. Das gilt vor allem für weniger komplexe Maschinen, die sich mit einer geringeren Zahl von Datenpunkten überwachen lassen. Hier gewinnen unabhängig von der Stromversorgung Wirtschaftlichkeitserwägungen die Oberhand: Existiert nur eine begrenzte Menge von Datenpunkten, muss das IoT Gateway dies preislich widerspiegeln – was eine zusätzliche Herausforderung darstellt: Eine sichere Remote-Update-Funktion wie in Linux-basierten Gateways in einem Mikrocontroller- bzw. Firmware-basierten und deshalb kostengüns-

tigeren System zu realisieren ist alles andere als trivial. Hierfür müssen Unternehmen, wie bei Grossenbacher Systeme der Fall, mehrere Kompetenzbereiche zugleich beherrschen: die Integration von Sensorik und Wireless-Netzwerken, die sichere Kommunikation mittels Mikrocontrollern etwa auf TLS-Basis und schließlich die Integration des Microsoft Azure IoT Frameworks.

Zentrale Aufgabe eines IoT Gateways ist natürlich die Übertragung der Daten von und zur Cloud. Geleistet wird sie von Kommunikationsmodulen, die es für diverse Kommunikationsstandards gibt. Von besonderer Bedeutung ist zusätzlich die Wahl des Roaming-Anbieters, entscheidet sie doch darüber, ob und inwieweit eine weltweite Datenübertragung möglich ist. Will man mehrere Techniken wie LTE, CAT-M1 und NB-IoT nutzen können, so muss der Datenverkehr an deren Möglichkeiten angepasst werden – Remote Updates sind unter Umständen nicht in allen Fällen möglich. Übrigens empfiehlt es sich nach Erfahrung von Grossenbacher Systeme, weiterhin auf klassische SIM-Karten statt auf die moderneren eSIM-ICs zu setzen. Der Grund liegt in der größeren Flexibilität beim Anbieterwechsel: Der Wechsel einer SIM-Karte ist verglichen mit einem Austausch der eSIM ein Kinderspiel – gerade im Feld und bei langer Einsatzdauer der IoT Gateways.

### *Cloud oder individuelle Datenhoheit?*

Eine mindestens ebenso große Herausforderung wie die Hardware stellt die Software dar – einschließlich der Auswahl der Cloud-Anwendung und des Partners dafür sowie der Integration der entsprechenden Anbindungssoftware im IoT Gateway. Mit dem Azure IoT Framework bietet Microsoft eine Umgebung, die sowohl für die Geräte als auch in der Cloud einen großen Funktionsumfang bietet – Remote Update eingeschlossen. Die Revisionsverwaltung muss dabei allerdings selbst erstellt werden. Die Cloud muss den aktuellen Hardware-Stand der jeweiligen Maschine kennen und Updates entsprechend steuern. Das erfordert komplexe manuelle Anpassungen, für die der Cloud-Spezialist auch etwas von Automatisierung und Embedded-Hardware im Feld verstehen sollte.

Eine weitere Herausforderung im Zusammenhang mit dem Azure IoT Framework ist die Synchronisation der Datenpunkte: Welche Informationen müssen mit welcher Häufigkeit übertragen werden? Gerade bei Datenobjekten mit Array-Strukturen kann dies bei Azure zu einem Stolperstein werden, wohingegen der einzelne Datenpunkt problemlos ist.

Nicht unproblematisch ist auch die Rechteverwaltung. Nehmen wir das klassische Szenario: Ein Maschinenbauer bietet seinen Kunden ein Cloud-basiertes Produkt an; jeder Kunde ist ein Mandant. Schnell tangiert ein Datenzugriff in die Cloud oder vom IoT Gateway grundlegende Privilegien bzw. Benutzerrechte. Stellt ein Kunde seine IT-Richtlinien um, so kann dies zu Problemen im Datenverkehr führen und die Maschine im Feld unerreichbar machen.

Gerade mittelständische Maschinenbauer und deren Kunden haben zudem – berechtigt oder nicht – bisweilen Bedenken, was die Aufbewahrung heikler Daten in der Azure Cloud betrifft. Es gibt also viele Argumente für Azure, aber auch gute Gründe, die Datenhoheit individuell zu gestalten. Für alle, die letztere Variante bevorzugen, arbeitet Grossenbacher Systeme mit dem deutschen Clouddanbieter Sabo Mobile IT zusammen. Gemeinsam bieten beide Unternehmen individuelle Lösungen für Field Device Management inklusive Hard- und Firmwarestand sowie Service-Informationen bei hochsicherer Datenhaltung an.

Eine weitere Herausforderung strategischer Art für Maschinenbauer stellt die Wahl des passenden Partners für IoT Gateways dar. Sie wird dadurch erschwert, dass Hard- und Software nicht ohne Weiteres aus einer Hand zu bekommen sind. Durch die eigene Azure-Kompetenz und die Zusammenarbeit mit Sabo Mobile IT kann Grossenbacher Systeme hier mit einem Angebot aus einer Hand auftreten.

Die Entscheidung für das passende IoT Gateway ist also für Maschinen- und Anlagenbauer schon heute eine wichtige und komplexe Frage, deren Bedeutung mit wachsender Verbreitung des IoT sogar noch zunehmen wird. Sie sind deshalb gut beraten, sich einen Partner zu suchen, der die Anforderungen „kleinster Footprint mit Option Batteriebetrieb" und „maximale Intelligenz für KI- und ML-Anwendungen" ebenso beherrscht wie die Sicherheits- und Kommunikationsanforderungen moderner Cloud-Systeme. Aus Sicht von Grossenbacher Systeme ergeben erst Erfahrungen in Messtechnik und robuster Elektronik-Entwicklung sowie Produktionskompetenz ein Gesamtangebot, das Maschinenherstellern einen Fokus auf die Kernkompetenzen erlaubt und ihnen zugleich eine erfolgversprechende Digitalisierungsperspektive eröffnet. (ak) ■