Auf die Schnelle

Das Wesentliche in 20 Sek.

- Secure Cloud Gateway rückt Security-Aspekt in den Fokus
- einfach zu handhaben
- Schlüsselschalter am Gerät verhindert Manipulationen
- Modularer Ansatz unterstützt gängige Feldbusse

später lesen/ weiter empfehlen

QR2mail

INTERVIEW MIT MICHAEL M. REITER UND SIEGFRIED MÜLLER

Nach unten flexibel, nach oben sicher

Wer Industrie 4.0 und IoT in der Produktion einführen will, braucht eine gleichermaßen flexible und sichere Kommunikationsinfrastruktur. Dazu haben sich Deutschmann Automation und MB connect line intensiv Gedanken gemacht und mit dem Secure Cloud Gateway eine ebenso interessante wie einfache Lösung kreiert, die die Geschäftsführer Michael M. Reiter und Siegfried Müller erläutern.

Herr Reiter, wie ist es zu der Kooperation zwischen MB connect line und Deutschmann Automation gekommen?

Reiter: Unsere Zusammenarbeit reicht inzwischen rund 15 Jahre zurück. Wir haben ja vor 15 Jahren schon das erste Mal gemeinsam auf der SPS IPC Drives ausgestellt. Und aus der Geschäftsfreundschaft ist längst auch eine private entstanden. Das Thema Kommunikation passt zu beiden Firmen und wir haben schon vor rund zehn Jahren darüber sinniert, die Feldbuskommunikation in die Fernwartung zu integrieren, das heißt die Unigate ICs in die M2M-Router.

Müller: Nur, damals waren die Anwendungen, die Geschäftsmodelle noch nicht da. Man hat keinen Nutzen darin gesehen, Daten über den Feldbus abzugreifen. Und für die reine Fernwartung hat es keinen wirklichen Nutzen gebracht, weil die davon lebt, dass man bei Bedarf auch auf die Steuerung Zugriff hat.

Reiter: Erst mit den Themen wie Monitoring und Datensammlung haben wir das Thema jetzt wieder aufgegriffen und eine Lösung umgesetzt.

> *Mit unserer einfachen Vorgehensweise ist das System schon vom Design her sicher.*
>
> **Michael M. Reiter**

Wie sieht die Arbeitsaufteilung aus?

Reiter: Deutschmann Automation liefert den Part der Feldbusanbindungen. MB connect line steuert das Know-how in Sachen Cloud und Fernwartung bei. Das sind die Zutaten für unser erstes gemeinsames Produkt, das Secure Cloud Gateway.

Müller: Wir gehen damit den nächsten logischen Schritt in unserer Partnerschaft. Wir haben das Potenzial erkannt, die beiden Komponenten zu verbinden, das Thema Feldbus und Cloud zusammenzuführen. Im Vergleich zu anderen Konzepten haben wir hier mit Sicherheit einen gewissen Vorteil.

Sie betonen die einfache und sichere Handhabung Ihrer Cloud-Gateways. Warum ist Ihnen Security so wichtig?

Müller: Wir kennen die Diskussionen über IT-Sicherheit und Cyber Security im Rahmen unserer Fernwartungslösung schon lange. Und IT-Sicherheit bedeutet letztendlich immer auch eine gewisse Disziplin beim Anwender. Wenn man sich die Szenarien heute anschaut, ist der Mensch eigentlich der größte Schwachpunkt in der Sicherheitskette. Deswegen war es uns sehr wichtig, dass die Handhabung der Gateways schon von sich aus quasi keine Lücke in die ‚Festung Netzwerk' reißt.

Was meinen Sie damit?

Müller: Bei einer typischen Firewall muss man konfigurieren, ob und welche Zugänge aufgemacht werden und sie müssen wieder geschlossen werden, etwa nach einem Service-Zugriff. Der Klassiker schlechthin ist, dass vergessen wird, diese Türen wieder zu schließen.

Reiter: Deswegen haben wir konsequent das Thema Security by Design umgesetzt, wie es etwa das BSI empfiehlt, eigentlich State of the Art ist, aber im Automatisierungssektor nie im Vordergrund stand. Denn hier lag der Fokus schon immer auf der operativen Steuerung. Jetzt muss man auf der Automatisierungsseite den Security-Part hinzufügen. Deswegen war für uns die einfache Handhabbarkeit und Adaptierung wichtig. Daher auch der Schlüsselschalter am Gerät, über den zum Beispiel die Zugriffsrechte zusätzlich geregelt sind und ganz simpel administriert werden.

Das klingt so, als hätten Sie jetzt nicht unbedingt Vertrauen in das Know-how der Automatisierer und der Maschinen-/Anlagenbauer im Bereich Security?

Reiter: Das ist keine Frage des Vertrauens oder Know-hows, wie Sie es formulieren. Wir haben einfach eine technische Lösung gewählt, die von vornherein die Risiken minimiert. Natürlich

Michael M. Reiter (links), Deutschmann Automation, und Siegfried Müller, MB connect line

kann auch jemand den Schlüsselschalter auf bidirektionalen Verkehr einstellen und vergessen, den Schlüsselschalter wieder zu entfernen – ein Klassiker, den viele kennen. Das können auch wir nicht ausschließen. Aber da unsere Lösung auf einer Hardwareschaltung basiert, kann sie niemand per Software überlisten. Wir nennen unser Konzept die hardbasierte Daten-Diode; der Schwachpunkt Software ist somit gar nicht erst vorhanden.

Müller: Ich habe früher selbst Maschinen projektiert und programmiert. Daher kann ich sehr gut nachvollziehen, welche Arbeiten Automatisierer eigentlich machen. Das reicht von der Programmierung der Steuerung bis zur Antriebstechnik, Bedienpanels und Visualisierung und dann noch Feldbus, Netzwerktechnik und Security dazu. In diesem Kontext ist unser Ansatz der einfachen Handhabung zu sehen, zumal es in vielen Firmen nicht für jeden dieser Bereiche einen Spezialisten gibt. Daher begrüßen viele Anwender die einfache Handhabung per Schlüsselschalter, mit dem wir ihnen die Arbeit ein Stück weit abnehmen.

Wie funktioniert denn die Daten-Diode konkret?

Müller: Für uns ist wichtig, die Transparenz so weit darzustellen, dass schon ein Zugriff von außen nach innen hardwarebedingt nicht möglich ist. Das ist die Grundidee unseres Konzeptes, das jeder versteht: Eine sichere Hardwarebeschaltung, wie man sie aus der funktionalen Sicherheit kennt.

Reiter: Im Prinzip setzen wir auf einer seriellen Schnittstelle auf, bei der aber nur ein Kanal nach außen freigeschaltet ist. Nur über den Schlüsselschalter lässt sich dann der bidirektionale Datenverkehr aktivieren beziehungsweise deaktivieren.

Müller: Dazu sind zwei Prozessoren in den Gateways integriert, bei denen quasi die Tx-Leitung des Feldbus-Prozessors der Unigate-ICs mit dem Rx-Eingang des Cloud-Prozessors hart verdrahtet ist. Nur der Rückkanal ist gewissermaßen über den Schlüsselschalter und eine Transistorschaltung zuschaltbar.

Haben Sie sich dieses Prinzip patentieren lassen?

Reiter: Das Konzept mit einem Schlüsselschalter für Freigaben ist nicht neu. Das angemeldete Patent bezieht sich in erster Linie auf die Gewährleistung der Sicherheit durch die Reduzierung auf einen Datenrichtungskanal mittels unserer Daten-Diode.

Und wie kommen die Daten in die Cloud?

Müller: Wir müssen zwei Themen unterscheiden: Wie bringe ich die Daten von der Maschinenebene zur Cloud, ist das eine The-

„Das Bewusstsein für die Problematik Datensicherheit könnte generell noch ausgeprägter sein."

Michael M. Reiter

„Feldbus-Gateways mit Fernwartung zu kombinieren – die Idee hatten wir schon vor zehn Jahren."

Siegfried Müller

ma. Wie die Daten von der Cloud zur Applikation kommen, das andere. Für beides zeichnet sich am Markt aktuell ab, OPC UA zu nutzen, in Kombination mit einem Publisher/Subscriber-Verfahren analog zu MQTT. Nur eines wird aus meiner Sicht für den Transfer Maschine – Cloud zu wenig beachtet, ein bisschen unter den Tisch gekehrt: die vorhandenen Kommunikationslayer, die draußen im Feld überhaupt zur Verfügung stehen.

Alle Konzepte rund um IoT und Industrie 4.0 basieren darauf, dass niemand den Stecker zieht, dass Mobilfunk oder Netzwerk immer da ist und nie gestört ist. Jeder geht also von einer hundertprozentigen Verfügbarkeit der Layer-2-Kommunikation aus. Nach fast 20-jähriger Fernwartungserfahrung weiß ich: Das ist nicht so.

Daher haben wir unsere Technologie so konzipiert, dass wir bei Verbindungsunterbrechungen in den Systemen die Daten zwischenspeichern und nach einem Abbruch die Kommunikation auch relativ schnell wieder aufbauen können – ohne großen Kommunikations-Overhead wie beispielsweise bei OPC UA.

Bilder: Redaktion IEE

Über einen Schlüsselschalter am Gerät lassen sich Zugriffsrechte regeln.

Denken Sie denn nicht darüber nach, OPC UA in Ihre Cloud-Gateways mit zu implementieren, als Schnittstelle letztendlich in andere Systemwelten?

Müller: Der erste Schritt ist, OPC UA als Serverfunktion in die Cloud zu implementieren. Wir sorgen schon dafür, dass die Daten effizient in die Cloud kommen. Für die sogenannte Third-Party-Anbindung, also wie vorher gesagt die Applikation, unterstützen wir bereits verschiedene Formate wie CSV, Excel oder My SQL. Der zweite Schritt wird sein, OPC UA direkt in den Geräten zu implementieren, um zum Beispiel den Applikationen den direkten Zugriff auf die Maschinenebene zu geben.

Wie sicher ist denn ihre Cloud-Infrastruktur?

Müller: Durch unsere Zusammenarbeit und Mitgliedschaft bei Teletrust sind wir da sehr stark involviert und sensibilisiert. Aktuell gibt es Zertifizierungen für die IT-Sicherheit, die ‚Common Criteria for Information Technology Security Evaluation' zum Beispiel. Diese Zertifizierung ist für ein mittelständisches Unternehmen eigentlich nicht realisierbar, weil sie mit sehr hohen Kosten verbunden ist. Wir lassen daher regelmäßig Sicherheitsaudits durchführen und mindestens einmal im Jahr externe Penetrationstests durch wechselnde BSI-zertifizierte Unternehmen.

Und diese Unternehmen prüfen nach den BSI-Richtlinien?

Müller: Das Hauptproblem ist die Normenlage. Es gibt die IEC62443, Common Criteria, den BSI-Grundschutz und das ICS-Kompendium vom BSI. Woran sollen sich Anwender halten? Es gibt keine konkrete Vorschrift, sondern nur Empfehlungen. Wenn eine Norm kommen würde, wäre es für Maschinenbauer und Anwender leichter. Deswegen kann man aktuell eigentlich keine ernstzunehmende Zertifizierung machen, die erschwinglich wäre. Und wenn ein Wettbewerber aktuell ein Zertifikat ausstellt, dass Industrie-4.0-zertifiziert ist, dann ist das nichts anderes als ein Marketing-Buzz. Das hat keinerlei rechtliche Grundlage.

Reiter: Security ist für jemanden wie MB connect line, der Fern-

„Wir führen die Themen Feldbus und Cloud in einem Gerät zusammen."

Siegfried Müller

„Daten lesen geht immer, Schreiben und Konfigurieren nur per Schlüsselschalter."

Michael M. Reiter

wartungslösungen betreibt, eine Kernkompetenz. Wenn hier das Vertrauen fehlt, gibt es keine Geschäftsgrundlage. Man darf auch die anderen Aspekte von Security nicht vergessen, die Manipulation. Die verhindern wir mit unserer Technologie ebenso nachhaltig. Es kann niemand in das bestehende Feldbussystem – sprich in meine Fabrik, in meine Anlage – eindringen und die SPS umprogrammieren. Das ist ja auch ein Gefahrenpotenzial, das der Schlüsselschalter nachhaltig unterbindet.

Die Kommunikation im Feld ist die Expertise von Deutschmann Automation. Welche Systeme werden denn zum Start verfügbar sein und wie wollen Sie die zigtausenden von installierten alten Maschinen mit in die Cloud-Szenarien integrieren?

Reiter: Damit haben wir uns intensiv befasst, weil der Nachrüstmarkt sicherlich ein interessanter Einstieg für unser Produkt sein wird. Für die existierenden Anlagen entwickeln wir verschiedene Varianten, allen voran MPI und Modbus. Darüber hinaus stehen zum Start natürlich auch Profibus, Profinet und Ethernet zur Verfügung.

Müller: Später wird es auch eine reine serielle Implementierung geben, für die ganz alten Systeme. Der Fokus liegt in erster Linie auf der Nachrüstung. Wenn jemand wirklich in Industrie 4.0 einsteigen will, dann braucht er in erster Linie Daten aus seinem existierenden Maschinenpark, denn seinen bestehenden Maschinenpark will er dafür sicher nicht erneuern.

Reiter: Deswegen beginnen wir auch mit Bussystemen, die eine Master/Master-Kommunikationen unterstützen. Denn hier braucht man in die bestehende Steuerungstechnik nicht einzugreifen und kann die Gateways einfach aufsetzen. Wenn der Markt ein noch nicht implementiertes Bussystem erwartet, dann können wir auf unseren umfangreichen Fundus zurückgreifen und dieses System nachziehen.

Wie haben Sie die Modularität umgesetzt?

Reiter: Wir setzen hier das Unigate IC ein, das für die verschiedenen Feldbusvarianten verfügbar ist. Softwareseitig sind dann lediglich die Kommunikation zwischen Cloudseite und Feldebene anzupassen.

Sie haben die Datenspeicherung bei Verbindungsstörungen erwähnt. Das setzt eine gewisse Leistungsfähigkeit Ihrer Gateways voraus. Braucht das nicht auch unterschiedliche Gateway-Varianten?

Müller: Unsere klassische Routerplattform erfährt genau unter diesem Aspekt ein Redesign und bekommt unter anderem mehr Ressourcen hinsichtlich Speicher und Prozessorleistung, um die Daten auch länger puffern zu können. Unter anderem wird es einen zusätzlichen Steckplatz für SD-Karten geben.

Gibt es da auch so eine Art Time Out, nach dem das Gateway Alarm schlägt, wenn der Schlüsselschalter nicht wieder verriegelt wird?

Müller: Das ist werksseitig vorkonfiguriert und wir empfehlen jedem eine Signallampe über den vorhandenen digitalen Ausgang anzuschließen, die das signalisiert. Aber wie jede überlagerte Alarmierung könnte auch das bei der Erstkonfiguration ausgeschaltet werden.

Reiter: Der Schlüssel gehört grundsätzlich eigentlich nicht ans Gerät.

Und wann sind die Geräte verfügbar?

Reiter: Wir werden Sie auf der SPS IPC Drives 2016 vorstellen. Im zweiten Quartal 2017 soll die Serie dann auf den Markt kommen. ○

Das Interview führte Stefan Kuppinger, Chefredakteur IEE

Auf die Schnelle

Das Wesentliche in 20 Sek.

- Zum Patent angemeldete Schaltung mit Schlüsselschalter verhindert Manipulation von außen
- Modulare Kommunikationsbaugruppen sorgen für Flexibilität im Feld
- Flexible Infrastruktur – erst public, später private Cloud

später lesen/ weiter empfehlen

Vom Feldbus sicher in die Cloud

Nachrüstbare Secure Cloud Gateways zur zuverlässigen Datenkommunikation im IoT

Mit den Secure Cloud Gateways schlagen Deutschmann Automation und MB connect line eine sichere und zuverlässige Brücke von der Feldbus-Ebene in die Welt des Internets. Als Kernbausteine für Industrie-4.0-Anwendungen ermöglichen sie Nutzern und Anwendungen über eine sichere Verbindung den Zugriff auf wichtige Daten aus der Produktion.

Autoren: Michael M. Reiter, Siegfried Müller

Die steigende Zahl bekannt gewordener Fälle von Hackerangriffen zeigt Wirkung: Das Bewusstsein für IT-Sicherheit ist deutlich gestiegen; die Sicherung von Geräten und Netzen, um Angriffe abzuwehren und sensible Daten zu schützen, ist daher wesentlicher Bestandteil vieler Projekte.

Eine sichere Datenkommunikation in der vernetzten Industrie der Zukunft ist dabei ein wichtiger Baustein. Dieser Aufgabe haben sich die beiden mittelständischen Unternehmen Deutschmann Automation und MB connect line im Rahmen einer strategischen Partnerschaft gestellt. Deutschmann Automation mit Sitz in Bad Camberg entwickelt und fertigt bereits seit zwei Jahrzehnten Protokollkonverter, Feldbus- und Industrial-Ethernet-Gateways und Embedded-Lösungen sowie passende Entwicklungswerkzeuge. MB connect line ist spezialisiert auf Lösungen zur Fernwartung von Maschinen, Anlagen und Infrastruktur über das Internet. Kernkomponente ist die zentrale Remote-Service-Plattform mbConnect24 als universelle Lösung für Fernwartung, Datenerfassung und M2M-Kommunikation.

Beide Unternehmen haben ihre sich ergänzenden Kompetenzen in einem gemeinsamen Projekt gebündelt, dem Secure Cloud Gateway. Ziel ist, eine sichere und zuverlässige Datenkommunikation

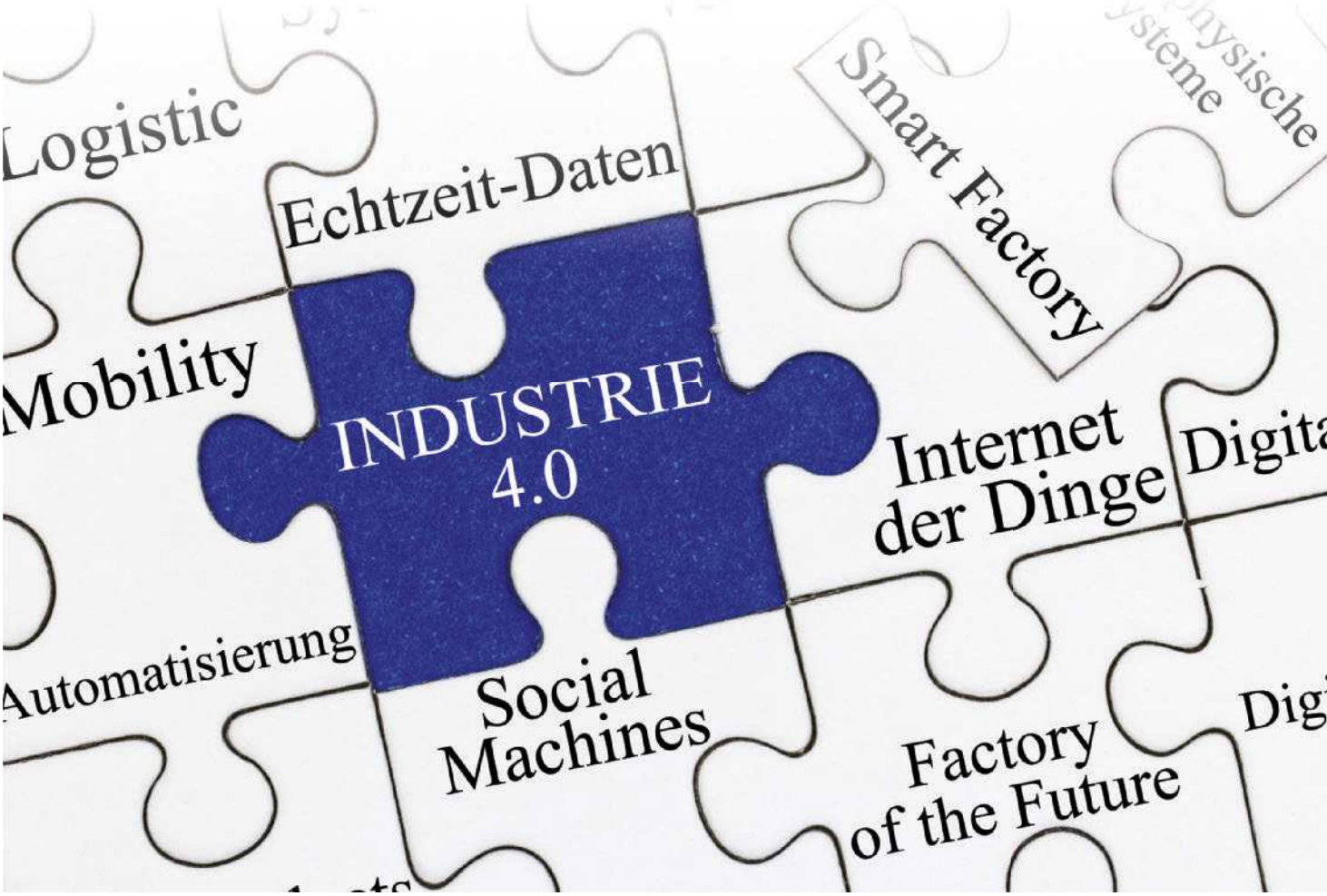


Bild: Magele-Picture,Elfstudioart/Fotolia.com

von der Feldbus-Ebene in die Welt des Internets im Industrie-4.0-Umfeld zu gewährleisten. Für einen wirksamen, das heißt hundertprozentigen Schutz gegen einen unautorisierten Zugriff von außen auf die sensitiven Bereiche und Daten der Feldebene, sorgt ein zum Patent angemeldetes Konzept.

Ein weiterer Aspekt ist die Integration der Secure Cloud Gateways, sowohl in bestehende Anlagen als auch für neue Installationen. Entsprechend flexibel sind die Geräte in der Busanschaltung (beispielsweise MPI, Profinet, Modbus) und in der Kommunikationstechnologie zum Internet (Mobilfunk, WiFi) ausgelegt.

Security-Branche profitiert von Industrie 4.0

Durch die stetig zunehmende Digitalisierung und der damit einhergehenden Durchdringung der IT ist es von zentraler Bedeutung, dass Unternehmen in den Schutz ihres Know-hows investieren. Die Studie ‚Der IT-Sicherheitsmarkt in Deutschland' des Bundesministeriums für Wirtschaft und Energie, kommt zu dem Ergebnis, dass die IT-Sicherheitswirtschaft eine der leistungsfähigsten Zukunftsbranchen in Deutschland ist. Die IT-Sicherheit verzeichnete, so die Studie, im Zeitraum 2005 bis 2013 ein überproportionales Wachstum von durchschnittlich 7,3 % pro Jahr. Die Importquote von nur etwa 20 % in 2012 macht deutlich, dass die Nachfrage nach IT-Sicherheitsprodukten und -dienstleistungen in Deutschland vorwiegend durch heimische Produktion gedeckt wird und sich die Branche im internationalen Wettbewerb gut behaupten kann. Angesichts der zunehmenden Vernetzung industrieller Leit- und Regelungssysteme im Industrie-4.0-Umfeld wird die IT-Sicherheit auch in Zukunft ein attraktives und wichtiges Geschäftsfeld bleiben.

Einer Studie der deutschen Wirtschaftsprüfungs- und Beratungsgesellschaft PwC zufolge, will die deutsche Industrie bis 2020 jährlich bis zu 40 Milliarden Euro in Industrie-4.0-Projekte investieren. Das Ziel sind Effizienzsteigerungen und Kosteneinsparungen, aber auch qualitative Vorteile wie mehr Flexibilität und die Möglichkeit, auf individuelle Kundenwünsche einzugehen.

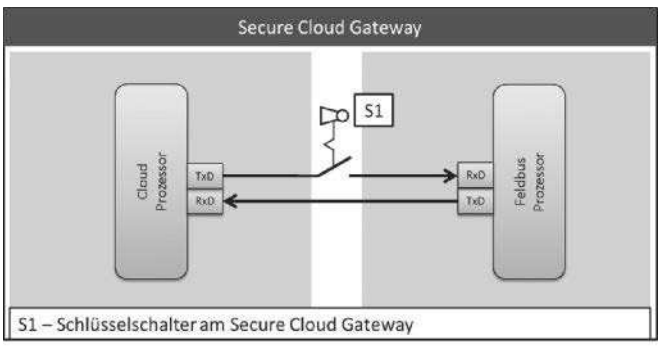
Anlagen ohne Risiken nachrüsten

In klassischen Fabriken findet man vernetzte, jedoch oft ungeschützte Steuerungssysteme. Diese Systeme wurden ursprünglich nicht für eine hochgradige Vernetzung entwickelt und haben den Fokus auf der operativen Steuerungsfunktion. Die Nachrüstung von Industrie 4.0 in solchen Bestandsanlagen ist problematisch, da die daraus resultierende Verbindung zum Internet ein hohes Sicherheitsrisiko birgt und somit hohe Anforderungen an die IT-Sicherheit stellt. Ebenso dürfen in der Regel an den Anlagen keine Veränderungen vorgenommen werden. Auch diese Gegebenheiten – nachträgliche Integration bei höchstem Sicherheitsniveau – wurden im Konzept berücksichtigt.Daher lassen sich die Secure Cloud Gateways integrieren, ohne dass in die Anlagenkonfiguration eingegriffen werden muss – vorausgesetzt das in den Bestandsanlagen installierte Bussystem unterstützt eine Master/Master-Kommunikation. Typische Vertreter dieser Feldbus-Kategorie sind beispielsweise MPI, Profibus und Modbus-Systeme. Bei Neuinstallationen gibt es diese Einschränkung nicht, da die Master/Slave-Strukturen bereits in der Planungsphase berücksichtigt werden und geeignete Bussysteme zum Einsatz kommen.

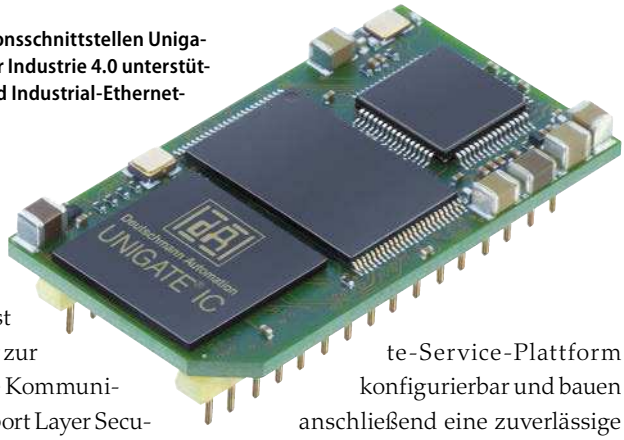
Hardware-Schloss nicht zu knacken

Die Secure Cloud Gateways garantieren eine Hardware-basierte IoT-Sicherheit, die im Gegensatz zu Software-Lösungen nicht überlistbar ist. Grundlage dafür bildet eine zum Patent angemeldete Hardware-Daten-Diode. Aktiviert, erlaubt sie ausschließlich die Kommunikation in eine Richtung – von der Datenquelle zur Cloud-Schnittstelle. Eine Kommunikation von der Cloud-Schnittstelle zur Datenquelle ist dagegen Hardware-technisch gesperrt. Die beiden Prozessoren auf der Feldbus- und Cloud-Seite sind über eine einkanalige, serielle Verbindung gekoppelt, die beide Kommunikationskanäle physisch trennt. Diese Einbahnstraße lässt sich nicht per Software überlisten. Unberechtigte Datenzugriffe sowie das Einschleusen von Schad-Software in die Anlage in Form von manipuliertem Programm-Code werden zuverlässig verhindert.

Im Gegensatz zu einer klassischen Firewall sind bei diesem Ansatz auch Sicherheitslücken von außen oder eine



Secure Cloud Gateways integrieren eine Hardware-Daten-Diode, die die Kommunikation ausschließlich in eine Richtung zulässt.



Die Embedded-Kommunikationsschnittstellen Unigate IC als Kernkomponenten für Industrie 4.0 unterstützen die gängigen Feldbus- und Industrial-Ethernet-Standards.

fehlerhafte Konfiguration systembedingt ausgeschlossen. Zusätzlich ist der Kommunikationsweg zur Cloud über verschlüsselte Kommunikation mittels TLS (Transport Layer Security) beziehungsweise SSL (Secure Sockets Layer) gesichert. Die Authentifizierung erfolgt über Zertifikate plus Benutzerpasswort. Sie sorgt für Datenvertraulichkeit sowie für die Verschlüsselung für die Datenintegrität. Dies stellt sicher, dass die empfangenen Daten absolut identisch zu den verschickten Daten sind und von außen nicht verändert wurden. Die hohe Sicherheit der Secure Cloud Gateways wird zudem über ein gehärtetes Betriebssystem mit Secure Boot erreicht.

Um die Gateways zu konfigurieren, ist ein Hardware-Schlüssel nötig, mit dem sich das Gerät vor Ort – und nur dort – in den Konfigurationsmodus umstellen lässt. In dieser Betriebsart lässt die Daten-Diode auch eine Kommunikation in umgekehrter Richtung zu. Daneben gibt es den Lese-/Schreibmodus, um einen bewussten Zugriff von außen nach innen zu erlauben. Auch dieser Modus muss per Schlüsselschalter aktiv geschaltet werden.

Vielfältige Kommunikations-Matrix

Die Secure Cloud Gateways lassen sich über verschiedene Optionen wie Ethernet, Mobilfunk (LTE, 3G) oder WiFi mit dem Internet verbinden. Dabei sind die Geräte über eine Cloud beziehungsweise Remote-Service-Plattform konfigurierbar und bauen anschließend eine zuverlässige und sichere VPN-Verbindung auf. Die Busanschaltung ist durch die Vielfalt an vorzertifizierten Embedded-Kommunikationsschnittstellen der Serie Unigate IC von Deutschmann Automation gegeben. Busknoten sind für alle gängigen Feldbus- und Industrial-Ethernet-Standards, Profibus, Profinet, Ethernet/IP, Ethernet/TCP, Ethercat sowie für Devicenet, Modbus RTU/TCP, CANopen und Lonworks erhältlich. Alle für die unterschiedlichen Protokolle ausgelegten Baugruppen sind Pin-kompatibel, können also ohne zusätzlichen Aufwand ausgetauscht werden. Die Kommunikationsmodule umfassen einen Mikrocontroller, Flash, RAM und weitere Komponenten wie Optokoppler und Bustreiber und sind in einem 32-DIL-Gehäuse mit einer Fläche von 45 x 25 mm untergebracht. Die Embedded-Lösung lässt sich über eine UART-Schnittstelle an den Mikrocontroller des Endgeräts anbinden oder auch Stand-alone betreiben. Die ersten Secure-Cloud-Gateway-Familien werden MPI/Profibus, Profinet, Modbus und Ethernet/IP unterstützen.

Wozu der ganze Aufwand?

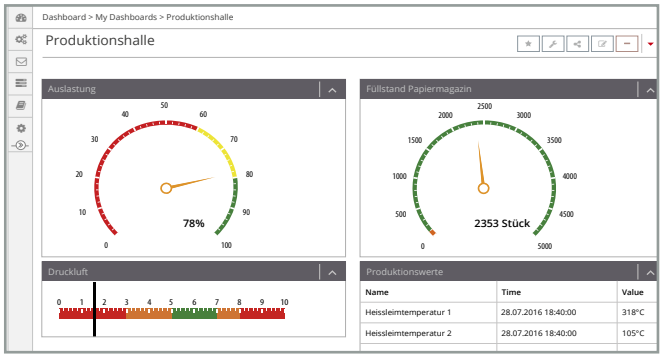
In der Cloud lassen sich unterschiedlichste Daten speichern, beispielsweise Verbrauchsdaten und Messwerte, Stückzahl- und Effizienzdarstellungen, Alarmsignale bei Schwellwertüberschreitung oder Signale der vorausschauenden Wartung. Für die Integration in die Cloud bieten sich zwei Lösungen an: In einer Public Cloud lassen sich die Daten bequem und sicher archivieren und auswerten. Möchte der Kunde die Cloud in seine Intranet-Lösung einbinden oder einen beliebigen Webservice nutzen, lässt sich ebenso eine Private Cloud installieren. Es besteht kein Zwang, die Public Cloud zu nutzen.

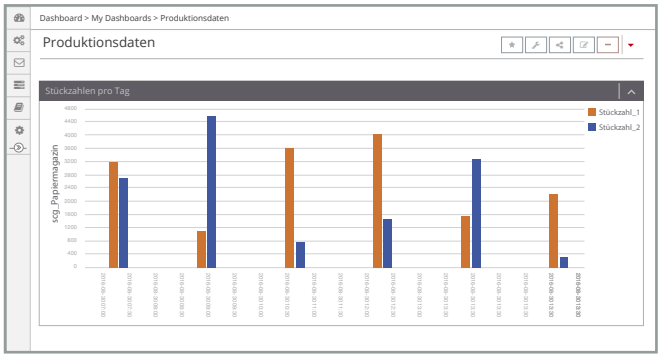
Unabhängig vom Standort kann der Nutzer über eine sichere Verbindung einzelne Maschinen abfragen und auf Daten wie Funktion, Produktivität und Auslastung zugreifen. Über Historiendaten lässt sich die Verfügbarkeit der jeweiligen Maschine im täglichen/wöchentlichen Rhythmus abfragen. Zudem können Störungsanalysen durchgeführt werden, um Maschinen mit hohen Ausfallzeiten zu identifizieren. Die Lösung eignet sich auch für Anwendungen im eigenen Betrieb, um Daten zu sammeln und per Tablet oder Smartphone sicher abzufragen. Die Secure Cloud Gateways wachsen mit den veränderten Anforderungen von Industrie 4.0 zukünftig mit. *(sk)*

Autoren

Michael M. Reiter,
ist Geschäftsführer von Deutschmann Automation in Bad Camberg.

Siegfried Müller,
ist Geschäftsführer von MB connect line in Dinkelsbühl.





Bilder: Deutschmann/MB connect line

Sind die Daten erst einmal sicher in eine Cloud-Infrastruktur übertragen, sind den Auswertungsmöglichkeiten fast keine Grenzen mehr gesetzt: als Dashboard einer Maschine (links) oder KPI-Auswertungen (Key Performance Indicator) von Produktionslinien (rechts).