



Spezifische Kennzeichnung

Von Warenidentifikation bis Echtheitsprüfung



THEMEN NEWS SPECIALS CORPORATE CHANNEL E-PAPER

SUCHEN NACH ...

ANMELDEN

REGISTRIEREN

P&A WEEK NEWSLETTER



Schutz vor Produktpiraterie bietet ein Lizenzmanagement aus der Cloud.
Bild: iStock, namussi

☆☆☆☆☆

Internet der Dinge

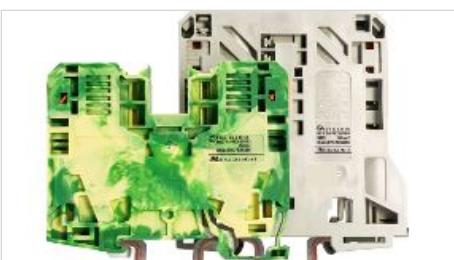
GUT GESCHÜTZT VOR PIRATERIE

TEXT: OLIVER WINZENRIED, WIBU-SYSTEMS

05.04.2017 | Die Chancen der Digitalisierung können nur mit sicheren Systemen umgesetzt werden. Dabei lässt sich der Schutz von IoT-Geräten vor Produktpiraterie oder Manipulationen mit einem Lizenzmanagement aus der Cloud monetarisieren.

TAGS | LIZENZ LIZENZMANAGEMENT INTERNET DER DINGE EMBEDDED SOFTWARE WIBU-SYSTEMS AG

Sponsored Content



News

Sichere Einspeisung in der Ex-Zone 2

Neue Ex-Zulassung für Wago-Hochstromreihenklempen der Serie 285 in den Querschnittsgrößen 35 mm² und 50 mm²



Brandhemmendes Material

Kunststoff rettet Leben



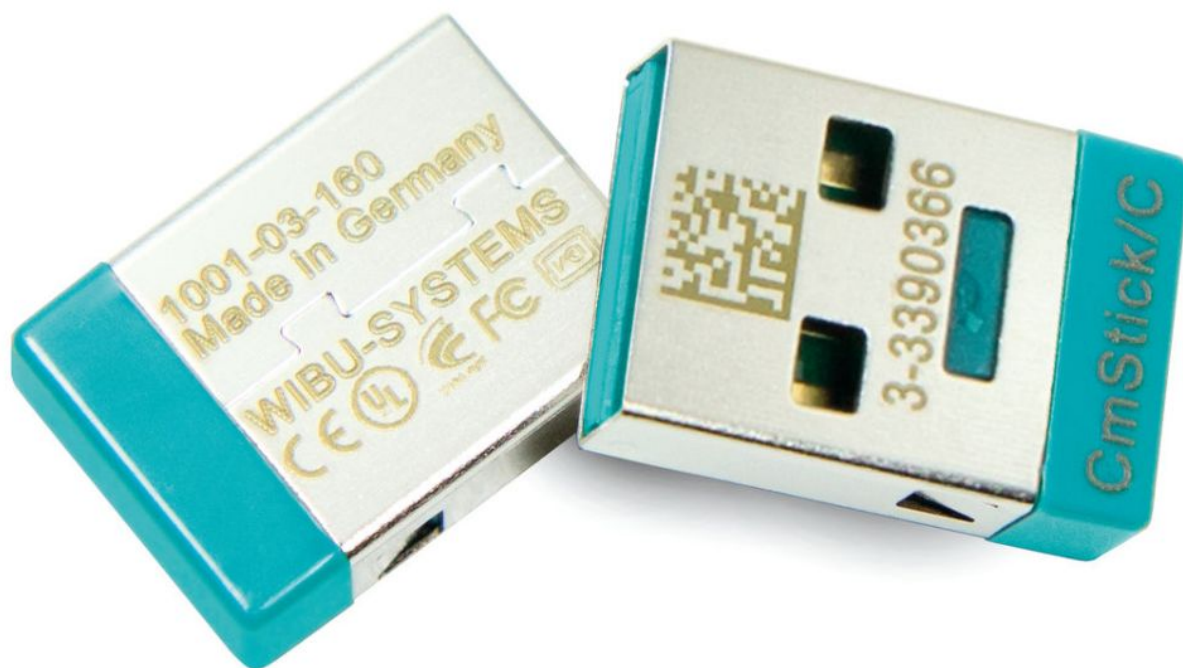
Rund 400 Brandtote und zehnmal so viel Verletzte im Jahr gibt es alleine in Deutschland. Das lässt sich verhindern ...

Ganze Nationen sehen in den technischen Möglichkeiten des IoT (Internet of Things) ihre Zukunft, investieren massiv in die Forschung und beziehen es in ihre langfristige Strategie ein. In den USA etwa sprechen Unternehmen und Regierung von Connected Systems; und der deutsche Industrie-4.0-Gedanke inspirierte die chinesischen Zukunftsplaner zum Strategiepapier „Made in China 2025“.

Einfache Wartung, vorausschauende Planung von Serviceeinsätzen, kundenspezifische oder kostenoptimierte Einzelstückfertigung und weniger Produktionsstillstand sind nur einige der vielen Vorteile, die das industrielle IoT im Gepäck hat. Der steigende Kostendruck forciert den Trend in diese Richtung. Der verfügbare Markt dafür wird für 2020 auf rund 1,8 Billionen US-Dollar (Frost & Sullivan) geschätzt.

IoT-Systeme bestehen aus räumlich auseinanderliegenden Komponenten, die über ein Netzwerk miteinander kommunizieren. Sind viele Teilnehmer miteinander vernetzt, bietet das Angriffsfläche für Manipulationen. Zudem nutzen diese Systeme der Zukunft öffentliche Netze. Doch dies ist kein sicherer Raum. Gefahren lauern aus allen möglichen Richtungen: Hacker spähnen für ihre dunklen Zwecke unbewachte Hintertürchen ins System aus; Industriespione kidnappen Daten, um sie auszuwerten; Saboteure versuchen Daten zu verändern, um Schaden anzurichten. Weil es im Internet der Dinge viel mehr Angriffspunkte gibt, muss jede einzelne Komponente adäquat geschützt sein.

BILDERGALERIE



Eine Lizenz lässt sich auch lokal auf einem CmStick speichern.

Bild: Wibu-Systems



Auch auf einer CmCard/MicroSD kann die Lizenz lokal zur Verfügung

Bild: Wibu-Systems

Daher wird die Konfiguration software-realisierter Funktionen in vernetzten Geräten, den IoT-Devices, immer wichtiger. Technisch erfolgt dies durch Lizenzierung. Sinnvoll ist es daher, diesen Prozess vollautomatisch mit einem Lizenzmanagement aus der Cloud zu gestalten.

Vom Embedded-System zum IoT

Embedded-Systeme „sehen“ mit Kameras, „fühlen“ mit Drucksensoren oder orientieren sich mit GPS (Global Positioning System). Sie nehmen ihre Umwelt wahr und fällen danach eigene Entscheidungen. So bringen etwa im Automobilwerk fahrerlose Transportwagen Halbzug zur nächsten Bearbeitungsstation. In der Fertigung entnehmen Roboter je nach Arbeitsschritt passendes Werkzeug aus ihrem eigenen Werkzeugkasten, positionieren es und bearbeiten damit Werkstücke. Dies sind weitestgehend in sich geschlossene Systeme und hochpreisige Investitionsgüter.

IoT-Systeme hingegen werden Aufgaben auf völlig neue Art erledigen oder Herausforderungen bewältigen, die bisher als unmöglich erschienen. Zum Beispiel können wir damit die Tiefsee erkunden, Roboter in gefährliche Einsätze bei der Feuerbekämpfung, im Rettungswesen oder bei der Minenräumung schicken, pflegebedürftigen Menschen mit „denkenden“ Maschinen helfen, Pflanzen sensorgesteuert ziehen oder Tiere individuell füttern.

Trends im Internet der Dinge

Während das bisherige IoT sich auf abgeschlossene Systeme konzentriert, wird das Internet der Dinge langfristig in jeden Bereich unseres Lebens eindringen. Es wird unsere Produktionsmethoden verändern und die kurzlebigen Konsumgüter erreichen. Ein Trend dabei ist, dass der USP (Unique Selling Point) eines Gerätes sich mit der Digitalisierung verschiebt und mehr in der Software liegen wird. Computing Hardware und Betriebssysteme werden immer stärker standardisiert. Geräte unterscheiden sich dann hauptsächlich durch ihre Applikationssoftware. Tief im Gerät verankerte Schutzlösungen sorgen für die Integrität der eingesetzten Software, schützen vor Re-Engineering, Produktpiraterie und Manipulation. Dabei entstehen neue Geschäftsmodelle. Software-gestützte Funktionen können nachträglich über Lizenzierungen vermarktet werden. Kostenpflichtige Upgrades, zukauf- und freischaltbare Optionen, zeit- oder mengengesteuerte Nutzung tragen zum wirtschaftlichen Erfolg des Geräteherstellers bei. Je besser die Möglichkeiten zum Lizenzieren sind, umso mehr Geschäftsmöglichkeiten ergeben sich daraus. Denn Lizenzierung und Berechtigungen sind Geschäftsgaranten, aber nur, wenn sich die dazugehörige Logistik in die Prozesse des Herstellers und des Endkunden transparent einfügt.

Auch zeigt sich, dass mehrere Hersteller in ein System liefern. Komponenten unterschiedlicher Hersteller und Software aus den verschiedensten Quellen müssen sowohl im einzelnen Gerät als auch im Gesamtsystem zusammenarbeiten. Durch die Möglichkeit von nachträglichen Erweiterungen oder Änderungen bleibt das System flexibel. Es entstehen neue Anwendungsgebiete und Dienstleistungen. Immer mehr Geräte werden im IoT vernetzt sein. Im Mobile Cyber Physical System werden Embedded-Systeme in mobilen Geräten wie Autos oder Smartphones zu „Intelligenzflächen“ zusammengeschlossen – Apps dafür entstehen. Simple Komponenten werden zudem schutzbedürftig. Ein umfassender Schutz erstreckt sich auf alle Teilnehmer im System, auch auf physikalisch kleine Komponenten und Geräte mit wenig Speicher und Computing Power.

Schutz und Lizenzierung im IoT

Neben einem guten Produkt, Marketing und den damit verbundenen Vertriebsaktivitäten spielen im IoT zusätzlich Schutz, Integrität und Lizenzierung für den Geschäftserfolg eine wichtige Rolle. Erfolgsfaktoren sind dabei: Geld verdienen durch Lizenzierung von Funktionsoptionen, neue Anwendungen über Berechtigungen verwalten und somit Servicetechnik anzubieten, sogenannte Produktpiraterie durch Nachbau, Klonen, Re-Engineering, Kopieren verhindern, Integrität der Kommunikation und der eigenen Komponenten per Design vor Manipulationen schützen. Im IoT muss die Sicherheit per Design in alle Komponenten einfließen. Damit stehen Industrietauglichkeit, Footprint der Soft- und Hardware, Entwicklungsunterstützung, herstellerübergreifendes Zusammenspiel sowie lückenloser Schutz ab hardwarenaher Software-Ebene im Vordergrund.

Eine IoT-fähige Schutzlösung muss physikalisch und funktional skalierbar sein. In den Geräten und der Software sollten daher geräteorientierte Lizenzierungen eingebaut sein, die sich auf vielen Plattformen über einen Multiplattform-Support integrieren lassen. Ein durchgängiger Ready-to-use-Schutz und dessen Lizenzierung von der Geräteentwicklung bis hin zu Betrieb und Wartung ist einzuplanen. Weiterhin sind industrietaugliche Eigenschaften gefragt sowie die Unterstützung von OPC UA und Secure Boot. Für Upgrades und Updates gilt: nur sichere Updates, lizenzierbare Upgrades und deren Nachrüstbarkeit bei Netzerweiterungen. Die Lizenzmodelle müssen speziell auf das IoT abgestimmt sein. Lizenzverwaltung, Berechtigungen und Zertifikate müssen sich einfach in alle Geschäftsprozesse wie Entwicklung, Produktion, Vertrieb und Service einbinden lassen.

Lizenzierung aus der Cloud

Zur Lizenzverwaltung in der Cloud mit 24/7-Self-Service-Fähigkeit gehören Aktivierung und Rückgabe, Umzug auf andere Geräte, Upgrades, Lizenzerneuerung oder -entzug dazu. Für ein skalierbares Schutzangebot gilt es, verschiedene Preis- und Leistungsoptionen für unterschiedliche Anforderungen anzubieten, durchgängige Hardware-, Software- und Cloudlösungen sowie industrietaugliche Dongles in gängigen Formfaktoren gehören ebenso ins Angebot. Den Nutzen der Konfiguration Software-realisierter Funktionen ist oben bereits beschrieben. Die Lizenzen können direkt in der Cloud gespeichert und von dort genutzt werden, was aber eine permanent verfügbare Internetanbindung erfordert. Vorteilhaft ist die Speicherung der Lizenz lokal im IoT-Gerät mit automatischer Aktualisierung aus der Cloud. Dann funktioniert das Gerät, auch wenn die Internetanbindung unterbrochen ist. Lokal wird die Lizenz entweder in einer Datei oder sogenannten Dongles gespeichert, die in industrietauglicher Ausführung beispielsweise in Form von CmAsics, CmCards oder CmSticks von Wibu-Systems verfügbar sind.

Integriert ist ein Secure Element, ein Smart Card Chip, ähnlich wie im Reisepass, der für Sicherheit sorgt. Die Chancen der offenen IoT-Systeme der Zukunft sind stärker schutzbedürftig als es die abgeschlossenen Systeme der Vergangenheit waren. Das ermöglicht neue Geschäftsmodelle wie zum Beispiel das Lizenzmanagement.

Firmen zu diesem Artikel

WIBU-SYSTEMS AG

KARLSRUHE, DEUTSCHLAND

21 Artikel/News

2 Videos

Verwandte Artikel



Condition Monitoring im Bienenstock

IOT GEGEN DAS BIENENSTERBEN

Ob seine Bienen gesund sind, verrät dem Imker in Zukunft ein Blick in eine App. Die nötigen Sensordaten werden ihm ...



Sick auf der Hannover Messe

WAS MÜSSEN INDUSTRIE 4.0-SENSOREN KÖNNEN?

Auf der Hannover Messe zeigt Sick anhand eines exemplarischen Wertschöpfungsablaufs, welche Sensormerkmale zu mehr ...



Firmware für Thin Clients

WEITE ENTFERNUNGEN? KEIN PROBLEM!

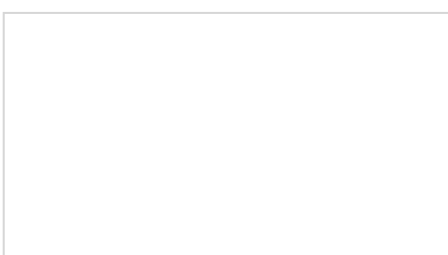
Thin Clients haben sich als Bedienterminals im Feld etabliert. Der Remote-Zugriff auf Server und virtuelle Maschinen ...



FactoryTalk Analytics

CLOUD ALS BINDEGLIED ZWISCHEN ANLAGENBAUERN UND FERTIGUNGSKUNDEN

Die Maschinenbau-Anwendung FactoryTalk von Rockwell basiert auf der Microsoft Azure Cloud und liefert Anlagenbauern ...



Eat in Time

NIE WIEDER LEBENSMITTEL WEGWERFEN

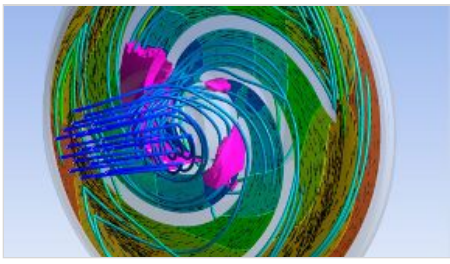
Wann muss ich Obst, Gemüse & Co. wegwerfen? Antworten darauf liefert das smarte System Eat in Time - und verhindert ...



Analyse per Prototyp

DIGITALE ZWILLINGE EROBERN DAS IOT

Ansys hat mit Flowserve, einem Anbieter von Fluid Motion- und Regelungsprodukten, eine unternehmensweite Lizenz- ...



INDUSTR.



energy_{4.0}

FASZINATION
ELEKTRONIK



URBAN20