Sicherheit und Zuverlässigkeit:

Schlüsselelemente in drahtlosen Netzwerken für das industrielle Internet of Things

Bild 1: Metall und Stahlbeton – auch wenn zwischen Metallgestellen und Gasleitungen platziert, müssen drahtlose Zugriffsknoten funktionieren

Das industrielle Internet of Things (IoT) schreit nach drahtlosen Sensoren und Steuerknoten für die vielen Applikationen in Fabriken, Industrieprozessen, in der Gebäudeenergieeffizienz bis hin zum intelligenten Parken und zur kommerziellen Landwirtschaft. In allen diesen Applikationen wird jahrelanger Betrieb der drahtlosen, industriellen IoT-Lösungen erwartet, oft in unwirtlicher HF-Umgebung und unter extremen Wetterbedingungen. Anders als bei Konsumer-Applikationen, wo Kosten im Vordergrund stehen, spielen in den Industrie-Applikationen Zuverlässigkeit und Sicherheit die erste Geige. Nach einer Umfrage von OnWorlds unter Nutzern von drahtlosen Sensornetzwerken (WSN), stehen Zuverlässigkeit und Sicherheit an erster Stelle. Das überrascht nicht, ist doch der Profit und die Qualität sowie die Effizienz der gefertigten Güter von diesen Netzwerken abhängig, ebenso die Sicherheit des Personals. Anbieter von industriellen IoT-Lösungen sehen in der richtigen Auswahl einer WSN-Plattform eine Schlüsselrolle für den Erfolg im drahtlosen industriellen IoT-Business. In diesem Artikel geht es um die Wichtigkeit der Datenzuverlässigkeit und Netzwerksicherheit in industriellen IoT-Applikationen. Dabei werden Real-life Fallstudien begutachtet und die Schlüsselkriterien bei der Auswahl von drahtlosen industriellen IoT-Lösungen diskutiert.

Datensicherheit in drahtlosen Sensornetzwerken

In industriellen Anlagen und Fabriken steht die Zuverlässigkeit an erster Stelle, führt doch der Ausfall von Daten zur Abschaltung oder zu Sicherheitsproblemen. In vielen Industrieapplikationen kann ein kurzfristiger Datenverlust toleriert werden, längere Ausfallperioden in der Kommunikation sind aber nicht akzeptabel. Eine Fehlerrate von 1% ist zu hoch, führt sie doch zu einem Ausfall von 3,65 Tagen im Jahr. Anbieter von industriellen IoT-Lösungen behaupten, dass ein Kommunikationsausfall von einem halben Tag, Kunden irritiert und zu zusätzlichen Kosten zur Ursachenbeseitigung führt. Im Wiederholungsfall kann man sogar den Kunden verlieren.

Deshalb wird in industriellen Lösungen eine Datenzuverlässigkeit von >99,999% gefordert, auch um die HF-Probleme zu überwinden, die sich im Laufe der vielen Jahre des Betriebs ergeben haben. Damit ein drahtloses Netzwerk über Jahre wartungsfrei läuft, muss es so geschneidert werden, dass es auf verschiedene Arten alle Probleme löst.

Redundanz

Ein grundlegendes Prinzip beim Design eines zuverlässigen Netzwerks ist Redundanz. Ausfallsichere Mechanismen müssen es Systemen ermöglichen, Probleme ohne Datenverlust zu lösen. In einem drahtlosen Sensornetzwerk gibt es zwei grundlegende Möglich-

Zahl der drahtlosen Knoten	32 (jeder mit 4 Sensoren, die Daten liefern)
Mesh Netzwerk-Tiefe	4 (Sprünge) Hops vom entferntesten Knoten zum Gateway
Datengenerationsrate des gesamten Netzwerks	3 kbits pro Sekunde
Gesamt gesendete Daten	>18,8 Gigabits über 83 Tage
Datenzuverlässigkeit	>99,999996%

Tabelle 1: Netzwerkstatistik - SmartMesh IP Netzwerk in Linear Technologies Wafer Fab

Autor:

Ross Yu, Product Marketing Manager, Dust Networks Product Group, Linear Technology

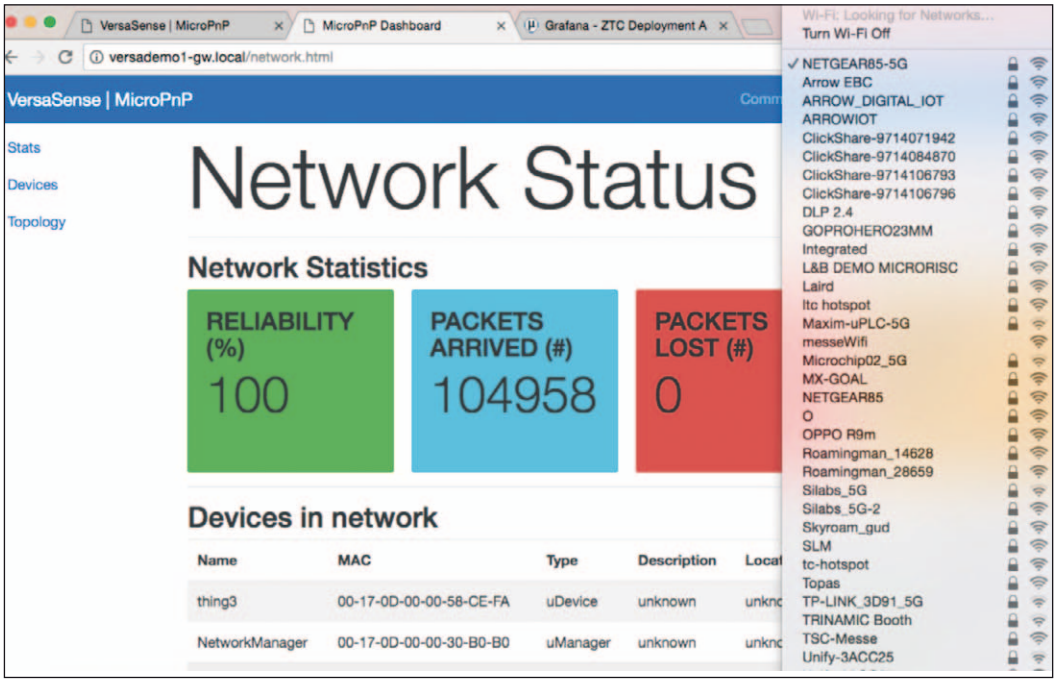

Bild 2: Netzwerk-Zuverlässigkeit auf der electronica 2016 – Sogar in Anwesenheit von über 50 WiFi-Netzwerken liefert das SmartMesh IP-Netzwerk über 75,5 Mbits an Daten (104,958 Pakete mit 90 Byte Nutzdaten) mit 100% Datenzuverlässigkeit

keiten, die Redundanz zu nutzen. Die Erste ist die räumliche Redundanz, bei der jeder drahtlose Knoten immer mit mindestens zwei weiteren Knoten kommunizieren kann. Ein Routingschema ermöglicht den Daten den Zugang zu einem dieser Knoten, stellt aber sicher, dass das ursprünglich angesteuerte Ziel erreicht wird. Ein sorgfältig aufgebautes Maschennetzwerk – eines bei dem jeder Knoten mit zwei oder mehr benachbarten Knoten kommunizieren kann – bietet höhere Zuverlässigkeit als ein Punkt-zu-Punkt-Netzwerk, da es Daten über einen alternativen Pfad senden kann, wenn der ursprüngliche nicht verfügbar ist. Eine zweite Redundanz erreicht man durch die Nutzung mehrerer HF-Kanäle im Übertragungsbereich. Beim Kanalsprungverfahren können bei der Verbindung zwischen zwei Knoten die Kanäle gewechselt werden, so kann man sich auf die raue HF-Umgebung, wie sie typisch ist für die industrielle Umgebung, einstellen. Nach dem IEEE 802.15.4 2,4-GHz-Standard gibt es 15 Kanäle, die für das Kanalsprungverfahren zur Verfügung stehen. Es ist somit belastbarer als ein Einkanalsystem ohne Kanalsprungverfahren. Es gibt verschiedene Standards für drahtlose Maschennetzwerke, diese schließen die Redundanz von Raum und von Kanälen ein, bekannt als Time Slotted Channel Hopping (TSCH), mit dem IEC62591- (WirelessHART) und dem aufkommenden IETF 6TiSCH Standard (Ref 2). Diese Standards für drahtlose Maschennetzwerke ermöglichen den weltweiten Einsatz von Funkgeräten im lizenzfreien 2,4-GHz-Spektrum. Sie haben sich durch Aktivitäten der Dust Networks Gruppe von Linear Technology entwickelt, die ab 2002 erstmals das TSCH Protokoll in low Power, Ressourcen begrenzten Geräten mit SmartMesh Produkten eingesetzt haben.

Da TSCH ein essenzieller Baustein für die Datenzuverlässigkeit in rauer HF-Umgebung ist, ist dessen Einsatz und Unterhaltung ein Schlüsselelement in Maschennetzwerken für einen kontinuierlichen, problemlosen Einsatz über viele Jahre. Ein industrielles drahtloses Netzwerk muss oft über viele Jahre funktionieren, und in dieser Zeitspanne wird es Veränderungen in der HF-Umgebung und bei der Datenübertragung geben. Deshalb ist eine Schlüsselanforderung für einen sicheren Betrieb, vergleichbar einem Kabelnetzwerk, eine intelligente Netzwerk-Managementsoftware, die die Netzwerktopologie dynamisch optimiert und kontinuierlich die Linkqualität für einen maximalen Durchsatz, unabhängig von Interferenzen oder Änderungen in der HF-Umgebung, überwacht.

Fallstudie Nr.1 – TSCH Netzwerk in einem Halbleiterwerk

Ein TSCH-basiertes SmartMesh IP-Netzwerk von Linear Technology wurde in der eigenen Halbleiterfabrik im Silicon Valley eingerichtet, um den Druck von hunderten Spezialgaszylindern zu überwachen, die in den verschiedenen Halbleiterprozessen beim Ätzen und Reinigen zum Einsatz kommen. Früher wurde jeder Zylinderdruck dreimal am Tag geprüft, was vier Stunden manuelle Arbeitszeit beanspruchte. Zur Automatisierung der Messung und Übertragung der Daten an eine Steuerzentrale wurde ein SmartMesh IP-Netzwerk installiert. Im Gasbunker wurden 32 drahtlose Knoten installiert, wobei jeder Knoten jeweils ein Zylinderpaar auf Tankdruck und Druckregelung überwacht. Das Netzwerk überträgt jede Sekunde drei Kilobits an Sensordaten. Die HF-Bedingungen in der Fabrik sind typisch für eine Industrieumgebung mit drahtlosen Knoten umgeben von Metall, Stahlbeton und mit Personen und Geräten, die sich den ganzen Tag in dieser Umgebung bewegen. Das Netzwerk hat über 83 Tage kontinuierlich gearbeitet und dabei über 18,8 Gigabits an Daten übertragen und eine Zuverlässigkeit von >99,99999% (auch „sieben Neunern“ genannt) erzielt.

Fallstudie Nr. 2 – Das TSCH Netzwerk auf der electronica 2016

Messehallen sind generell mit HF-Störungen belastet und so eine gute Prüfung für die Zuverlässigkeit von WSNs. Auf der electronica 2016 demonstrierte die belgische Firma VersaSense ihr SmartMesh IP-basiertes drahtloses System. Die HF-Umgebung war mit 52 aktiven Wi-Fi-Netzwerken stark belegt, zusätzlich zu den tausenden Handys und Bluetooth-Geräten der Besucher. Während der vier Messetage hat das VersaSense-System über 75,5 Mbits an Daten mit 100% Datenzuverlässigkeit in dieser gesättigten HF-Umgebung übertragen.

Die Wichtigkeit der Netzwerksicherheit

Sicherheit ist ein weiteres kritisches Attribut eines drahtlosen Sensornetzwerks. Die primären Ziele bei der Sicherheit in WSNs sind:

- **Vertraulichkeit** – Der Datentransport im Netzwerk soll nicht von jedem mitgelesen werden, nur vom eigentlichen Empfänger
- **Integrität** – Jede empfangene Nachricht muss mit der gesendeten übereinstimmen, ohne Zusätze, Kürzung oder Manipulation des Inhalts
- **Authentizität** – Die Quelle der Nachricht muss bekannt sein. Wird die Zeit als Teil des Authentizitätsschemas verwendet, wird die Nachricht davor geschützt, aufgenommen und wiedergegeben zu werden.

Vertraulichkeit ist nicht nur in sicherheitskritischen Applikationen wichtig, sondern auch in Allerweltsapplikationen. Sensorinformationen über den Produktionsstatus oder über den Zustand der Maschinen sind für den Mitbewerb von Interesse. Beispielsweise veröffentlicht die National Security Agency (NSA) nicht den Stromverbrauch ihres Datencenters, da diese Daten Rückschlüsse auf die Computerleistung zuließen.

Sensordaten sollten verschlüsselt sein, damit sie nur der vorgesehene Empfänger nutzen kann.

Bild 3: Sicherheit in industriellen WSN – umfasst Vertraulichkeit, Integrität, und Authentizität der industriellen Daten

Dabei müssen Mess- und Steuerinformation unbeschädigt ankommen. Meldet ein Sensor „Tankpegel ist 72 cm" oder der Controller fordert „Ventil um 90 Grad drehen", kann es schlecht ausgehen, wenn ein Digit in den genannten Zahlwerten falsch ist.

Man muss den Meldungen vertrauen können. Jeder der beiden oben genannten Meldungen kann zu schlimmen Konsequenzen führen, wenn sie gehackt werden. Ein extremes Beispiel für eine Falschmeldung ist z.B. eine Aufforderung wie: „hier neues Programm zum Installieren".

Die kritische Sicherheitstechnologie, die ein WSN aufweisen sollte, muss diese Ziele adressieren. Einschließlich einer starken Verschlüsselung (z.B. AES128) mit einem robusten Schlüssel und gutem Schlüsselmanagement mit einem Zufallsnummerngenerator hoher Kryptoqualität, um Replay-Angriffe abzuwehren, mit Message-Integritäts-Checks (MIC) in jeder Nachricht und Zugriffskontrolllisten (ACL), um Zugriffe auf spezifische Knoten zu verweigern oder zuzulassen. Diese State-of-the-Art drahtlosen Sicherheitstechnologien sind wohl in vielen Geräten heutiger WSNs integriert, aber nicht alle WSN-Geräte und -Protokolle enthalten alle diese Maßnahmen (Ref 3). Verbindet man ein sicheres WSN mit einem unsicheren Gateway, ist das eine Schwachstelle, und die End-zu-End Sicherheit muss beim Systemdesign besonders beachtet werden.

Die Konsequenzen einer schlechten Sicherheit sind nicht immer einfach zu ahnen. Beispeilsweise erwartet man bei einem drahtlosen Temperatursensor oder Thermostat keine Notwendigkeit für Sicherheit. Beschreibt aber eine Zeitung, wie Kriminelle ein Radio verwenden, um die Einstellungen eines Thermostats zu ermitteln, um dann das Haus auszuräumen, wenn die Bewohner außer Haus sind, gibt es ein Sicherheitsproblem. Der Einfluss auf die Treue des Kunden, abgesehen vom Geschäft, wird dramatisch sein. Deshalb ist der sicherste Weg die Verschlüsselung aller Daten.

Schaden durch Hacker

In der industriellen Prozessautomation sind die Konsequenzen eines Hackangriffs katastrophaler als der Verlust eines Kunden. Ein Hacker kann großen Schaden anrichten, wenn falsche Prozessdaten an die Steuerzentrale gelangen. Meldet z.B. ein Sensor eine zu niedrige Motordrehzahl oder einen zu niedrigen Tankinhalt, kann sich das katastrophal auswirken, vergleichbar mit der Stuxnet-Attacke auf die Uranzentrifugen im Iran. Selbst eine fehlgeschlagene Attacke oder die Enthüllung einer potentiellen Schwäche kann zu Verlusten beim Verkauf führen, zu zusätzlichem technischen Aufwand und zu einer schlechten Presse.

Neue industrielle IoT-Lösungen sind möglich

Hohe Zuverlässigkeit und Netzwerksicherheit sind kritische Anforderungen nicht nur für sicherheitsrelevante Applikationen und in der Prozessteuerung, sondern für alle industrielle IoT-Applikationen. Zum Glück gibt es felderprobte WSN-Lösungen, die die Anbieter von industriellen IoT-Lösungen in die Lage versetzen, Systeme zu liefern, die in herausfordernden Umgebungen reibungslos und zuverlässig über viele Jahre arbeiten.

■ *Linear Technology*
www.linear.com