Wie LAN und WLAN in Smart Spaces der Zukunft zusammenwirken werden

Die zunehmende Verbreitung von Smart Spaces bedeutet, dass unbedingt dafür gesorgt werden muss, dass diese Installationen über alle erforderlichen Infrastrukturkomponenten verfügen. Jeder Versuch, mit einer einzelnen Netzwerklösung auszukommen, ist dabei sicher zum Scheitern verurteilt.

Welche Herausforderungen bestehen für Smart Spaces? Wie werden LAN und WLAN gemeinsam die Netzwerke der Zukunft unterstützen? Und welche Lösungen gibt es für LAN-Optionen?

Das Problem für Smart Spaces

Es besteht kein Zweifel daran, dass die Zahl der IoT-Geräte immer weiter ansteigen wird, und es dauert nicht mehr lange, bis 20 Milliarden IoT-Geräte weltweit im Einsatz sein werden. Einzelne Sensoren haben sicher ihre Vorteile, doch nur die Kombination sehr vieler Sensoren wird zu den wichtigsten Veränderungen führen.

Arrow Central Europe GmbH
www.arrow.com

So kann etwa ein einzelner IoT-Thermostat die Temperatur eines einzelnen Raumes steuern, aber die Kombination mehrerer Umgebungssensoren in einem Gebäude kann es ermöglichen, die Luftströmungen zwischen Räumen, die Luftqualität und die optimalen Heizmöglichkeiten für das gesamte Gebäude zu verstehen.

Zum Aufbau solcher Systeme ist jedoch eine starke zugrunde liegende Infrastruktur erforderlich, die Energie und Konnektivität bereitstellen kann. Ingenieuren stehen viele Optionen zur Verfügung, aber diese gehören immer zu einer von zwei Kategorien: drahtgebunden und drahtlos. Jede dieser Technologien hat ihre eigenen Vor- und Nachteile. Viele Ingenieure sind aber darauf fixiert, ausschließlich eine davon zu verwenden. Wenn die falsche Wahl getroffen wird, können künftige Upgrades kostspielig oder sogar unmöglich sein, weshalb man sich solche Entscheidungen keinesfalls leicht machen darf.

Die Herausforderungen bei Kabeln

Kabel sind schon seit mehr als hundert Jahren das primäre Kommunikationsmittel, da sie relativ einfach zu konstruieren und zu betreiben sind. Da die Herstellung von Kabeln unproblematisch ist, erweist sich ihr Einsatz für die Kommunikation über kurze Distanzen als sehr kosteneffektiv. Zwar ist die Installation von Kabeln über größere Distanzen mit hohen Arbeitskosten verbunden, die Implementierung der Infrastruktur für das Senden von Nachrichten über Tausende von Kilometern hinweg ist jedoch einfacher und günstiger als bei drahtlosen Alternativen.

Andererseits sind Kabel vielen physischen Phänomenen ausgesetzt, was Datenübertragungen mit hoher Geschwindigkeit erschwert. Beispielsweise basieren Datensignale mit hoher Geschwindigkeit fast immer auf einem verdrillten differenzierten Aderpaar, um Rauschen zu eliminieren, und wenn diese Paare nicht sorgfältig ausgerichtet sind, kann die Signalintegrität beeinträchtigt werden. Schlimmer noch ist, dass ältere Kabelinstallationen modernen Datenraten oft nicht gewachsen sind, weshalb Aktualisierungen von Systemen den Austausch aller Datenkabel erfordern können. So unterstützen ältere Ethernet-Kabel etwa Geschwindigkeiten bis zu 100 Mbit/s, doch keines dieser Kabel kann für moderne Verbindungen mit 1 Gbit/Sek. genutzt werden.

Ein weiteres Problem bei Kabeln besteht darin, dass ihre Installation einen hohen physischen Arbeitsaufwand erfordert, oft Erdarbeiten zur unterirdischen oder den Bau von Masten zur überirdischen Verlegung. Selbst Rechenzentren benötigen umfangreiche Kabelbaugruppen und Routing-Systeme, deren Einbau und Reparatur sehr schwierig sein können.

Je nach Technologie können Kabel, die elektrische Signale verwenden, nur ein Gerät pro Kabel unterstützen, was bedeutet, dass für die Verbindung mehrerer Geräte zusätzliche Kabel erforderlich sind. Natürlich gibt es Busprotokolle, die die Verbindung mehrerer Geräte mit einem einzelnen Kabel ermöglichen, solche Arrangements reduzieren aber die Bandbreite des Kabels deutlich.

Und schließlich gilt, dass viele ältere LAN-Netzwerke sehr anfällig gegenüber Angriffen sind. Je nach der verwendeten Infrastruktur implementieren viele LAN-Technologien nicht standardmäßig Zugangsdaten, weshalb jedes Gerät, dass sich mit einem Netzwerk verbunden kann, dies auch nutzen darf. Dies ist einer der wichtigsten Gründe dafür, dass Hacker nach exponierten LAN-Anschlüssen suchen, die nicht aktiv verwendet werden.

Probleme für drahtlose Technologien

Im Vergleich zu Kabeln können drahtlose Lösungen tatsächlich viele Probleme beseitigen. Dazu gehört etwa die Möglichkeit, unterschiedliche Frequenzen für die Kanaltrennung zu nutzen (was die Zahl der einander störenden Geräte reduziert), oder die Verwendung direktionaler Antennen für Strahlen, die nicht mit anderen auf derselben Frequenz interagieren (was die Bandbreite erhöht).

Wenn es so ist, dass Kabel so viele Probleme machen, dann ist die logische Wahl doch eine drahtlose Lösung, richtig? Nun, nicht nur Kabel können problematisch sein, für drahtlose Installationen gilt dies leider ebenfalls. Dies zeigte sich besonders bei der Einführung von 5G, bei der von vielen Störungen berichtet wurde, nicht zu vergessen die negativen Presseberichte rund um Beschwerden von Menschen, in deren Nachbarschaft Mobilfunkmasten errichtet werden.

Zunächst gilt, dass die Frequenz, die ein drahtloses System nutzt, seine effektive Reichweite bestimmt (genauer gesagt ist die Frequenz umgekehrt proportional zur Reichweite). So können Funksysteme mit niedrigen Frequenzen über Dutzende von Kilometern hinweg kommunizieren, während Hochfrequenzsysteme auf kürzere

Entfernungen beschränkt sind. Gleichzeitig ist aber auch die Bandbreite einer Funkwelle (d. h. die Datenmenge, die sie pro Sekunde bereitstellen kann) direkt proportional zu ihrer Frequenz. Dies bedeutet, dass die Kommunikation über längere Distanzen oft nur geringe Bandbreiten ermöglicht, während die Bandbreite über kürzere Entfernungen hinweg hervorragend ist.

Ein sehr gutes Beispiel für die damit verbundenen Probleme ist 5G. Die Verwendung höherer Frequenzen ermöglicht deutlich höhere Bandbreiten als bei 4G. Die höhere Frequenz bedeutet jedoch, dass die 5G-Abdeckung sehr schlecht ist, daher mussten viele Mobilfunkmasten näher an die Nutzer (d.h. außerhalb von Wohnimmobilien) gebracht werden.

Ein weiteres Problem mit drahtlosen Netzwerken ist ihre Anfälligkeit für Remote-Angriffe. Während Ethernet-Kabel den physischen Zugriff erfordern, kann ein drahtloses Netzwerk leicht aus der Ferne angegriffen werden. Schlimmer noch: Mit „Funk-Paket-Sniffern“ können Angreifer den Datenverkehr in einem drahtlosen Netzwerk überwachen und bei einer Unterbrechung ein Gerät und die gesendeten Daten identifizieren.

Gleichzeitig kann es dazu kommen, dass drahtlose Netzwerke überlastet werden, wenn sich zu viele Geräte gleichzeitig damit verbinden. Mobilfunknetzwerke sind weniger anfällig für Überlastungen als WiFi, da sie dafür konzipiert sind, mit Tausenden gleichzeitiger Verbindungen umzugehen, doch Heimnetzwerke, die öffentlich zugängliche Frequenzen nutzen, leiden häufig darunter. Die Verbindung von Tausenden von Geräten mit einem einzigen Zugangspunkt kann schnell zu höherer Latenz führen, was sehr problematisch für Systeme ist, die in Echtzeit operieren müssen.

Warum sind Kabel für die Zukunft von Smart Spaces so wichtig?

Zum Thema Smart Spaces und Konnektivität wird oft gesagt, dass drahtlose Technologien wie 5G und WiFi dominieren werden – diese Denkweise ist sehr verständlich. Sie helfen nicht nur dabei, Kabelinstallationen zu reduzieren, sondern ermöglichen auch größere Freiheit bei der Installation von Geräten. Anstatt durch die Länge eines Ethernet-Kabels eingeschränkt zu sein, ermöglicht eine vollständig drahtlose Lösung die Installation von Geräten genau da, wo sie benötigt werden. Wahrscheinlicher ist jedoch, dass Installationen der Zukunft die Vorteile von Kabeln und von drahtlosen Lösungen nutzen werden, anstatt ausschließlich auf eine der beiden Optionen zu setzen.

Immerhin werden die Smart Spaces der Zukunft aus tausenden von Geräten bestehen – viel zu vielen für ein einzelnes drahtloses Netzwerk. Natürlich sind Mobilfunktechnologien für sehr hohe Lasten gedacht, aber da Latenz und Bandbreite immer wichtiger werden, ist der Betrieb aller Geräte mit drahtlosen Signalen sehr kostspielig und schwierig zu implementieren.

Nicht nur die schiere Zahl der Geräte ist ein Problem, sondern auch, dass viele davon einen Energiebedarf haben, der für Energiesammler viel zu hoch ist. Beispielsweise müssen Sicherheitssysteme stets zu 100% aktiv sein und sind daher nicht zur Verwendung mit Energiesammlern geeignet. Vor dem Hintergrund, dass diese Smart Spaces aus Tausenden von Geräten bestehen, kommt auch ein Batteriebetrieb nicht dafür in Frage – die Wartung solcher Geräte ist äußerst problematisch. Es können zwar Batterien verwendet werden, die für die gesamte Lebensdauer eines Geräts ausreichen, doch dies führt schnell zu großen Mengen Elektronikmüll, und damit ist die heutige Welt bereits gründlich bedient.

Daher ist eine permanente Energiequelle erforderlich und eine dedizierte Verbindung per LAN bietet nicht nur ausreichend Bandbreite, sie kann auch über ein einzelnes Kabel per Power-Over-Ethernet (PoE) die Stromversorgung leisten. Tatsächlich kann die Verwendung von PoE-Kabeln die Installation dadurch vereinfachen, dass ein Gerät nur noch ein Kabel benötigt. So können mehr Kabel in einem Bereich gebündelt und mehr Geräte versorgt werden.

Geräte, die Energiesammler nutzen, müssen wahrscheinlich nahe an Zugangspunkten positioniert werden, um die Energiekosten der Übertragung zu reduzieren. In einem solchen Fall benötigt der Zugangspunkt wahrscheinlich PoE für Strom und Konnektivität, was den Bedarf an Kabeln in einem Smart Space weiter unterstreicht.

Der Sicherheitsaspekt von Smart Spaces führt auch dazu, dass Kabel gegenüber drahtlosen Netzwerken bevorzugt werden, besonders für sicherheitsrelevante Geräte wie Kameras, Mikrofone und Alarmsysteme. Die Verwendung von Kabeln verhindert Remote-Angriffe und der Einsatz von Anmeldedaten und Zertifikaten für verbundene Geräte kann den Zugriff auf von Hackern ins Netzwerk eingeschleuste, nicht identifizierte Geräte abwehren. Möglicherweise werden zukünftige PoE-Versionen erkennen, wenn ein Gerät getrennt wurde, woraufhin die Energieüberwachung der einzelnen PoE-Geräte dazu genutzt werden kann, verdächtige Aktivitäten aufzudecken – mit drahtlosen Geräten ist dies sehr schwierig.

Und schließlich sind drahtgebundene Geräte immun gegen Störungen, was es ermöglicht, Tausende von Geräten nahe beieinander zu positionieren. Der Einsatz von Kabeln verhindert auch „Wireless Jamming“, sodass Smart Spaces sehr wirksam gegen Angriffe geschützt werden können.

Welche Lösungen gibt es im LAN-Bereich?

Die gute Nachricht für Ingenieure ist, dass es zahlreiche LAN- und WLAN-Lösungen gibt, die heutzutage für Smart Spaces implementiert werden können und hohe Bandbreite sowie gute Widerstandsfähigkeit gegen Sicherheitsbedrohungen bieten. Für seine Netzwerklösungen für IoT-Geräte bekannt ist etwa Lantronix. Das Unternehmen hat verschiedenste Lösungen im Angebot, darunter SoM (System on Modules), Netzwerkschalter und Gateways.

Ein Beispiel ist das XPCW-1002100B, ein serielles WiFi-Modul, das eine äußerst kompakte Netzwerklösung mit niedrigem Energieverbrauch darstellt, die drahtlose LAN-Verbindungen gemäß IEEE 802.11 bei praktisch jeder Lösung mit SPI oder serieller Schnittstelle ermöglicht. Durch die verringerte Komplexität drahtloser Designs ermöglicht das XPCW1002100B Ingenieuren, IoT-Geräte schnell zu testen und zu fertigen und mit ihnen über Netzwerke zu kommunizieren, als wären diese physisch mit einer seriellen Schnittstelle verbunden. Für alle, die nach einer Ethernet-Lösung suchen, ist das XPC100100B-01 dem XPCW1002100B insoweit ähnlich, als es Seriell-zu-Netzwerk-Verbindungen ermöglicht. Anstatt über WLAN erfolgt die Verbindung dabei jedoch über LAN.

Auf dem Gebiet der Netzwerkkonnektivität bietet Lantronix auch zahlreiche Lösungen mit Gateways und Schaltern, beispielsweise das Modell SGX5150020US. Dieses Gerät stellt ein 5-GHz-WiFi-Netzwerk mit Internet-Verbindung über LAN bereit. Solche Zugangspunkte können dabei helfen, Netzwerke voneinander zu trennen, wobei gleichzeitig drahtlose Funktionen bereitgestellt werden.

Insgesamt ist es wahrscheinlich, dass IoT-Smart Spaces der Zukunft einen Mix aus verkabelten und drahtlosen Lösungen nutzen werden, um die Vorteile beider Technologien sinnvoll zu nutzen. ◄