

WLAN – Mit Plan zum Plan

Dr.-Ing. Stefan Schemmer, Dipl.-Inf. Sebastian Vandersee, rt-solutions.de GmbH, Köln, Prof. Dr. Martin Gergeleit, FH Wiesbaden

Kurzfassung

Die industrielle Automation bietet vielversprechende Anwendungsfelder für den Einsatz drahtloser Netzwerke, so etwa das mobile Warten- und Bedienen, Logistikanwendungen mit portablen Endgeräten oder die Vernetzung mobiler Anlagenteile. Bedenken, ob WLAN den Anforderungen dieser Anwendungen genügen kann, stellen aber immer noch ein Hindernis für den Einsatz dieser Technik dar. Der vorliegende Beitrag befasst sich mit der Frage, inwiefern sich solche Anforderungen durch aktuelle Produkte, WLAN-Standards und Architekturen erfüllen lassen. Er stellt darüber hinaus aufgrund von Projekterfahrungen dar, welche Schritte bei der Planung einer WLAN-Installation zu beachten sind, um auf der aktuellen technologischen Grundlage zu einer anforderungsgerechten WLAN-Lösung zu gelangen.

1. Einleitung

Drahtlose LANs (WLANs) nach dem IEEE 802.11-Standard [1] sind inzwischen weit verbreitet. Der Standard erfüllt mit seinen relativ hohen Reichweiten und Durchsatzraten einen Großteil der Anforderungen, die an drahtlose Kommunikation – zumindest in der Bürovernetzung – gestellt werden. Die kabellose, breitbandige Vernetzung eröffnet aber auch in der industriellen Automatisierung ganz neue Möglichkeiten. Speziell in der Logistik (Kommissionierung, Lager, Transport) hat sich WLAN bereits einen festen Platz erobert. Doch auch für die flexible Produktion bietet WLAN ein großes Potential. Als Anwendungsfelder seien hier die Anbindung mobiler Einheiten in Hochregallagern, Elektrohängebahnen und Flurfördersystemen ebenso genannt wie mobile Bedienterminals, Wartungszugänge über Laptops und PDAs oder der Ersatz von Schleppkabeln und Schleifkontakten in beweglichen Anlagenteilen.

Aus der industriellen Umgebung und der Anwendung in Produktionsprozessen ergeben sich aber weitergehende Anforderungen an die Kommunikation, darunter u. a. Robustheit gegen Umgebungseinflüsse (Staub, Feuchtigkeit, aggressive Atmosphäre), Montage und Anschluss nach Industriestandards, hohe Verfügbarkeit, vorhersagbares Zeitverhalten sowie die Ein-

bindung in industrietypische Überwachungs- und Wartungsprozesse. Wie schon bei der Vernetzung mit Feldbussen, lassen sich daher die Standards aus der Bürokommunikation nicht ohne weiteres in die industrielle Automatisierung übertragen. Vielmehr sind die Anforderungen industrieller Applikationen nur durch den Einsatz angemessener Produkte einerseits und eine angemessene Planung der WLAN-Installation andererseits zu erfüllen. Beide Aspekte werden im Folgenden näher erläutert. Dazu wird zunächst untersucht, inwiefern die Erfüllung dieser Anforderungen durch aktuelle Standards, Produkte und Architekturen unterstützt wird (Abschnitte 2 und 3), um dann darauf einzugehen, welche Schritte im Rahmen einer ganzheitlichen Planung einer WLAN-Lösung zu beachten sind, um auf der beschriebenen technischen Grundlage die Anforderungen der jeweiligen Applikation und Umgebung zu erfüllen (Abschnitt 4). Abschnitt 5 fasst die Ergebnisse in einem Fazit zusammen.

2. Standards und Produkte

Alle gängigen industriellen Produkte implementieren IEEE 802.11b/g und bieten damit Bruttodatenraten von 11 bzw. 54 MBit/s, Produkte mit IEEE 802.11a/h Unterstützung sind in Europa seltener anzutreffen. IEEE 802.11a/h bietet im 5 GHz-Band ebenfalls maximal 54 MBit/s Bruttobandbreite, jedoch sind deutlich mehr Kanäle überlappungsfrei nutzbar, wodurch eine höhere Flächenbandbreite und eine höhere Systemdichte erreicht werden können. Als Securitystandard hat sich IEEE 802.11i [2] durchgesetzt. Vermehrt etabliert sich auch der für Echtzeitanforderungen im WLAN konzipierte Standard IEEE 802.11e [3] in Industrieprodukten. Von den beiden darin spezifizierten Zugriffsverfahren ist bisher nur die sog. EDCA von den Chipherstellern implementiert, die einen prioritätenbasierten Zugriff mit 4 Prioritäten ermöglicht. Auf dieser Grundlage können die Zeitanforderungen vieler (wenn auch nicht aller) Applikationen durch eine entsprechende Planung der Verkehrsklassen und ihrer Lasten erreicht werden. Das weitergehende sog. HCCA-Verfahren für einen deterministischen, zeitlich geplanten Zugriff wäre für industrielle Anwendungen noch erheblich besser geeignet, wird aber bisher von den großen Chipherstellern nicht implementiert.

Industrielle WLAN-Produkte unterscheiden sich von Office-Produkten durch ihre robuste Bauart für den Einsatz in rauer Umgebung. Darüber hinaus bieten sie industrietypische Montage- und Anschlussarten, z.B. zur Spannungsversorgung. Teilweise werden auch spezielle Features implementiert, um den besonderen Anforderungen hinsichtlich Echtzeit und Roaming gerecht zu werden. Industrielle Client-Produkte sind häufig als Konverterlösungen konzipiert, wobei ein WLAN-Gerät über Ethernet mit einem oder auch mehreren Endgeräten, z.B. einer Steuerung, verbunden wird.

Auch zukünftig ist damit zu rechnen, dass sich neue WLAN-Standards im industriellen Umfeld etablieren werden – wenn auch durchaus mit anderen Schwerpunkten als in Office-Umgebungen. So verspricht der derzeit noch nicht verabschiedete IEEE 802.11n deutlich höhere Bandbreite. Für industrielle Produkte hingegen wesentlich interessanter ist die verstärkte Robustheit der eingesetzten MIMO-Technik unter den für industriellen Applikationen typischen Reflektionen und daraus resultierenden Mehrwegausbreitungen. Für mobile Anwendungen ist schnelles Roaming eine wesentliche Anforderung, die durch den derzeit in der Entwicklung befindlichen Standard IEEE 802.11r abgedeckt wird. Für Anwendungen in Umgebungen, die eine kabelgebundene Anbindung der APs nicht erlauben, verspricht der kommende Standard IEEE 802.11s (sog. Mesh-Netzwerke) eine Lösung.

Dies zeigt, dass wesentliche Anforderungen schon durch aktuelle Standards (Sicherheit und Unterstützung für Echtzeitverkehr) und Produkte (z.B. robuste Bauart) erfüllt werden. Neuere Standards versprechen eine nochmals verbesserte Robustheit der Kommunikation sowie ein schnelles Roaming auf Standardbasis für echtzeitkritische Anwendungen. Ein Problem, das von den Standards der IEEE allerdings nicht abgedeckt wird, ist die Verwaltung großer WLAN-Installationen. In Installationen mit 50 und mehr APs sind Konfiguration, Update und Überwachung der Geräte über einzelne Web-Schnittstellen nicht mehr handhabbar. Switched-WLAN Architekturen, die im folgenden Abschnitt näher vorgestellt werden, bieten hier eine vielversprechende Lösung.

3. Switched WLAN

Beim Betrieb eines Netzwerkes lassen sich 3 Funktionsbereiche unterscheiden: Daten, Kontrolle und Management, also der eigentliche Datentransport, Funktionen zur unmittelbaren Kontrolle des Datentransportes (z.B. Bestätigungen und Reservierungen) und Managementfunktionen (z.B. Konfiguration und Überwachung). In bisherigen WLAN-Implementierungen werden alle diese Funktionen zusammen im AP realisiert (sog. autonomer oder Fat-AP). Solche autonomen APs sind heute weit verbreitet im Home- und Office-Bereich und auch alle gängigen Industrie-APs gehören zu dieser Geräteklasse.

In Netzwerken mit wenigen Geräten ist der Einsatz autonomer APs durchaus sinnvoll, da sie zu einem überschaubaren Preis alle Funktionen zum Betrieb eines drahtlosen Netzes bereitstellen. In großen Installationen steigt der Managementaufwand aber zu sehr an. Das haben auch die großen Hersteller im Office-Bereich erkannt und bieten seit geraumer Zeit WLAN-Management-Systeme an, die eine zentralisierte Verwaltung autonomer APs erlauben. Aber auch die Zentralisierung der Daten- und Kontrollebene bringt Vorteile mit sich und so entstand das weitergehende Konzept des „Switched WLAN“, bei dem auch große Teile dieser

Funktionsbereiche vom AP in eine zentrale Komponente, den Access Controller (AC), verlegt werden [6, 4]. Die APs werden zu reinen Wireless Termination Points (WTPs), die auch als „Lightweight APs“ bezeichnet werden und nur noch die Aufgabe haben, die Frames zwischen den WLAN-Clients und dem AC zu vermitteln. Die Vorteile, die sich aus einer solchen Zentralisierung der Funktionen ergeben, sind offensichtlich:

Im Management-Bereich kann insbesondere der Wartungsaufwand erheblich reduziert werden. Alle Netzwerk-Parameter und auch die Firmware werden zentral am AC gespeichert und automatisch auf die WTPs übertragen. Auch bei einem Wechsel der WTP-Hardware werden die korrekten Parameter automatisch eingerichtet. Zum Austausch von WTPs werden keine IT-Spezialisten mehr benötigt, so dass die MTTR sinkt und die Verfügbarkeit steigt. Außerdem kann der AC die erforderlichen individuellen Radio-Parameter (insb. Kanal und Sendeleistung) der WTPs dynamisch ausmessen und so die optimale Kanalbelegung und Funkzellengröße ermitteln. Bei WTP-Ausfällen oder Änderungen der Umgebung (z.B. Umbauten oder Störungen) kann das Gesamtsystem die Radio-Parameter selbstständig anpassen und so ein sog. „self healing“ umsetzen. Auch für die Sicherheit bringen Switched WLANs Vorteile. Durch die Zentralisierung kann der AC globale Sicherheitsrichtlinien (wie z.B. eine Nutzerauthentifizierung) konsistent umsetzen und durch eine zentrale Überwachung des Funknetzes Angriffe erkennen.

Im Kontrollbereich ermöglichen Switched WLANs eine verbesserte Quality-of-Service. So kann etwa der AC mit seinem zentralen Wissen über die Netzwerklasten eine Zugangskontrolle und Lastverteilung durchführen. Darüber hinaus kann der AC durch eine zentralisierte Klassifizierung der Verkehrsströme Prioritäten und damit letztlich Bandbreiten und Verzögerungszeiten für einzelne Verkehrsströme und/oder WLAN-Clients festlegen und durchsetzen. Gegenüber einem verteilten Ansatz mit autonomen APs liegt der Vorteil der Zentralisierung hier darin, dass die entsprechenden Spezifikationen global festgelegt werden können. Damit entfällt beim Zellwechsel die erneute Bekanntmachung und Planung. Zusätzlich können durch eine zentrale Authentifizierung und Schlüsselverwaltung Clients insbesondere beim Zellwechsel einen erheblichen Teil an Protokoll-Overhead einsparen.

Bei der Datenübertragung erlauben Switched WLANs die Implementierung von virtuellen Schicht-2/3-Strukturen. Beim Einsatz von autonomen APs in großflächigen Netzen tritt das Problem auf, dass verschiedene APs in verschiedenen Subnetzen angesiedelt sind und ihre Clients in verschiedenen IP-Bereichen arbeiten. Für einen Client, der zwischen zwei solchen APs wechselt, heißt dies, dass er entweder einen IP-Adresswechsel durchführen muss, z.B. via DHCP, oder dass er über komplexe Mechanismen wie Mobile IP eine Umleitung seines IP-Verkehrs einleiten muss. Mit VLANs lässt sich dieses Problem zwar teilweise umgehen,

was aber eine umfassende und konsistente VLAN-Strukturierung des gesamten drahtgebundenen LANs erfordert. Switched WLANs hingegen können den gesamten WLAN-Verkehr durch ein beliebiges IP-Netz vom WTP zum AC tunneln und einen Client so mit einer festen IP-Adresse überall unabhängig von seiner Position und der Subnetz-Zugehörigkeit des WTPs ansprechen, was wiederum ein schnelles und nahtloses Roaming ermöglicht.

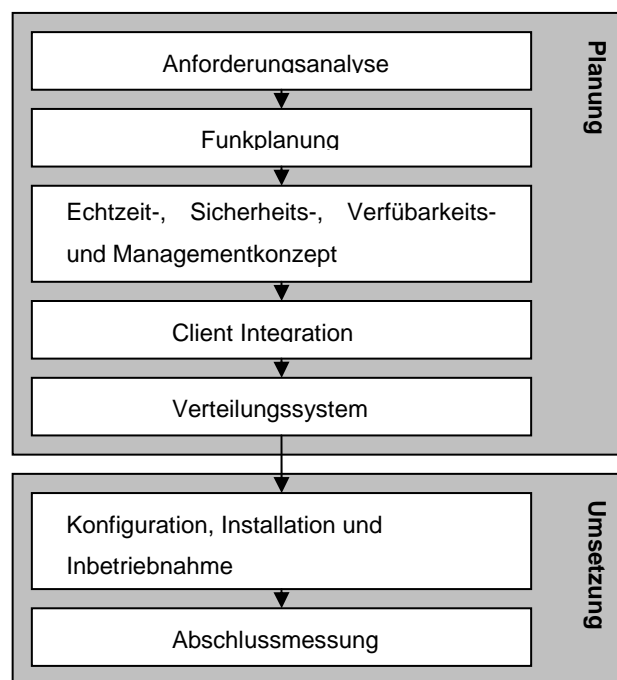


Bild 1: Schritte bei der Planung einer WLAN-Installation

4. WLAN-Planung für industrielle Applikationen und Umgebungen

Der bisher beschriebene aktuelle Stand der Technik bietet die Voraussetzungen, um für die meisten Anwendungen eine angemessene WLAN-Lösung zu entwickeln. Eine solche Lösung ist jedoch nicht durch einfaches Plug-and-Play der ausgewählten Komponenten zu realisieren, sondern erfordert eine strukturierte und bedarfsorientierte Planung. Abb. 1 zeigt die hierfür erforderlichen Schritte, die in den folgenden Abschnitten näher erläutert werden

4.1 Anforderungsanalyse

Grundsätzlich gilt, dass es *die* eine optimale Art eine WLAN-Installation auszulegen und zu konfigurieren nicht gibt. Vielmehr ist ein optimales Ergebnis jeweils abhängig von den spezifischen Randbedingungen hinsichtlich Anforderungen der Applikationen, technologischer Integration und Einsatzumgebung. Daher besteht der Anfang der Planung in einer Anforderungsanalyse. Diese muss vor allem die folgenden Punkte klären:

- Von welchen Anwendungen soll die WLAN-Installation verwendet werden?
- Welche Bereiche sollen ausgeleuchtet werden und wie sind in diesen Bereichen die Umgebungsbedingungen hinsichtlich Störung der Funkkommunikation, Montagemöglichkeiten und Belastung der eingesetzten Komponenten? Störungen können sich vor allem durch direkte Hindernisse, Reflektionen und andere Funktechniken ergeben. Die möglichen Montagepunkte können z.B. durch Höhenbegrenzungen (Flughäfen), Ex-Bereiche, schlechte Zugänglichkeit oder problematische Spannungsversorgung begrenzt sein.
- Welche Endgeräte werden zum Einsatz kommen?
- Welche Bandbreiten sind (in welchen Bereichen) erforderlich?
- Welche Anforderungen bestehen hinsichtlich Sicherheit (security), Echtzeit und Verfügbarkeit?
- Welche Randbedingung für das Verteilungssystem sind zu beachten, z.B. hinsichtlich der Möglichkeiten der Verkabelung?

Bei allen genannten Punkten sind neben dem aktuellen Stand vorhersehbare Änderungen (z.B. steigende Bandbreitebedarf der Applikationen oder Regal- und Füllstandsaufwuchs in Lagerhallen) mit zu berücksichtigen.

4.2 Funkausleuchtung

Auf Grundlage der definierten Anforderungen erfolgt die Planung der Funkausleuchtung, bei der die AP-Positionen, Antennen, Kanäle und Sendeleistungen so festgelegt werden, dass der erforderliche Bereich mit den festgelegten Flächenbandbreiten und Redundanzen abgedeckt ist. Wie diese Planung mit Hilfe von Simulationstools [7] sowie auf der Grundlage von Erfahrung und Vorabmessungen erfolgt, kann hier nicht im Detail erläutert werden. Stattdessen soll nur auf die AP-Dichte als einen wesentlichen Aspekt der Planung eingegangen werden.

Es ist nicht per se am besten einen gegebenen Bereich mit einer möglichst kleinen Anzahl APs auszuleuchten. Vielmehr wird die Anzahl der APs von einer Reihe von Anforderungen bestimmt. So kann es z.B. zum Erreichen einer hohen Flächenbandbreite sinnvoll sein, den von einem AP abgedeckten Bereich gezielt zu verkleinern, etwa durch gerichtete Antennen oder eine Verringerung der Sendeleistung. So lassen sich mehr APs überlappungsfrei und damit mehr Bandbreite auf der vorgegebenen Fläche installieren. Ein anderer Grund gezielt mehr APs einzusetzen, ist eine redundante Abdeckung, bei der an jedem relevanten Punkt mindestens zwei APs zu erreichen sind. So kann auch beim Ausfall eines beliebigen APs der ganze Bereich noch vollständig abgedeckt werden.

4.3 Echtzeitanforderungen

Mit einer Funkausleuchtung, die grundsätzlich den Kapazitätsanforderungen der Applikationen genügt, ist die Einhaltung zeitlicher Anforderungen noch nicht sicher gestellt. Vielmehr können durch die Konkurrenz der Stationen beim Medienzugriff sowie durch die Unterbrechung der Erreichbarkeit beim Roaming die Nachrichtenverzögerungen über den Anforderungen liegen. Um die Konkurrenz um das Medium so zu begrenzen und zu koordinieren, dass die zeitlichen Anforderungen eingehalten werden können, müssen die verschiedenen Verkehrsflüsse nach ihren zeitlichen Anforderungen auf die Prioritätenklassen aufgeteilt werden. Zumindest für die Klasse mit der höchsten Priorität ist durch eine Planung der Lasten die Auslastung des Mediums so zu begrenzen, dass die Echtzeitanforderungen erfüllt werden. Weitaus größeren Einfluss auf die Verzögerungen hat aber das Roaming [5]. Die Roamingverzögerungen sind deutlich größer als die Verzögerungen innerhalb einer Zelle. Wie das Roaming gesteuert wird, ist im Standard nicht festgelegt und daher meist von Client zu Client unterschiedlich. Ein Konzept muss also berücksichtigen, wie das Roaming des Client implementiert ist sowie welche Ansteuerungsmöglichkeiten und Parameter zur Kontrolle des Roaming zur Verfügung stehen. Eine Lösung kann dann auf Grundlage der Möglichkeiten der jeweiligen Produkte, die bei industriellen Produkten typischer Weise etwas reichhaltiger sind, so wie der anwendungsspezifischen Randbedingungen erarbeitet werden.

4.4 Verfügbarkeit und Management

Wesentlich für WLAN-Installationen im industriellen Bereich ist die Verfügbarkeit. Diese kann sichergestellt werden durch: die Verwendung robuster Produkte mit einer verlässlichen Infrastruktur (Spannungsversorgung, Verteilungssystem), eine Funkausleuchtung mit hinreichenden Reserven, einer redundanten Auslegung der Funkausleuchtung sowie einem Konzept für die schnelle Fehlererkennung und den schnellen Austausch betroffener Geräte. Letzteres erfordert insbesondere die Integration der APs in die bestehende IT- und/oder Anlagenüberwachung. Falls eine solche noch nicht besteht, muss sie zusammen mit der WLAN-Installation realisiert werden. Die Integration in eine Management-Lösung kann dabei über herkömmliche Methoden wie IO-Ausgänge der Geräte, syslog oder SNMP erfolgen oder aber über eine Switched-WLAN-Lösung. Letztere bieten dabei nicht nur eine genauere, WLAN-spezifische Überwachung des Funknetzes, sie vereinfachen zusätzlich eine eventuelle Reparatur oder realisieren sogar ein „self healing“ (s. Abschnitt 3).

4.5 Sicherheit

Sicherheit, d. h. der Schutz der übertragenen Daten vor Ausspähen und Manipulationen, ist ein wesentlicher Aspekt in WLAN-Installationen, und alle gängigen Produkte unterstützen die aktuellen Sicherheitsstandards WPA bzw. jetzt auch IEEE 802.11i (WPA2), die einen hinreichend Schutz bieten. Das alte WEP-Verfahren, das die Ursache für den zweifelhaften Ruf der WLAN-Sicherheit war, ist kaum mehr im Einsatz.

WPA und WPA2 bieten zwei Modi der Authentifizierung: basierend auf gemeinsamen Schlüsseln für alle Clients und APs oder durch zentrale Authentifizierung mittels IEEE 802.1x. Welches Verfahren gewählt wird, ist eine wesentliche Designentscheidung. Gemeinsame Schlüssel erfordern fast keinen zusätzlichen Aufwand beim Aufbau der WLAN-Installation. In großen Installationen wird mit IEEE 802.1x aber eine bessere Wartbarkeit und Sicherheit erreicht, da jeder Nutzer / jedes Gerät seine eigenen Zugangsdaten hat und diese in einer zentralen Datenbank verwaltet werden. Entsprechende Datenbanken sind oft schon vorhanden, weil sie für andere Zwecke (z.B. Windows-Logon, VPN etc.) schon verwendet werden. IEEE 802.1x hat zurzeit noch den Nachteil, dass es im Vergleich zu gemeinsamen Schlüsseln zu längeren Roaming-Verzögerungen führt. Dieses Problem wird allerdings durch Switched WLANs behoben. Wesentliche Aspekte für das Design der Sicherheitslösung sind also die Größe der Installation, bestehende Infrastruktur wie User-Datenbanken und Radius-Server, die zeitlichen Anforderungen sowie die Frage, ob sich neben eingebetteten Systemen auch menschliche Nutzer mit PDAs oder Laptops anmelden. Besonders zu beachten ist dabei auch die Behandlung von Altgeräten, die noch nicht die ausgewählten Sicherheitsverfahren unterstützen.

4.6 Client Integration

Beim Planen einer WLAN-Lösung ist es essentiell, neben der WLAN-Infrastruktur die Integration der Clients nicht zu vernachlässigen. Ist diese auch für typische Laptops fast immer trivial, so gilt dies für andere Systeme wie Handscanner, Staplerterminals usw. nicht mehr ohne weiteres, insbesondere dann, wenn Altgeräte integriert werden müssen. Aber auch für Neugeräte gilt oft, dass das Hauptkriterium der Auswahl nicht die WLAN-Tauglichkeit, sondern andere Aspekte, etwa die Qualität des Scanners; ist. Um Probleme während der Inbetriebnahme zu vermeiden, sollten daher grundsätzlich Tests zur Einsatzbarkeit der Client-Geräte in der WLAN-Installation durchgeführt werden. Neben der reinen Fähigkeit, sich unter Verwendung der ausgewählten Sicherheitsmechanismen anzumelden und Daten auszutauschen, sollte dabei auch das Roaming-Verhalten der Geräte untersucht werden. Dies gilt zum einen natürlich, wenn zeitliche Anforderungen an das Roaming oder Fail-Over der

Clients bestehen. Zum anderen ist aber das Roaming-Verhalten entscheidend dafür, ob die von der WLAN-Installation bereitgestellte Flächenbandbreite auch genutzt wird. Clients, die zu lange an einer schlechten Verbindung festhalten, erzielen nicht nur selbst eine geringe Bruttodatenrate, sie Bremsen auch andere Geräte aus. Ähnliches gilt auch für die Integration von 802.11b-Geräten. Diese erzielen nicht nur selbst geringe Datenraten, sie belegen auch für relativ lange Zeiten das Medium und erfordern von den 802.11g-Geräten das Senden zusätzlicher Nachrichten, so dass sie auch diese ausbremsen. Durch frühzeitige Tests mit den Clients können potentielle Probleme erkannt und durch eine entsprechende Konfiguration, ein Update oder eine Separierung der betroffenen Clients meist gelöst werden.

4.7 Verteilungssystem

Neben der Planung des eigentlichen Funknetzes aus WLAN-Clients und APs muss auch das Verteilungssystem, über das die APs mit dem restlichen Netzwerk und untereinander verbunden werden, geplant werden. Zu beachten ist dabei der Abstand zwischen den APs und den Switches. Bei Abständen über 100m müssen Lichtwelleleiter und damit APs mit entsprechenden Schnittstellen oder Medien-Konverter verwendet werden. Ist eine Verkabelung der APs gar nicht möglich oder zu kostenintensiv, kann ein drahtloses Verteilungssystem (Wireless Distribution System, WDS) geplant werden, bei dem die Anbindung der APs an die LAN-Infrastruktur selbst wieder über drahtlose Verbindungen erfolgt. Um auch bei dieser Art der Anbindung einen möglichst hohen Durchsatz zu erreichen, können APs mit zwei WLAN-Schnittstellen zum Einsatz kommen. Eine Schnittstelle dient dabei der Kommunikation mit den Clients, die andere dem Anschluss an das Verteilungssystem. Die IEEE ist derzeit dabei, in der Task Group 802.11s ein Protokoll zu entwickeln, das den interoperablen und selbstkonfigurierenden Betrieb eines solchen WDS ermöglicht (s. Abschnitt 2).

Bei der Planung der Topologie des Verteilungssystems und der IP-Adressen ist es häufig günstig, alle WLAN-Geräte in einem Segment zu betreiben. Dies vermeidet zum einen ein Layer-3-Roaming beim Zellenwechsel, zum anderen kann so an einem zentralen Punkt der Verkehr zwischen WLAN- und LAN-Infrastruktur gefiltert werden. Ist eine solche Struktur aufgrund der physischen Randbedingungen nicht zu realisieren, können die Geräte mittels VLANs auch in einem virtuellen Segment zusammengeführt werden. Auch Switched-WLANs ermöglichen in weitläufigen physischen Strukturen durch die Zentralisierung der Datenfunktionen die Zusammenfassung der WLAN-Geräte in einem Segment.

5. Fazit

Zur Realisierung drahtloser Anwendungen in der industriellen Automation gibt es heutzutage Produkte unterschiedlicher Hersteller, die neben einer robusten Bauart sowie den typischen Montage- und Anschlussmöglichkeiten auch die aktuellen und relevanten Standards der IEEE hinsichtlich Sicherheit und Echtzeitfähigkeit unterstützen. Ein Problem, das noch nicht vollständig zufriedenstellend gelöst ist, ist sicherlich das Management großer Installationen, auch wenn über SNMP grundsätzlich eine Möglichkeit der zentralen Verwaltung gegeben ist. Mit der Switched-WLAN-Architektur hat sich im IT-Umfeld schon eine Lösung durchgesetzt, die vor allem auch für die Automation vielfältige Vorteile bietet. Was fehlt sind derzeit noch spezifische industrielle Erweiterungen dieses Ansatzes, wie sie für APs und Clients bereits realisiert sind.

Grundsätzliches lassen sich auf dieser technologischen Basis die meisten, wenn auch nicht alle Anwendungen realisieren. Wesentlich ist eine strukturierte Planung, die neben der reinen Funkabdeckung auch andere Aspekte wie Sicherheit, Verfügbarkeit, Echtzeitfähig und die Client-Integration von Anfang an mit einbezieht. In komplexen Installationen sollten durch frühzeitige Messungen zur Funkabdeckung und zur Client-Integration potentielle Probleme vor der Inbetriebnahme erkannt und behoben werden.

7. Referenzen

- [1] IEEE Standard 802.11, Standards for Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999
- [2] IEEE 802.11i, Amendment 6: Medium Access Control Security Enhancements, 2004
- [3] IEEE 802.11e, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005
- [4] U. Mülder: Konzept und Implementierung einer offenen „Switched WLAN“ Infrastruktur, Diplomarbeit, FH Wiesbaden, Feb. 2005
- [5] S. Schemmer, S. Vandersee: Schnelles Roaming – Eine Schlüsselanforderung für industrielle drahtlose Netze, Wireless Technologies 2005
- [6] S. Schemmer, S. Vandersee, M. Gergeleit: Switched WLAN in der Automatisierung – Bessere Kontrolle für komplexe WLANs, Wireless Technologies 2006
- [7] K. Schwendler: Konzept, Realisierung und Validierung eines WLAN-Planungswerkzeuges auf der Basis grafischer Algorithmen, Diplomarbeit, FH Wiesbaden, Apr. 2006