SIEMENS

Systemhandbuch • 01/2016

Grundlagen zum Aufbau eines Industrial Wireless LAN

SCALANCE W

https://support.industry.siemens.com/cs/ww/de/view/22681042

Gewährleistung und Haftung

Hinweis

Die Anwendungsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Anwendungsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Anwendungsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Anwendungsbeispiele erkennen Sie an, dass wir über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden können. Wir behalten uns das Recht vor, Änderungen an diesen Anwendungsbeispiele jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesem Anwendungsbeispiel und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

Für die in diesem Dokument enthaltenen Informationen übernehmen wir keine Gewähr.

Unsere Haftung, gleich aus welchem Rechtsgrund, für durch die Verwendung der in diesem Anwendungsbeispiel beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z. B. nach dem Produkthaftungsgesetz in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit, wegen einer Übernahme der Garantie für die Beschaffenheit einer Sache, wegen des arglistigen Verschweigens eines Mangels oder wegen Verletzung wesentlicher Vertragspflichten zwingend gehaftet wird. Der Schadensersatz wegen Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit zwingend gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist hiermit nicht verbunden.

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.industry.siemens.com.

Inhaltsverzeichnis

Vorwort

Ziel des Dokuments

Dieses Dokument gibt Ihnen einen Überblick über die besonderen Anforderungen an den Aufbau eines Industrial Wireless LANs und macht sie mit den Eigenschaften der relevanten SIEMENS-Produkte vertraut.

Sie werden zuerst an die Thematik drahtloser lokaler Netzwerke („WLANs“) im industriellen Umfeld herangeführt, und es werden Ihnen die wesentlichen technischen Prinzipien vorgestellt. Wir zeigen Ihnen im Anschluss verschiedene SIEMENS-Produkte, beleuchten deren Einsatzmöglichkeiten und geben Ihnen Entscheidungshilfen an die Hand, um die für Ihre Aufgabenstellung optimale Lösung zu wählen.

Kerninhalte dieses Dokuments

Folgende Kernpunkte werden in diesem Dokument behandelt:

- Eigenschaften von WLANs im Allgemeinen,
- SIEMENS-Produkte zum Aufbau drahtloser Netzwerke im industriellen Umfeld im Besonderen.

Abgrenzung

Dieses Dokument enthält keine ausführliche Beschreibung zur Software-Installation und zur Inbetriebnahme der einzelnen Komponenten.

Aktuelle und detaillierte Informationen zu diesem Thema können Sie in den Handbüchern und Betriebsanleitungen der entsprechenden Produkte finden.

Referenz zum Automation and Drives Service & Support

Dieser Beitrag stammt aus dem Internet Applikationsportal des Siemens Industry Automation and Drives Technologies Service & Support. Durch den folgenden Link gelangen Sie direkt zur Downloadseite dieses Dokuments.

http://support.automation.siemens.com/WW/view/de/22681042

1 Funkwellen als Basis eines „Shared Medium“-Netzwerks

1.1 Übersicht Funkstandards

Es existieren derzeit eine Reihe verschiedenster Technologien für den Aufbau von Funknetzen, wie Bluetooth, GPRS und UMTS für mobile Telefonnetze, RFID-Tags zur Identifizierung und Warenverfolgung, etc. (siehe hierzu auch Kapitel 3).

Im Rahmen dieses Dokuments beschränken wir uns auf WLANs im engeren Sinne, also auf Funknetze, die dem IEEE 802.11-Standard (siehe Kapitel 2) folgen. Als "IWLANs" ("Industrial WLANs") bezeichnen wir WLANs, die durch besondere Maßnahmen "gehärtet", d. h. für die Anforderungen und Umgebungen des Industriebereichs nutzbar gemacht wurden.

1.2 Einführung in Funk-Netzwerke

1.2.1 Vergleich zwischen Funkwellen und Kabeln

Die Verwendung von Kabeln und Leitungen zur Kommunikation besitzt gewisse Vorteile, da hierbei ein exklusives Medium zur Verfügung steht: Die Übertragungseigenschaften dieses Mediums sind wohldefiniert und gleichbleibend (sofern nicht Kabel, Router o. ä. getauscht werden), und es ist jederzeit klar erkennbar, welche Teilnehmer mit einem „Local Area Network“ (soviel wie „Örtlich begrenztes Netzwerk“, Abk. „LAN“) verbunden sind und welche nicht.

Umgekehrt steigt der Aufwand für die Verkabelung (und die Möglichkeit für Kabelbrüche und andere Hardwarefehler) mit der Zahl der Teilnehmer. Die Kommunikation mit sich frei bewegenden Teilnehmern ist mit drahtgebundenen Methoden schließlich nur noch in Ausnahmefällen praktikabel. Funkstrecken ermöglichen außerdem auch die Überbrückung von Abschnitten, die anderenfalls schwer verkabelbar wären (Straßen, Gewässer).

In diesen Anwendungsfällen können funkgestützte Netzwerke ihre Vorteile (die zusammengefasst in ihrer geringeren Ortsgebundenheit liegen) zur Geltung bringen. In diesen Fällen wird der möglicherweise höhere Investitionsaufwand durch größeren Kundennutzen wettgemacht.

1.2.2 Komplexität des Funkfeldes

Radiowellen breiten sich durch den Raum aus, werden an Hindernissen gebeugt, reflektiert oder beim Durchgang abgeschwächt, und erzeugen so ein komplex gestaltetes Funkfeld, das sich noch dazu ändert, wenn sich die Hindernisse bewegen. So ist es offensichtlich, dass der Bereich, der durch einen oder mehrere Sender ausgeleuchtet wird, nicht scharf definiert ist. Demzufolge gibt es keine klare Abgrenzung des Funkfeldes, wodurch die Übertragungseigenschaften für die einzelnen Teilnehmer des Funknetzes je nach deren Position schwanken. Außerdem ist es praktisch unmöglich, einen „schweigenden Mithörer“ in einem Funknetz zu entdecken.

Diese Eigenschaften sind von großer Tragweite für Fragen der Verbindungszuverlässigkeit und der Abhör- bzw. Störsicherheit eines Netzwerks. Bei verantwortungsvoller Administration, sorgfältiger Planung und dem Einsatz geschulter Mitarbeiter, die für die besonderen Belange eines Funknetzes sensibilisiert sind, sind diese jedoch so zuverlässig, sicher und robust wie drahtgestützte Netzwerke.

1.2.3 Zugriffsregelung in einem „Shared Medium“-Netzwerk

Funknetze sind sogenannte „Shared Medium“-Netzwerke d. h., alle Stationen teilen sich das Netzwerk. Um Mehrfachzugriff auf das Netzwerk zu verhindern, bedarf es einer Regelung, welcher Teilnehmer wann senden darf.

Zu diesem Zweck dient das CSMA (Carrier Sense Multiple Access). Dieses Verfahren verlangt von jeder Station vor dem Sendevorgang eine Überprüfung, ob das Medium frei ist. Erst dann dürfen Daten gesendet werden.

Erfolgt die Überprüfung von zwei Stationen gleichzeitig, kann es aber vorkommen, dass beide das Medium als frei erkennen und zur selben Zeit Daten senden. Es kommt zu einer Kollision und die Daten werden unbrauchbar. Eine drahtlose Sendestation kann selbst keine Signalkollision feststellen. Das eigene Signal überdeckt die Signale der anderen Stationen, und Kollisionen können nicht von Störungen unterschieden werden.

Um solche nicht erkennbaren Kollisionen möglichst zu verhindern, wird zusätzlich das CA (Collision Avoidance)- Verfahren angewandt. Ist das belegte Medium nun frei, startet eine sendewillige Station nicht sofort mit der Datenübertragung, sondern wartet eine zufällig bestimmte Zeit. Nach Ablauf dieser Wartezeit überprüft die Station erneut den Status des Mediums. Durch die Zufallswartezeit ist es sehr unwahrscheinlich, dass beide gleichzeitig zu senden beginnen.

1.3 Bevorzugte Anwendungsbereiche

In zahlreichen Umgebungen sind Funknetze aufgrund ihrer besonderen Eigenschaften das bevorzugte, wenn nicht gar das einzige möglich einzusetzende Medium.

Zu denjenigen Anwendungsbereichen, für die Funknetze prädestiniert sind, zählen unter anderem:

- Verbindung frei beweglicher Teilnehmer untereinander und mit stationären Teilnehmern,
- Verbindung beweglicher Teilnehmer mit kabelgebundenen Netzen (Ethernet, etc.),
- Kontakt zu rotierenden Teilnehmern (Kräne, Karussells, ...),
- Anschluss von Teilnehmern mit begrenzter Mobilität (Einschienenhängebahnen, Hochregallager, ...), zum Ersatz von Schleifkontakte oder Schleppkabeln,
- Aufbau von Funkbrücken zwischen physisch getrennten (verschiedene Gebäude, Straßen, Gewässer, ...) kabelgebundenen Subnetzen,
- Kommunikation mit Teilnehmern in schwer zugänglichen Bereichen.

1.4 Die Physik von Funkwellen

1.4.1 Ausbreitung

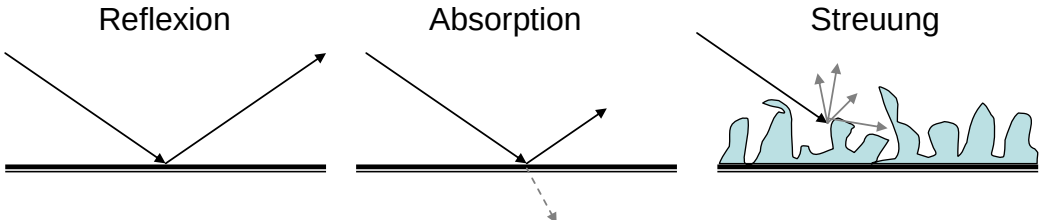
Im Gegensatz zu Signalen in einer Leitung breiten sich Radiosignale als elektromagnetische Wellen dreidimensional im Raum aus.

Durch Hindernisse und Gegenstände wird die Ausbreitung der Funkwellen beeinflusst; es treten Effekte wie Reflexion, Streuung, Absorption, Interferenz und Beugung auf.

Reflexion und Absorption

Treffen die Wellen auf einen Gegenstand, so werden sie so gut wie vollständig reflektiert, wenn der Gegenstand elektrisch leitend ist. Bei nichtleitenden Gegenständen wird ein Teil der Wellen reflektiert, ein anderer wird im Gegenstand absorbiert, und ein Rest wird schließlich durch den Gegenstand gelassen. Beim Auftreffen auf Kanten werden Funkwellen praktisch in alle Richtungen gestreut.

Abbildung 1-1



Fading und Beugung

Zwei weitere Eigenschaften sind für die Ausbreitung der Funkwellen noch von Bedeutung:

- Zum einen können sich Funkwellen (anders als inkohärentes Licht) gegenseitig verstärken oder sogar auslöschen (sog. „Fading oder Interferenz“). Befindet sich ein Empfänger also sowohl im direkten Strahl eines Senders als auch in dessen Reflexion, so detektiert er nicht notwendigerweise die doppelte Signalstärke, sondern er wird unter Umständen gar kein Signal mehr wahrnehmen.
- Zum anderen hängen die Ausbreitungseigenschaften der Wellen überdies von ihrer Wellenlänge ab, d. h. hochfrequente Funkwellen verhalten sich anders als niederfrequente. Insbesondere können langwellige (d. h. niederfrequente) Funkwellen um Gegenstände herum „gebeugt“ werden. Ähnlich wie bei Schall oder Wasserwellen ist es dann möglich, selbst im „Schatten“ einer Funkquelle Signale zu empfangen.

Interferenz- und Beugungsphänomene spielen sich grundsätzlich in Größenordnungen ab, die der Wellenlänge der verwendeten Strahlung entsprechen. Bei den WLANs, die dem IEEE 802.11-Standard folgen, liegt diese zwischen 12 cm und 6 cm, was bedeutet, dass Verschiebungen um eine Baugruppenbreite bereits zu einem veränderten Sende- und Empfangsverhalten führen können.

Frequenzabhängigkeit der Eigenschaften von Funkwellen

Als Faustregel lässt sich sagen, dass die Eigenschaften von Funkwellen sich denen des Lichts annähern, je höherfrequenter und kurzwelliger die Schwingungen sind: Hochfrequente Sender breiten sich in gerader Linie aus und erreichen keine Empfänger hinter Gegenständen mehr. An Oberflächen werden sie fast vollständig absorbiert oder reflektiert.

Längerwellige Signale hingegen gehen auch „um Gegenstände herum“ und dringen tiefer in nichtleitende Objekte ein bzw. können diese durchdringen.

1.4.2 Störungen

Jeder Gegenstand, der sich räumlich innerhalb eines Funknetzes befindet, kann dieses Netz stören, wenn er auf der von den Sendern verwendeten Frequenz Signale aussendet. Im Gegensatz zu Leitungen, die relativ einfach und zuverlässig abgeschirmt werden können, sind Funknetze anfällig für Störungen durch beliebige Geräte in ihrer Umgebung, die intermittierend oder ständig, auf eng begrenzten Kanälen oder breitbandig strahlen können.

Dazu zählen Geräte, die als Sender entworfen sind, wie Schnurlostelefone und Bluetooth-Geräte, aber auch Mikrowellenherde, Schweißgeräte, etc.

Derartigen Störungen kann jedoch durch eine sorgfältige Planung des Funknetzes bereits im Vorfeld begegnet werden.

1.4.3 Reichweite und Datenrate

Die Reichweite und die erzielbare Datenrate eines Funksenders hängen unter anderem von der verwendeten Frequenz ab.

Reichweite

Prinzipiell haben kurzwellige (höherfrequente) Sender eine geringere Reichweite als langwellige: Die kurzwelligen Signale verhalten sich ähnlicher dem Licht, können sich nur in gerade Linie ausbreiten und werden an Gegenständen vollständig absorbiert oder reflektiert. Das hat zur Folge, dass die Signalqualität stark abnimmt, wenn die freie Sichtverbindung zwischen Sender und Empfänger beeinträchtigt ist. Allerdings kann die Reichweite durch die Verwendung von Richtantennen noch einmal deutlich gesteigert werden.

Mit dem SIMATIC NET Selection Tool (siehe Kapitel 9.6) kann die Reichweite in Abhängigkeit von mehreren Parametern, wie Frequenz und Sendeleistung, ermittelt werden.

Datenrate

Die maximale Datenrate, die auf einer Trägerwelle übertragen werden kann, ist proportional zu der Bandbreite, die zur Verfügung steht, d. h. je größer die Bandbreite, desto größer die erreichbare Datenrate.[1]

Sender auf einer Frequenz von 2,4-GHz (wie sie das IEEE 802.11-Verfahren verwendet) können mit omnidirektionalen Antennen typischerweise Reichweiten zwischen ca. 30 m bzw. 100 m (im Innen- bzw. Außenbereich) erzielen (siehe auch Tabelle 2-2). Die Datenraten, die auf diesem Band übertragen werden können, betragen bis zu 450 Mbit/s.

[1] Die theoretisch erzielbare Brutto-Datenrate (in bit/s) ist proportional zu der Bandbreite. Diese Abhängigkeit wird durch das Shanon-Hartley-Theorem wiedergegeben.

Relevanz der Datenrate

Welche Datenrate für eine bestimmte Anwendung wirklich nötig bzw. ausreichend ist, hängt – selbst bei optimalen Verbindungen -- nicht nur vom Aufkommen der Nutzdaten ab. Protokollbedingt ergibt sich ein mehr oder minder großer Overhead für die Abwicklung des Funkverkehrs, und zwischengeschaltete Geräte wie Access Points, Router etc. führen ebenfalls Verzögerungen ein, die beim Weiterreichen der Signale entstehen.

So wird die erzielbare Netto-Datenrate in vielfältiger Weise von Gestaltung und Parametrierung des tatsächlich vorhandenen Funknetzes beeinflusst.

1.4.4 Frequenzen, Frequenzabstände und Kanäle

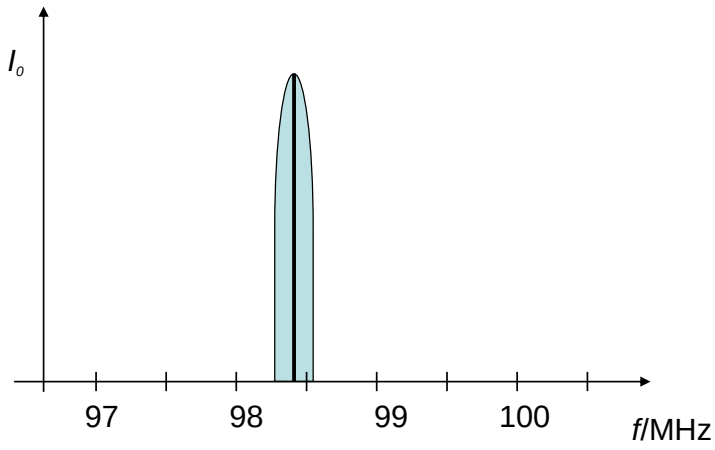
Auf jeder Funkfrequenz soll zu jedem Zeitpunkt nur ein Teilnehmer senden. Senden mehrere Stationen gleichzeitig auf derselben Frequenz, so ist keine von beiden zu empfangen; man spricht in so einem Fall von einer „Kollision“.

Eine der wichtigsten Aufgaben eines WLAN-Protokolls – d. h. der Regeln, nach denen die Teilnehmer des Netzwerks kommunizieren – ist es, das Auftreten von Kollisionen zu vermeiden, da Kollisionen immer ein zeitaufwendiges Wiederholen der einzelnen Telegramme erfordern.

Frequenzen und beanspruchtes Spektrum

Streng genommen ist die Aussage, dass ein Sender auf genau einer Frequenz abstrahlt, nicht korrekt: Das wäre nur der Fall bei einem reinen Sinus-Signal. Der Sender nimmt auch einen Bereich der Frequenzen oberhalb und unterhalb der Trägerfrequenz ein. Aus diesem Grund müssen die Sender einen Frequenz-Abstand voneinander halten, der proportional zur verwendeten Datenrate ist: Man spricht hierbei von der „Bandbreite“, die der Sender einnimmt.[2]

Abbildung 1-2



Die obige Abbildung zeigt beispielhaft das Verhalten eines UKW-Senders. Neben der eigentlichen Trägerfrequenz (ca. 98.4 MHz) wird hier noch ein Frequenzband zu beiden Seiten beansprucht (blau). Die Bandbreite ist in diesem Fall übertrieben; in der Realität genügen 40 kHz für ein FM-Signal.

[2] Umgangssprachlich wird als „Bandbreite“ generell die Übertragungskapazität bezeichnet.

Bänder und Kanäle

Um die Übersichtlichkeit zu wahren, ist das Radiospektrum, d. h. der gesamte Frequenzbereich des Funkverkehrs, in einzelne „Bänder“ gegliedert. Die verschiedenen Bänder unterscheiden sich durch das funktechnische Verhalten (Reichweite, Störanfälligkeit, mögliche Datenrate, etc.), und konsequenterweise auch in ihren Anwendungen.

Die Frequenzbänder ihrerseits sind in „Kanäle“ unterteilt, die in einem gewissen Abstand voneinander auf das jeweilige Band verteilt werden.

Der 2,4-GHz-Bereich des ISM-Bands[3] z. B. ist in dreizehn Kanäle mit Mittenfrequenz zwischen 2,412 GHz und 2,472 GHz unterteilt, wobei der Abstand zwischen benachbarten Kanälen jeweils 5 MHz beträgt. Theoretisch können dreizehn Sender das Band gleichzeitig verwenden.[4]

1.5 Antennen

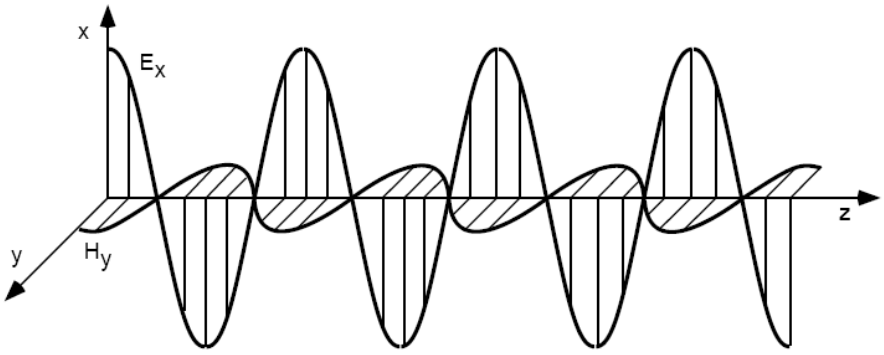
Aufgabe

Eine Antenne wandelt elektrische Ströme und elektromagnetische Wellen ineinander um. Sie sendet elektromagnetische Wellen in den Raum aus und empfängt diese im gleichen Maße. Jede Antenne besitzt einen bestimmten Frequenzbereich, innerhalb dessen die Kopplung zwischen dem Strom in der Antenne und der umgebenden Welle maximal ist.

Elektromagnetische Wellen

Elektromagnetische Wellen bestehen aus einem elektrischen Feldvektor E_x und einem magnetischen Feldvektor H_y. die stets rechtwinklig zueinanderstehen. Dabei ist der Strom die Ursache des magnetischen Feldvektors und die Spannung die Ursache des elektrischen Feldvektors (siehe Grafik).

Abbildung 1-3



[3] „Industrial, Scientific and Medical“; siehe hierzu auch das Glossar.

[4] Da die Frequenzbereiche von Sendern auf benachbarten Kanälen einander jedoch überlappen, gibt es nur drei Kanäle, die gegenseitig störungsfrei sind (siehe hierzu auch Kapitel 2.4.1).

1.5.1 Charakteristika einer Antenne

Impedanz

Als Impedanz wird ein frequenzabhängiger Widerstand beschrieben. Bei den IWLAN-Komponenten (Antenne, Kabel) liegt dieser Widerstand bei 50 Ohm. Dabei ist es wichtig, dass die Impedanzen einer Antenne (d. h. Ein- / Ausgang an der Antenne und am Antennenkabel) aufeinander abgestimmt sind.

Polarisation

Die Polarisation gibt die Richtung des Vektors der elektrischen Feldstärke in der ausgestrahlten elektromagnetischen Welle an. Man unterscheidet dabei zwischen linearer und zirkularer Polarisation. Bei der linearen Polarisation verlaufen die elektrischen Feldlinien in einer Ebene. Sind sie senkrecht zur Erdoberfläche gerichtet, spricht man speziell von vertikaler Polarisation; verlaufen sie horizontal zur Erdoberfläche, so liegt horizontale Polarisation vor.

Ist die Richtung der elektrischen Feldkomponente nicht fixiert, sondern läuft kontinuierlich in Kreisform, dann spricht man von zirkularer Polarisation. Je nach Umlaufsinn unterscheidet man hier noch in rechtsdrehender und linksdrehender Polarisation.

Tabelle 1-1

Polarisation	Elektrische Feldrichtung	Magnetische Feldrichtung
Linear vertikal	Vertikal	Horizontal
Linear horizontal	Horizontal	Vertikal
Zirkular	Konstant um die Achse der Ausbreitung zirkulierend (links- oder rechtsdrehend)	

Für optimalen Empfang ist es wichtig, dass bei korrespondierenden Antennen die Polarisation beider identisch ist. Unterscheiden sich die Polarisationsebenen z. B. um 90°, ist eine Dämpfung von 20 dB keine Seltenheit.

Daher ist insbesondere bei Antennen mit mehreren Strahlern in einem Gehäuse (Dual / MIMO) auf die Ausrichtungen der Polarisationsebenen zu achten.

1.5.2 Omnidirektionale- und Richtantennen

Antennen können entweder omnidirektional oder gerichtet abstrahlen. Die gerichteten Antennen erreichen generell höhere Reichweiten, was aber nicht der Effekt einer größeren Sendeleistung ist, sondern durch die Formgebung des Funkfeldes zustande kommt.

Antennengewinn

Der Antennengewinn ist eine Messgröße, die beschreibt, wie stark eine Antenne verglichen mit einem Referenzstrahler sendet und empfängt.

Als Referenz dient hierbei ein isotroper Kugelstrahler, d. h. ein idealisierter Punktstrahler, der gleichmäßig in alle Richtungen des Raums sendet bzw. empfängt. Der Gewinn des isotropen Kugelstrahlers wird dazu gleich null gesetzt.

Die Einheit des Antennengewinns ist üblicherweise „dBi“ (i = isotroper Kugelstrahler). Ein Gewinn von 3 dBi entspricht dabei ungefähr einer Verdoppelung der Sende- / Empfangsleitung.[5]

Antennendiagramme

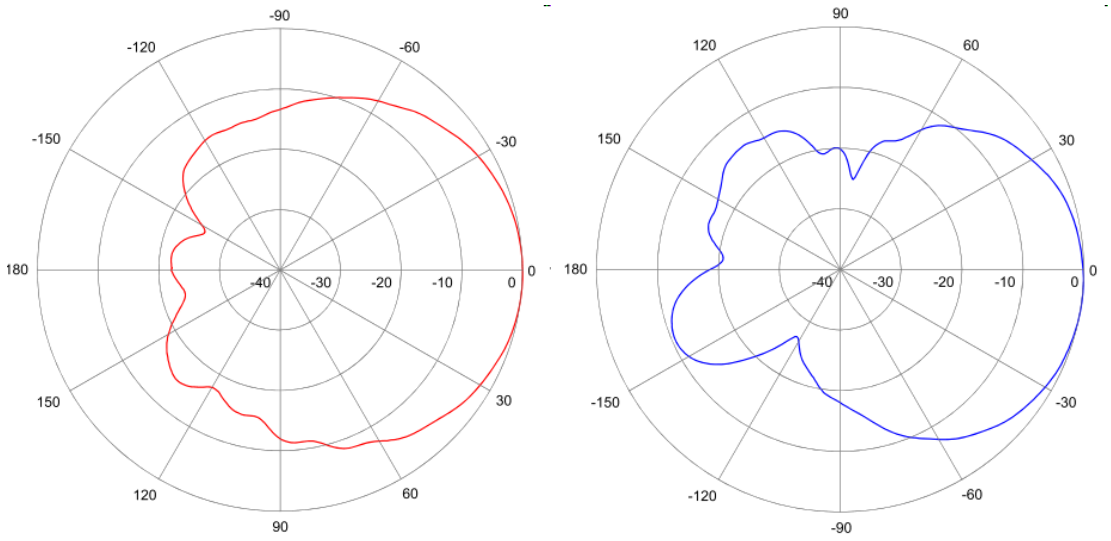
Ein Antennendiagramm beschreibt die Richtcharakteristik einer Antenne, indem der richtungsabhängige Antennengewinn gemessen wird. Üblicherweise erfolgt die Darstellung des Richtdiagramms in Polarkoordinaten.

Ein horizontales Antennendiagramm ist eine Draufsicht auf das elektromagnetische Feld einer Antenne mit der Antenne im Mittelpunkt. Aufgetragen wird der Gewinn als Abstand vom Zentrum des Koordinatensystems über dem Sende- / Empfangswinkel.

Ein vertikales Antennendiagramm ist eine Seitenansicht des elektromagnetischen Feldes der Antenne. Aufgetragen wird also der Antennengewinn über dem Winkel zur Symmetrieebene der Antenne.

Die folgende Grafik zeigt ein horizontales (links) und ein vertikales (rechts) Antennendiagramm einer Richtantenne.

Abbildung 1-4

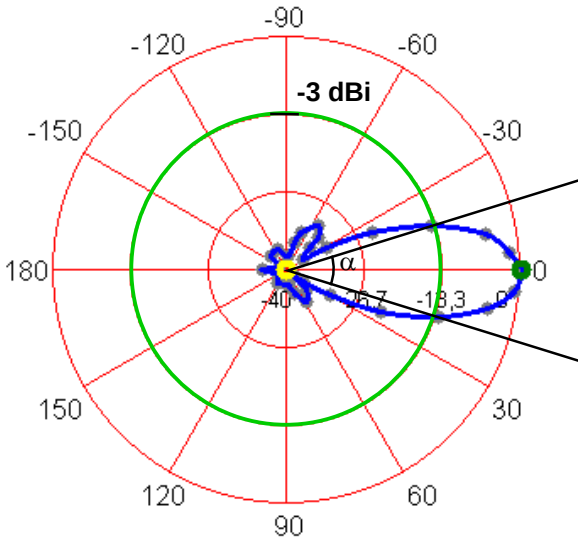


[5] Da der Antennengewinn in Logarithmen gemessen wird, entsprechen 6 dBi einer Vervierfachung der Leistung, 9 dBi einer Verachtfachung etc.

Öffnungswinkel

Als Öffnungswinkel wird der Winkelabstand bezeichnet, bei dem die Feldstärke der Antenne auf ungefähr die Hälfte ≈ 3 dBi des Maximums abgefallen ist. Die folgende Grafik zeigt am Beispiel eines Antennendiagramms wie der Öffnungswinkel bestimmt werden kann. Grün dargestellt ist der -3-dBi-Kreis, der die Hälfte des Signalmaximums (= 0 dBi) markiert. Die Schnittpunkte des blauen Antennengewinndiagramms mit dem grünen Kreis definieren den Öffnungswinkel α der Antenne. (Hier: ca. 30°)

Abbildung 1-5



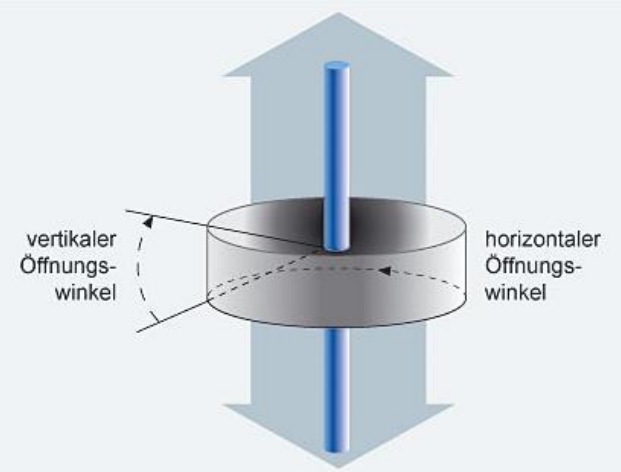
Je nach Geometrie sind die horizontalen und vertikalen Öffnungswinkel einer Antenne in der Regel voneinander verschieden.

Omnidirektionale Antennen

Omnidirektionale Antennen haben prinzipiell die Form eines Stabes oder geraden Drahtes. Die Bezeichnung ist insofern irreführend, als die Abstrahlung nicht wirklich isotrop, d. h. nicht in allen Richtungen gleich stark ist. Das Funkfeld der Antenne erreicht die höchste Intensität in einer Ebene, die im rechten Winkel zur Antennenachse verläuft (vgl. Abbildung 1-6). Oberhalb und unterhalb des "vertikalen Öffnungswinkels" von dieser Ebene nimmt die Feldstärke rasch ab, und senkrecht über und unter der Antenne ist schließlich meist kein nennenswertes Signal mehr zu erwarten.

Das Funkfeld ist hierbei radialsymmetrisch, das heißt, bei Draufsicht entlang der Antennenachse ist das Feld in allen Richtungen gleichstark ausgeprägt. Der "horizontale Öffnungswinkel" beträgt in diesem Fall 360°.

Abbildung 1-6

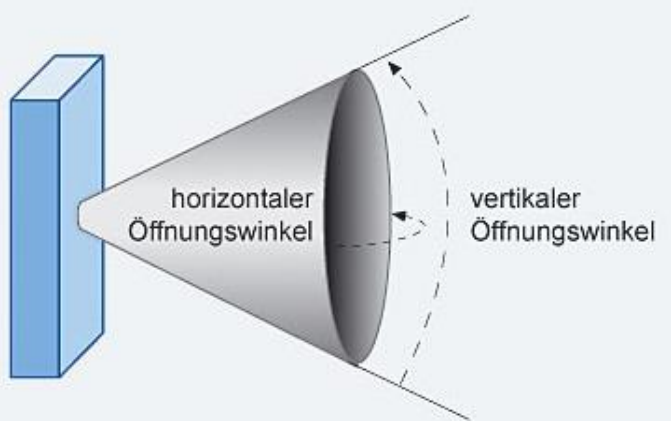


Richtantennen

Richtantennen, die typischerweise die Form eines flachen Kastens besitzen, erzeugen ein Funkfeld in Gestalt eines Kegels oder einer Keule, die senkrecht zu dem Kasten steht.

Der Kegel ist durch einen horizontalen und einen vertikalen Öffnungswinkel definiert, außerhalb dessen die Feldintensität rasch abfällt.

Abbildung 1-7



In der Richtung maximaler Feldstärke ist die Reichweite einer Richtantenne typischerweise zehnmal so groß wie die einer omnidirektionalen Antenne.

Antennen für SCALANCE W-Geräte

Im Kapitel 9.3 findet sich eine Übersicht über Antennen, die für den Betrieb mit SCALANCE W-Geräten geeignet sind.

Leckwellenleiter

Alternativen zu konventionellen Antennen sind die Leckwellenleiter, bei denen das entstehende Funkfeld auf die unmittelbare Umgebung des Leiters begrenzt ist.

Das Einsatzgebiet für derartige Leckwellenleiter sind bewegte Teilnehmer, die sich entlang festgelegter Bahnen bewegen (z. B. Einschienenhängebahnen, fahrerlose Transportsysteme), sowie Tunnel und ähnliche, mit Verkabelung schwer zu erfassende Bereiche.

Ein Beispiel für einen Leckwellenleiter ist die RCoax-Leitung aus Kapitel 9.1.

1.5.3 Fresnel-Zone

Wie im vorangehenden Kapitel erläutert, kann durch Hindernisse und Gegenstände die Ausbreitung der Funkwellen und somit die erzielbare Reichweite beeinflusst werden.

Um die mögliche Reichweite bestimmen zu können, wurde die Fresnel-Zone definiert. Die Fresnel-Zone beschreibt bestimmte räumliche Bereiche zwischen Sender- und Empfangsantenne und charakterisiert damit die Signalausbreitung. Für eine Kalkulation der Freiraumdämpfung wird hier gefordert, dass

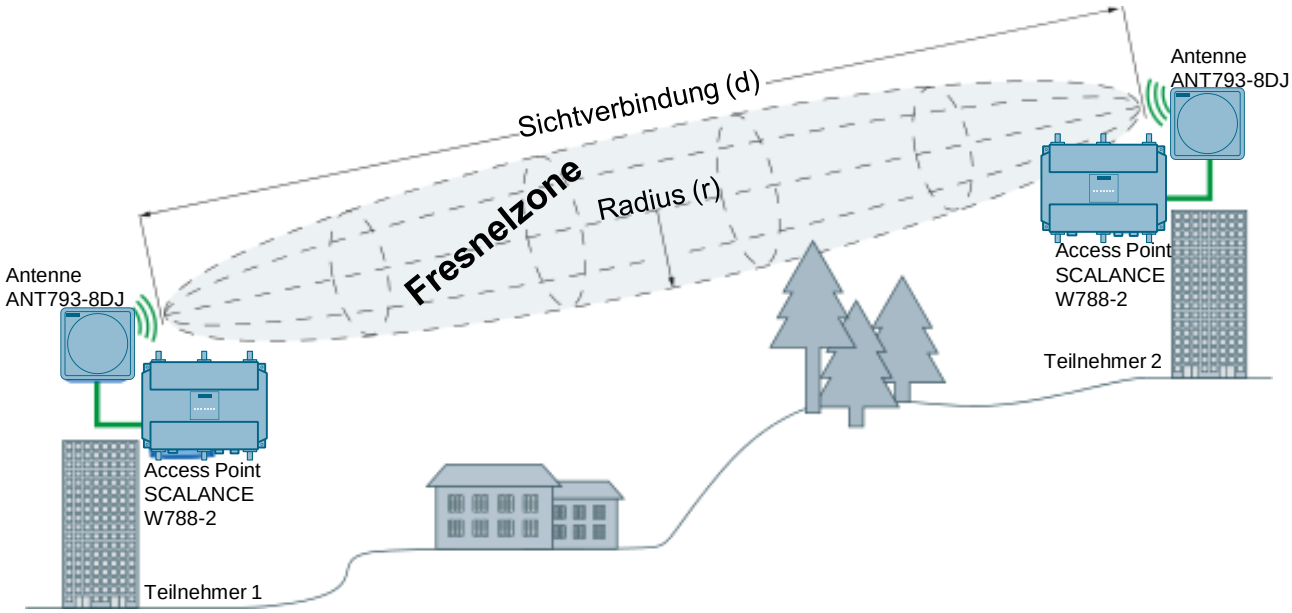
1. zwischen der Übertragungsstrecke von Sender und Empfänger eine direkte Sichtverbindung besteht und
2. um diese Sichtverbindung ein weiterer Bereich existiert, der ebenfalls frei von Hindernissen sein muss.

Sie ist in mehrere Ordnungen unterteilt. Die erste Ordnung[6] ist die bedeutendste, da in dieser der Hauptteil der Signalenergie übertragen wird.

Die oben genannten Bedingungen für die Anwendung der Freiraumdämpfung sind erfüllt, wenn die erste Fresnel-Ordnung hindernisfrei ist.

Die Fresnel-Zone gleicht in der Form einem Ovoid und ist abhängig von der Frequenz der Funkwellen und der Entfernung zwischen Sender und Empfänger. Mit steigender Frequenz wird der Durchmesser dieser Zonen kleiner und mit größer werdender Entfernung zwischen Sende- und Empfangsstation wird er größer.

Abbildung 1-8



[6] Die erste Fresnel-Zone ist der Ort, wo die Abstandssumme beider Antennen um λ/2 größer ist als die Sichtverbindung d (λ entspricht der Wellenlänge der Frequenz).

1.6 Modulations- und Multiplexverfahren

Um mittels einer Schwingung ein Signal zu übertragen, muss das Signal auf eine Trägerwelle „aufmoduliert“ werden. Die „Summe“ aus Trägerwelle und Signal wird zum Empfänger übertragen, der die Trägerwelle von der empfangenen Schwingung „abzieht“ und so wieder das reine Signal erhält.

Bei analogen Radioübertragungen kann sich z. B. die Amplitude der Trägerwelle oder deren Frequenz in Abhängigkeit vom Signal ändern. Bei Mittelwelle-Sendern wird die erstere Methode, bei UKW die Letztere verwendet, weswegen diese Bänder im angloamerikanischen Sprachraum als „AM“ („Amplitude Modulation“) bzw. „FM“ („Frequency Modulation“) bezeichnet werden.

Zur Übertragung digitaler Daten dienen komplexere Verfahren wie das Modulationsverfahren „Orthogonal Frequency Division Multiplexing“ (OFDM) und „Direct Sequence Spread Spectrum” (DSSS) (siehe Kapitel 2.2).

1.7 Anforderungen an Funkkommunikation im industriellen Umfeld

Industrielle Netzwerke unterscheiden sich in ihren Anforderungen in einigen Punkten von Netzen in der Office- oder Heim-Umgebung.

Datenvolumen

In Büroumfeld werden typischerweise Dateien mit mehreren Megabyte Umfang bewegt, bei der industriellen Anwendung sind die Datenpakete in vielen Fällen wesentlich kleiner.

Übertragungsgeschwindigkeit und Latenz

Bei der Kommunikation zwischen Bürogeräten ist eine zeitliche Verzögerung z. B. zwischen dem Senden eines Druckauftrags und seiner Ausführung in aller Regel unproblematisch. Im industriellen Umfeld müssen Messwerte und Steuerbefehle (wie z. B. ein Not-Aus) jedoch häufig im Millisekundenbereich ausgetauscht werden.

Fehlersicherheit und Zuverlässigkeit

Der Verlust oder die Verfälschung von Daten bei der Übertragung im Büroumfeld ist in der Regel nicht kritisch, da die Übertragung immer wiederholt werden kann. Bei Industrieanlagen sind die Verzögerungen durch ausgefallene Übertragungen und deren Wiederholung aber oft nicht akzeptabel.

Zusätzliche Störungen im industriellen Bereich

Der Office- und Heimbereich ist im Allgemeinen durch ein geringes Maß an Störungen von Gegenständen, die nicht zum Funknetz gehören, gekennzeichnet. Das industrielle Umfeld weist jedoch naturgemäß zahlreiche, teilweise sehr intensive Störquellen auf, die für die Ausbreitung elektromagnetischer Wellen ungünstig sind. Denn fast überall sind Metallteile oder andere Signalquellen wie RFID zu finden, die die Übertragung stören oder unterbrechen können.
Die Metallflächen z. B. reflektieren Funkwellen, was zu Paketverlusten oder sogar zur Auslöschung des Funksignals führen kann.

2 Der WLAN-Standard IEEE 802.11

2.1 Die Netzwerk-Standards der IEEE 802-Serie

Das *Institute of Electrical and Electronics Engineers* IEEE[7] hat es sich zur Aufgabe gemacht, elektronische und elektrotechnische Standards zu entwickeln, zu publizieren und zu fördern.

Unter der Projektnummer „802“ sind dabei eine Reihe von Arbeitsgruppen mit der Entwicklung von Standards für die Anlage und den Betrieb von Netzwerken beauftragt worden. Die Gruppe „802.3“ ist zum Beispiel mit den Standards für Ethernet-Verbindungen befasst.

Von der Arbeitsgruppe „802.11“ sind nun Spezifikationen für Wireless LANs erarbeitet worden. Diese Spezifikationen sind heutzutage der De-facto-Standard für Funknetze, mit den wichtigsten Varianten „802.11a/b/g/h/n“.

Das IEEE entwickelt die Standards kontinuierlich weiter, um sie neuen Anforderungen und technischen Gegebenheiten anzupassen.

Die folgende Tabelle gibt einen Überblick über die Themen einiger IEEE 802-Standards mit Bezug zu IWLANs.

Tabelle 2-1

Standard	Definitionsbereich
802.11a	Kommunikation
802.11ac	Kommunikation
802.11ad	Kommunikation
802.11b	Kommunikation
802.11e	Quality of Service (siehe Kapitel 2.3.1)
802.11g	Kommunikation
802.11h	Kommunikation (Störungsreduktion)
802.11i	Datensicherheit (siehe Kapitel 5.2.1)
802.11n	Kommunikation
802.1Q	Virtual LANs (siehe Kapitel 4.5.1)
802.1X	Datensicherheit (siehe Kapitel 5.2.1)

[7] Siehe hierzu auch http://www.ieee.org/portal/site,

2.2 Kommunikationsstandards des IEEE 802.11

Der ursprüngliche 802.11-Standard[8] (heute der Klarheit wegen oft als „*802.11 legacy*“ bezeichnet) definierte die Verbindung der Netzwerkteilnehmer über Funk im Frequenzband bei 2,4 GHz.

Die Brutto-Datenrate betrug bis zu 2 Mbit/s; der tatsächlich erreichte Netto-Durchsatz lag jedoch deutlich darunter.

Verbesserungen des Standards bestanden in den Erweiterungen „b“, „a“, „g“, „h“ und „n“, die in dieser Reihenfolge auf den Markt gebracht wurden.

Die verschiedenen Standards unterscheiden sich hinsichtlich der verwendeten Frequenzbänder (2,4 GHz und 5 GHz), der gleichzeitig nutzbaren Kanäle und der maximalen Datenrate.

Steigerungen der Übertragungskapazitäten wurden hier durch komplexere und leistungsfähigere Modulationsverfahren erzielt.

Im Laufe der Zeit wurden noch andere Standards definiert, die jeweils bestimmte Aspekte des Betriebs drahtloser Funknetze behandelten.

Die folgende Tabelle listet die technischen Eigenschaften der aktuell gängigen 801.11-Standards auf.

Tabelle 2-2

	802.11a/h	**802.11b**	**802.11g**	**802.11n**	**802.11 ac**	**802.11 ad**
Frequenzband	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz und 5 GHz	5 GHz	60 GHz
Max. Brutto-Datenrate	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	7 Gbit/s	7 Gbit/s
Modulations- / Multiplexverfahren*)	OFDM	DSSS	OFDM	MIMO und OFDM	MIMO und OFDM	

*) zu den einzelnen Modulationsverfahren, siehe Kapitel 1.6

Ist die Verbindungsqualität nicht gut genug, um die maximale Datenrate aufrechtzuerhalten, so wird die Übertragungsgeschwindigkeit schrittweise reduziert, bis wieder eine stabile Verbindung erreicht ist.

Prinzipiell kann ein 802.11a -Gerät nicht mit einem 802.11b/g-Gerät kommunizieren, da sie in verschiedenen Frequenzbändern senden. Die „b“-,“n“- und „g“-Versionen der Standards sind jedoch zueinander kompatibel.

[8] Siehe hierzu auch http://grouper.ieee.org/groups/802/11/, http://standards.ieee.org/wireless/overview.html#802.11

2.2.1 IEEE 802.11a

Beschreibung

Der IEEE 802.11a-Standard wurde im Jahr 1999 verabschiedet. Er nutzt das 5-GHz-Frequenzband und verwendet das Orthogonal Frequency Division Multiplexing (OFDM) Modulationsverfahren und die SISO-Technologie. Damit kann eine maximale Bruttodatenrate von 54 Mbit/s erreicht werden.

Dieses Frequenzband wird vor allem vom Militär für Radar im Flug- und Schiffsverkehr genutzt. WLAN ist hier eher zweitrangiger Nutzer.

Um Interferenzen zwischen WLAN und dem Radar zu verhindern, muss in manchen Ländern das Transmit Power Control und Dynamic Frequency Selection (siehe Kapitel 2.3.2) mit implementiert werden. Zu diesem Zweck wurde der Standard IEEE 802.11h als Erweiterung zum IEEE 802.11a entwickelt.

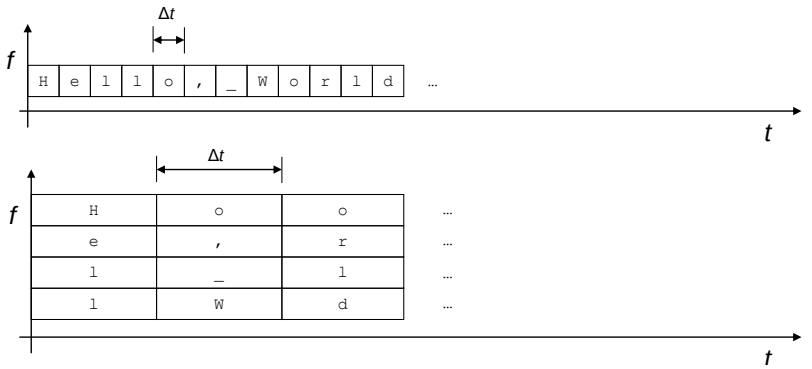
Modulationsverfahren „Orthogonal Frequency Division Multiplexing (OFDM)

OFDM verwendet nicht eine Frequenz, um sein Signal zu übertragen, sondern sendet auf mehreren hundert bis mehreren tausend nahe beieinander liegenden Kanälen, von denen jedem Einzelnen aber nur ein schmales Frequenzband zur Verfügung steht.

Durch die massiv parallele Datenübertragung wird die Datenrate, die über jeden *einzelnen* Kanal geht, drastisch reduziert d. h. es steht viel mehr Zeit zur Verfügung, die einzelnen Bits zu übertragen. Infolge dessen sind OFDM-Verbindungen deutlich weniger anfällig für kurzfristiges Rauschen oder auftauchende Echos. Selbst bei beträchtlichen Laufwegsunterschieden ist die Wahrscheinlichkeit groß, dass ein eintreffendes Echo noch zu demselben Bit gehört wie dasjenige, das gerade über den „direkten Weg“ übertragen wird.[9] Durch die reduzierte Übertragungsgeschwindigkeit wird außerdem erreicht, dass kurzfristige Rausch-Peaks meist weniger lang dauern als die Übertragung eines Bits.

Die folgende Abbildung zeigt die schematische Funktionsweise von OFDM (unten) im Gegensatz zu konventioneller Übertragung (oben): Die Verwendung etlicher paralleler Kanäle (hier sind der Übersichtlichkeit halber nur 4 Kanäle dargestellt; in der Praxis ist die Zahl wesentlich höher) erhöht die Zeitspanne Δ*t*, die für die Übertragung eines einzelnen Zeichens zur Verfügung steht, erheblich, sodass kurzes Rauschen oder Echos durch Laufwegsunterschiede deutlich weniger ins Gewicht fallen.

Abbildung 2-1



In der vorigen Darstellung wird oben die „konventionelle“ Sendeweise, unten die Übertragung mit OFDM dargestellt. Es ist deutlich zu sehen, wie die Übertragungs-

[9] Mit anderen Worten: Der Laufzeitunterschied bleibt noch geringer als die Dauer der Übertragung eines Bits.

zeit Δ*t* für ein einzelnes Zeichen gesteigert wird, ohne die Gesamt-Datenrate der Übertragung zu kompromittieren.

OFDM wird in einer Vielzahl von Übertragungsverfahren verwendet, z. B. bei ADSL, DAB (Digital Audio Broadcasting) oder DRM (Digital Radio Mondiale).

2.2.2 IEEE 802.11b

Beschreibung

Ebenso im Jahr 1999 entstand der IEEE 802.11b-Standard und arbeitet im 2,4-GHz-Frequenzband. Als Modulationsverfahren kommt hier das Direct Sequence Spreading Spectrum (DSSS) in Verbindung mit der Single Input Single Output (SISO)-Technologie zum Einsatz. Dadurch ist eine maximale Datenrate von 11 Mbit/s möglich.

Modulationsverfahren „Direct Sequence Spread Spectrum (DSSS

Eine Alternative zu OFDM stellt DSSS dar, das auf den ersten Blick den umgekehrten Weg geht: Der Datenstrom, der übertragen werden soll, wird mit einer Folge von Pseudo-Zufallszahlen (sog. „Chips“) multipliziert, die eine größere Datenrate als der Datenstrom hat.

Der Empfänger, der die „Chips“ kennen muss (diese können entweder durch einen Schlüsselalgorithmus generiert oder vorher separat übermittelt worden sein), subtrahiert diese einfach vom empfangenen Strom und erhält das unverfälschte Signal zurück.[10]

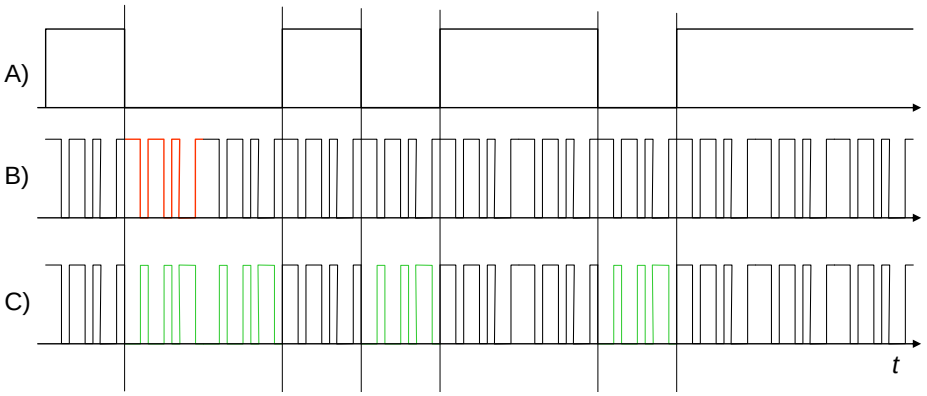
Das hat mehrere Effekte zur Folge:

- Obwohl nur eine Trägerwelle verwendet wird, verbreitert sich das Spektrum des übertragenen Signals überproportional. Störungen, die auf einen sehr engen Bereich des Spektrums begrenzt sind, wirken sich dadurch weniger stark aus.
- Die Verwendung von Pseudo-Zufallszahlen führt dazu, dass das übertragene Signal auf den ersten Blick wie Rauschen aussieht. Mit anderen Worten, für einen Mithörer ist nicht ersichtlich, dass überhaupt eine Übertragung stattfindet.
- Selbst wenn ein Mithörer weiß, dass eine Übertragung läuft, kann er diese nur dann mithören, wenn er weiß, welche Sequenz von Chips der Sender verwendet hat.

DSSS findet außer bei WLANs beispielsweise auch Anwendung bei GPS, UMTS und WirelessUSB.

[10] Dies ist natürlich eine vereinfachte Darstellung, und streng genommen handelt es sich um keine Additionen oder Subtraktionen, sondern um XOR-Verknüpfungen der Daten mit ihren Schlüsseln.

Abbildung 2-2



Die Illustration oben verdeutlicht die Funktion von DSSS.

A) Das Nutzdatensignal,

B) Die „Chips“, die zur Verschlüsselung verwendet werden. Hierbei handelt es sich nur um eine kurze Sequenz (rot dargestellt), die ständig wiederholt wird. Die Bitfolge ändert sich bei den „Chips“ sehr viel schneller als bei den Nutzdaten.

C) Das verschlüsselte Signal ist identisch zu den Chips, solange das Nutzdatensignal „1“ ist (schwarze Abschnitte); sonst entsteht es durch Invertierung der Chips (grün).

In der Praxis wären die Chips komplizierter, und man würde keine Bitlänge für die Nutzdaten verwenden, die ein Vielfaches der Chiplänge beträgt.

2.2.3 IEEE 802.11g

Beschreibung

Dieser Standard ist die Erweiterung von IEEE 802.11b und arbeitet ebenso im 2,4-GHz-Frequenzband. IEEE 802.11g arbeitet mit dem OFDM-Modulationsverfahren und der SISO-Technologie und kann somit eine maximale Datenrate von 54 Mbit/s erzielen. Dieser Standard ist abwärtskompatibel zu IEEE 802.11b. Werden in einem Netz beide Standards verwendet, kommt das Modulationsverfahren DSSS mit der entsprechend niedrigeren Datenübertragungsrate zum Einsatz.

Modulationsverfahren OFDM

Siehe Kapitel 2.2.1

2.2.4 IEEE 802.11n

Beschreibung

Das IEEE 802.11n ist der neueste Standard und kann sowohl das 2,4 GHz, als auch das 5-GHz-Band nutzen. Zusätzlich zum Modulationsverfahren OFDM wird die Multiple Input Multiple Output (MIMO)-Technologie eingesetzt. Dadurch wird die Übertragungsgeschwindigkeit im Vergleich zu den zuvor erwähnten Standards erheblich erhöht und kann bis zu 600 Mbit/s betragen.

WLANs nach 802.11n sind zu 802.11a-, 802.11b-, 802.11g- und 802.11h-Netzen kompatibel.

Modulationsverfahren OFDM

Siehe Kapitel 2.2.1

Diversity-Systeme

Diversität ist eine Technologie zur Erhöhung der Übertragungssicherheit in einem Funksystem. Das Prinzip besteht darin, die Informationen in einem Funkkanal mehrfach (redundant) zu senden bzw. zu empfangen. Basis aller Diversity-Systeme ist demnach, die Signale über mehrere parallele und voneinander unabhängige Wege zu übertragen. Die Trennung kann zeitlich, über die Frequenz oder räumlich erfolgen.

In heutigen Funksystemen wird vor allem die räumliche Trennung verwendet.

Die Raum-Diversity zeichnet sich dadurch aus, dass sie ohne zusätzliche Ressourcen wie Übertragungszeit und -bandbreite umsetzbar ist. Es werden hier die räumlichen Unterschiede im Kanal ausgenutzt. Dafür werden mehrere Antennen entweder am Sender (MISO; Multiple Input Single Output) oder am Empfänger (SIMO; Single Input Multiple Output) verwendet.

Welche Information von welcher Antenne ausgewertet wird, wird durch Testmessungen entschieden, die während des Verbindungsaufbaus durchgeführt werden. Die Antenne, welche die Daten mit dem besseren Signal-Rausch-Abstand empfängt, wird für die weitere Datenübertragung genutzt. Das Signal der anderen Antenne wird ignoriert. Konkret verwendet werden also nur die Daten eines Übertragungsweges.

Multiple Input / Multiple Output- Systeme

Um die Empfangsfeldstärke und damit die Empfangsqualität und die übertragbare Datenrate zu erhöhen, wird die MIMO-Technologie eingesetzt. Diese Technik wird in der IEEE 802.11n-Erweiterung genutzt.

Ein MIMO-System unterscheidet sich dadurch von den Diversity-Systemen, dass hier nicht nur ein Kanal zur redundanten Signalübertragung verwendet wird, sondern mehrere parallele Subkanäle. Diese zusätzlichen Datenkanäle ermöglichen es, unabhängig voneinander im selben Frequenzband, gleichzeitig und mit denselben Antennen unterschiedliche Daten zu übertragen, sogenanntes Multiplexing („spatial multiplexing“).
Die Technologie fordert, dass sowohl Sender als auch Empfänger jeweils mit wenigstens zwei und maximal vier Antennen ausgestattet sind.

Durch Beamforming am Sender und am Empfänger ist es möglich, störende Überlagerungen (Interferenzen) im Kanal auszublenden und so eine sichere und qualitativ hochwertige Verbindung herzustellen.

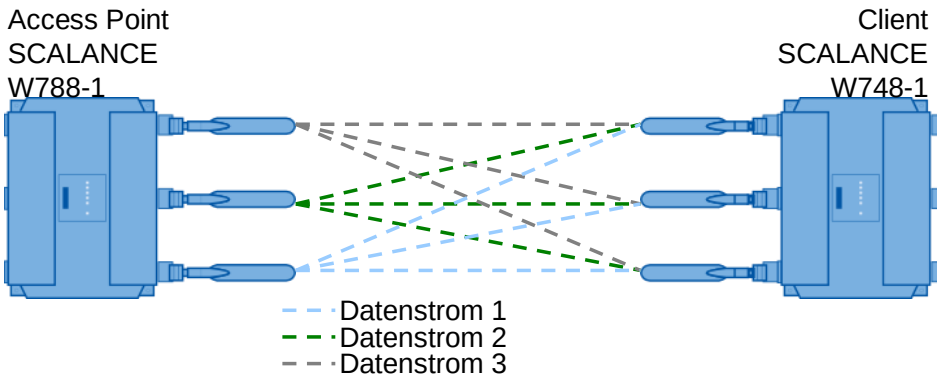
Das Prinzip besteht darin, die Signale der einzelnen Antennenelemente über einstellbare Phasenschieber und Verstärkungsfaktoren zu kombinieren. Hierdurch

entsteht eine Richtwirkung („Beamforming“), die elektronisch durch sogenannte intelligente Antenne (smarte Antennen) eingestellt werden kann.

Durch diese MIMO-Methode lässt sich der Datendurchsatz stark erhöhen. Je Datenstrom werden bei IEEE 802.11n brutto maximal 150 Mbit/s transferiert. Bei Ausnutzung der maximal möglichen vier Datenkanäle ergeben sich so 600 Mbit/s.

Die folgende Grafik verdeutlicht die MIMO-Technologie bei Verwendung von drei Antennen und drei Datenströme:

Abbildung 2-3



Verkürztes Guard-Intervall

Das Guard-Intervall verhindert, dass sich verschiedene Übertragungen vermischen. Nach Ablauf der Sendezeit wird eine Sendepause (Guard Interval) zwischen zwei übermittelten OFDM-Symbolen eingelegt, bevor die nächste Übertragung beginnt.

Das Guard-Intervall von IEEE 802.11a/b/g beträgt 800 ns. IEEE 802.11n kann das verkürzte Guard-Intervall von 400 ns benutzen.

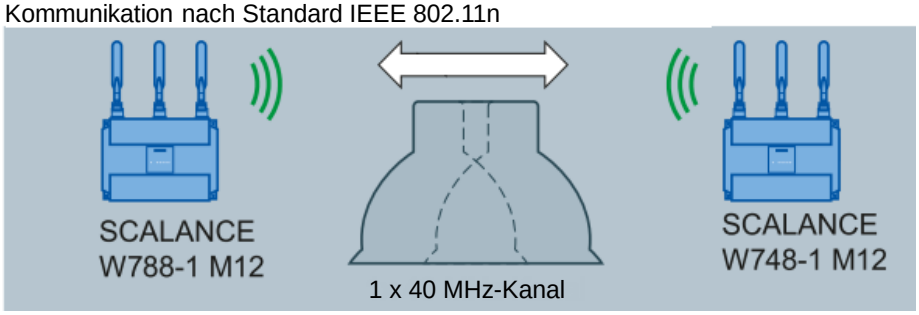
Channel Bonding

Channel Bonding („Kanalbündelung“) bedeutet die Zusammenfassung mehrerer Kanäle, um einen höheren Datendurchsatz zu erzielen.

Bei IEEE 802.11n können Daten über zwei direkt benachbarte Kanäle übertragen werden. Die beiden 20 MHz-Kanäle werden zu einem Kanal mit 40 MHz zusammengefasst. Dadurch lässt sich die Kanalbandbreite verdoppeln und der Datendurchsatz steigern. Um die Kanalbündelung zu nutzen, muss der Empfänger 40 MHz-Übertragungen unterstützen. Wenn nicht, wird automatisch auf 20 MHz reduziert. Das garantiert die Kompatibilität zwischen IEEE 802.11n- und IEEE 802.11a/b/g-Geräten.

Abbildung 2-4

Kommunikation nach Standard IEEE 802.11n



Maximale Datenrate: 450 Mbit/s

Frame Aggregation

Bei IEEE 802.11n ist es möglich, Einzel-Datenpakete zu einem größeren Datenpaket zusammen zufassen (Frame Aggregation).
Durch dieses Verfahren wird der Paket-Overhead minimiert, die Wartezeit zwischen den Datenpaketen verkürzt und somit der Durchsatz gesteigert.
Es gibt zwei Arten der Frame Aggregation:

- Aggregated MAC Protocol Data Unit (A-MPDU) und
- Aggregated MAC Service Data Unit (A-MSDU).

Die Frame Aggregation kann nur benutzt werden, wenn die Einzel-Datenpakete für dieselbe Empfänger-Station (Client) vorgesehen sind.

MCS ("Modulation and Coding Schemes")

Der Standard IEEE 802.11n unterstützt unterschiedliche Datenraten.
Die Datenraten basieren auf der Anzahl der Sender- und Empfangsströme (Spatial Streams), dem Modulationsverfahren und der Kanalkodierung. Die verschiedenen Kombinationen werden im „Modulation and Coding Shemes" beschrieben.

Auf der Web Based Management-Seite der SCALANCE W-Geräte (IEEE 802.11n) werden die verfügbaren Datenübertragungsgeschwindigkeiten für den WLAN-Modus 802.11n anzeigt. Diese können beliebig kombiniert und ausgewählt werden. Ausschließlich die gewählten Datenübertragungsgeschwindigkeiten werden dann vom Access Point zur Kommunikation mit den Clients verwendet.

2.2.5 IEEE 802.11ac

Beschreibung

IEEE 802.11ac ist ein im November 2013 verabschiedeter Funknetz-Standard für ein WLAN mit Datenraten im Gigabit-Bereich. Durch die Verbesserung des Übertragungsprotokolls und der WLAN-Technik sowie Nutzung des Modulationsverfahrens OFDM sind Datenraten bis zu 7 Gbit/s möglich. Die Datenübertragung erfolgt ausschließlich im 5-GHz-Band.

WLANs nach 802.11ac sind zu 802.11a-, 802.11h- und 802.11n-Netzen kompatibel.

Technisch gesehen bringt dieser Standard keine wesentlichen Neuerungen als der Vorgänger IEEE 802.11n. Die höhere Übertragungsrate wird vor allem durch breitere Kanäle (bis 160 MHz), bis zu acht gleichzeitig nutzbare Sende- und Empfangseinheiten, eine hochwertige Modulation sowie eine Multi-User-MIMO erzielt.

Modulationsverfahren OFDM

Siehe Kapitel 2.2.1

2.2.6 IEEE 802.11ad

Seit dem Jahr 2012 liegt ein neuer Standard für Wireless Gigabit vor. Es handelt sich hierbei um eine Spezifikation nach IEEE 802.11ad für eine drahtlose Verbindung zwischen digitalen Videosystemen im Gigabit-Bereich. Die hohen Datenraten werden durch den Frequenzbereich-Wechsel auf das 60-GHz-Band und der Optimierung des Zugriffsprotokolls erreicht.

WLANs nach 802.11ad verlieren durch den Frequenzband-Wechsel die Abwärtskompatibilität zu den anderen IEEE 802.11-Standards.

2.2.7 Reichweite und besondere Antennen

Die verwendeten Antennen erreichen innerhalb von Gebäuden Reichweiten von typischerweise 30 m. Da im Außenbereich Effekte wie Reflexionen und Abschattungen weniger zum Tragen kommen, sind dort Reichweiten bis 100 m und mehr erreichbar. Besonders vorteilhaft erweist sich eine Verbindung mit direkter Sicht ("line of sight"), weil sich dann die Funkwellen ungestört ausbreiten können.

Durch den Einsatz von Richtantennen kann dieser Wert auf viele 100 m gesteigert werden. Je nach Einsatzland, Sichtzone und der Fresnel-Zone (siehe Kapitel 1.5.3) können sogar Reichweiten über mehrere Kilometer überbrückt werden.

2.3 Weitere IEEE 802.1x-Standards

Im Laufe der Zeit wurden für IEE 802.11 eine Reihe weiterer Standards definiert, die meist einzelne Aspekte der Funkkommunikation betrafen:

- 802.11e: Einführung von „Quality of Service“-Features zur Erhöhung der Übertragungsqualität.
- 802.11h: Anpassungen an 802.11a, um Störungen mit anderen Geräten im 5-GHz-Band zu vermeiden.
- 802.11i: Sicherheitsfunktionen zur Datenverschlüsselung und Authentifizierung.

Daneben existieren noch IEEE 802.1-Standards, die für den Betrieb von WLANs eine Rolle spielen:

- 802.1Q: Virtual LANs zur Separierung eines Netzwerks
- 802.1X: Sicherheitsfunktionen für WLANs und VLANs

2.3.1 IEEE 802.11e und WMM: „Quality of Service “

IEEE 802.11e

Im Winter 2005/2006 wurde von der IEEE der Standard 802.11e verabschiedet. Dieser ergänzt die bestehenden Netzwerkstandards um „Quality of Service“-Kriterien, d. h., bei Erfüllung dieses Standards ist eine bestimmte Verbindungsqualität garantiert.

Die Qualität wird dabei nicht nur an der mittleren erzielbaren Datenrate gemessen, sondern es werden auch Untergrenzen für Verbindungszuverlässigkeit, die Dauer möglicher Verbindungsunterbrechungen etc. definiert. Für eine angenehme Telefonverbindung ist es z. B. nicht nur notwendig, eine angemessene Tonqualität zu übertragen, sondern Aussetzer und Sprachverzögerungen dürfen sich ebenfalls nur in engen Grenzen bewegen.

Während frühere 802.11-Standards auf die „Quality of Service“ weniger Rücksicht nahmen als auf Bruttodatenraten, ist mit der Variante „e“ ein Standard ins Leben gerufen worden, der die Belange des QoS ausdrücklich mit aufnimmt.

WMM

„WMM“ („Wireless Multimedia Extensions“) sind ein Subset des 802.11e-Standards, das von der „WiFi-Alliance“ definiert wurde, um Multimediadienste ausdrücklich in die Netzwerke zu integrieren.

2.3.2 IEEE 802.11h und das 5-GHz-Band

IEEE 802.11h

Zwar wird das 5-GHz-Band außer für WLAN nur für wenige andere Anwendungen genutzt, bei einer dieser Anwendungen handelt es sich jedoch um Radar, dessen Betreiber möglichen Störungen natürlich sehr empfindlich gegenüberstehen.

Aus diesem Grund wurden mit dem IEEE 802.11h-Standard Modifikationen eingeführt, mit deren Hilfe Interferenzen zwischen einem unter 5 GHz betriebenen WLAN und Radar minimiert werden. Zu den neu eingeführten Technologien zählen „DFS“ und „TPC“.

DFS (Dynamic Frequency Selection)

DFS beschreibt das automatische Ausweichen auf einen anderen Kanal, wenn auf dem aktuellen WLAN-Kanal Störungen entdeckt werden, die von einem Radar-Gerät stammen.

TPC (Transmit Power Control)

Mit TPC wird die Sendeleistung der Teilnehmer solange reduziert, bis das Minimum für eine zuverlässige Übertragung mit der projektierten Datenrate erreicht ist. TPC stellt so einen Kompromiss zwischen sicherer Kommunikation und der Vermeidung von Überreichweiten dar.

2.4 Kanalverteilung im IEEE 802.11-Standard

Der 802.11-Standard benutzt als Frequenzkanäle die ISM-Bänder 2,4 GHz und 5 GHz.

2.4.1 Das 2,4-GHz-Band

Das Frequenzband bei 2,4 GHz ist ein in praktisch allen Nationen lizenzfrei zu nutzender Frequenzabschnitt.[11] Da Sender und Empfänger relativ günstig herzustellen sind, ist die 2,4-GHz-Technologie sehr beliebt und wird nicht nur für WLAN, sondern auch durch eine Vielzahl anderer Anwendungen belegt.

Das 2,4-GHz-Band, wie es im Standard 802.11b/g benutzt wird, wird in der Regel in 13 Kanäle unterteilt,[12] die jeweils einen Abstand von 5 MHz voneinander haben und eine Bandbreite von ca. 20 MHz (siehe Kapitel 1.4.4). Das bedeutet aber keinesfalls, dass 13 nicht überlappende Kanäle für jedes WLAN zur Verfügung stehen.

Um also auszuschließen, dass die Sender im WLAN einander stören, müssen sie mindestens diesen Abstand voneinander halten. Das reduziert die Zahl unabhängig voneinander verwendbarer Frequenzen in der Praxis auf drei: Üblicherweise werden bei 802.11-Netzwerken nur die Kanäle 1, 7 und 13 (die sog. „überlappungsfreien Kanäle“) gleichzeitig verwendet.

Mit dem Standard 802.11n ist eine Erweiterung der Bandbreite auf 40 MHz pro Kanal möglich (Channel Bonding; siehe Kapitel 2.2.4). Dadurch werden höhere Datenraten erreicht.

[11] Aktualisierte Listen mit Länderzulassungen für die einzelnen SCALANCE W-Produkte finden Sie unter http://www.siemens.de/funkzulassungen.
[12] Die Details der zugelassenen Kanäle sind von Land zu Land unterschiedlich. Das Thema wird in Kapitel 7 ausführlich behandelt.

Werden viele Access Points in einem Netz eingesetzt, so müssen auch viele voneinander unabhängige, d. h. nicht-überlappende Kanäle verwendet werden. In diesem Fall kann ein Ausweichen auf das 5-GHz-Band der 802.11a/h/n-Standards sinnvoll sein, welches eine größere Anzahl nicht-überlappender Kanäle bietet.

2.4.2 Das 5-GHz-Band

Für das 5-GHz-Band sind in den einzelnen Regionen der Welt unterschiedliche Anzahl an nicht überlappenden Kanälen zugelassen.[13]

Generell sind 5-GHz-Wellen „härter“, d. h. das Ausbreitungsverhalten ist ähnlicher dem von Lichtstrahlen: Die Beugung um Gegenstände herum ist geringer, die Absorption größer und die Eindringtiefe geringer als bei 2,4-GHz-Wellen. Generell ist darum die praktisch zu erzielende Reichweite geringfügig kleiner als im 2,4-GHz-Band.

Verglichen mit dem 2,4-GHz-Band ist das 5-GHz-Band deutlich weniger „belegt“, und es gibt nur wenige Störquellen in diesem Bereich. Eine Ausnahme sind militärische Radar sowie Satelliten- und Ortungssysteme, deren Betreiber naturgemäß empfindlich darauf reagieren, wenn ihre Anlagen durch ein WLAN gestört werden.

Um den Betrieb von 5-GHz-WLANs mit diesen Anlagen zu harmonisieren, wurde der IEEE-Standard 802.11h (siehe Kapitel 2.3.2) geschaffen.

[13] Vergleiche hierzu die Bemerkungen über die Länderzulassungen der Komponenten, siehe Kapitel 7.
Aktuelle Zulassungslisten finden sich im Internet unter http://www.siemens.de/funkzulassungen

2.4.3 Vergleich der Eigenschaften des 2,4-GHz- und des 5-GHz-Bandes

Verbindungssicherheit und Störung durch andere Geräte:

Die große Popularität des 2,4-GHz-Bandes führt auch dazu, dass eine Vielzahl von Geräten, die eigentlich mit WLANs nichts zu tun haben, ebenfalls in diesem Bereich senden – dazu zählen Mikrowellenherde ebenso wie Bluetooth-Geräte und schnurlose DECT-Telefone.
Dies kann zu Störungen und Problemen bei der Errichtung eines WLANs führen. Je nach Art der Störquellen kann unter Umständen ein Ausweichen auf das 5-GHz-Band sinnvoll sein.

In jedem Fall muss vor dem Aufbau einer Anlage durch eine Funkfeldanalyse abgeklärt werden, wie Ausleuchtung, Frequenzband und Antennen optimal konfiguriert werden.

Abmaße

Bedingt durch die geringere verwendete Wellenlänge lassen sich 5-GHz-Komponenten mit kleineren Abmaßen als 2,4-GHz-Baugruppen herstellen. (Dies gilt natürlich nicht für Geräte, die für den Betrieb in beiden Bändern („dual-use“) ausgelegt sind.)

Lizenzierung

Sowohl 2,4-GHz- als auch 5-GHz-Netze können in den meisten Staaten lizenzfrei betrieben werden. Im Kapitel 7 wird das Thema Länderzulassungen ausführlicher beschrieben.

3 Alternative Funktechnologien zu IWLAN

Neben dem IEEE 802.11-Standard für WLANs gibt es noch eine Reihe anderer Technologien, die mithilfe des Funknetzes kommunizieren und die im industriellen Umfeld Anwendung finden.

3.1 Bluetooth

„Bluetooth“ ist der Name für den IEEE 802.15.1-Standard, der die Vernetzung von Kleingeräten über kurze Distanzen beschreibt. Sein hauptsächliches Anwendungsgebiet ist der Ersatz von Kabelverbindungen zwischen Bürogeräten wie PDAs, Handys, Computern, Druckern und anderer Peripherie.

Bluetooth arbeitet im Frequenzbereich von 2,402 GHz bis 2,480 GHz im ISM-Band, kollidiert also mit dem von 802.11 verwendeten 2,4-GHz-Band.

Die maximale Sendeleistung beträgt 100 mW mit einer Reichweite von höchstens ca. 100 m (Die meisten portablen Geräte senden jedoch mit geringerer Leistung, um ihre Akkus zu schonen; typische Reichweiten liegen darum unter 10 m.). Dabei werden Daten mit einer Geschwindigkeit bis zu 24 Mbit/s übertragen.

Der Standard wird von der „Bluetooth Special Interest Group“ kontrolliert und weiter entwickelt.

Hinweis Weitere Informationen zu diesem Thema finden Sie auf dem Web unter der URL: https://www.bluetooth.org

3.2 Wireless HART

HART („Highway Addressable Remote Transducer) ist ein Feldbus-Kommunikationsstandard, der als „WirelessHART“ auch die drahtlose Kommunikation definiert (basierend auf IEEE-Standard 802.15.4).

WirelessHART benutzt ebenfalls das ISM- Frequenzband (2,4 GHz mit maximal 250 kbit/s) und baut selbsttätig vermaschte Netze auf, deren Ausdehnung deutlich größer als die nominelle Funkreichweite eines Einzelteilnehmers (ca. 200 m) sein kann. Das Netz organisiert sich selbst, indem alle Verbindungsinformationen von dem WirelessHART Gateway (IE/WSN-PA Link) ausgewertet werden, um mit diesen Informationen automatisch redundante Pfade zur Verfügung zu stellen. Damit kann eine sehr hohe Verfügbarkeit der Kommunikationsverbindung erreicht werden, da schlechte Verbindungen bzw. der Ausfall einzelner Knoten überbrückt werden können. Darüber hinaus kann die Verfügbarkeit des gesamten Netzwerkes über den Betrieb zweier redundanter Gateways signifikant erhöht werden.

Das Augenmerk bei der Entwicklung von WirelessHART lag außerdem auf der einfachen Inbetriebnahme und Wartung des selbstorganisierenden Netzes, sodass die Konfiguration nur minimalen Aufwand erfordert. Erkauft wird dies mit dem Verlust der Echtzeitfähigkeit; d. h., es werden unter WirelessHART keine Antwortzeiten garantiert.

Der Hauptanwendungsbereich von WirelessHART liegt hierbei in der regelmäßigen Übertragung geringer, nicht zeitkritischer Datenmengen in größeren Abständen (typischerweise zwischen ca. 15 Sekunden und mehreren Stunden) über relativ große Entfernungen (wie z. B. in der Prozessindustrie). Durch den geringen Energieverbrauch der WirelessHART Geräte können lange Batterielaufzeiten von fünf bis zehn Jahren erreicht werden, d. h. die WirelessHART- Feldgeräte erweisen sich als äußerst wartungsarm während der Betriebsphase.

Das Protokoll ist sehr robust und „heilt“ bei genügender Ausleuchtung des vermaschten Netzwerks den Ausfall von Zwischenstationen selbsttätig.

WirelessHART wird von der „HART Communication Foundation“ (HCF) verwaltet.

Hinweis

Weitere Informationen zu diesem Thema finden Sie auf dem Web unter den URLs:

http://www.siemens.de/wirelesshart

http://www.hartcomm.org/

3.3 Zigbee

Zigbee basiert wie WirelessHART auf dem IEEE-Standard 802.15.4 und benutzt ebenso das ISM-Band bei 2,4 GHz. Im Unterschied zu HART liegt der Fokus hier jedoch nicht auf dem industriellen Umfeld, sondern im Bereich der Gebäudeautomatisierung und Haustechnik. Ziel ist es, Geräte in schwer zugänglichen Bereichen zu installieren, die über Jahre ohne Wartung in Betrieb bleiben können (Strom- oder Heizungszähler, Lichtschalter, etc.).

Das Zigbee-Protokoll ist weniger „robust“ als das von WirelessHART, und bei Ausfall eines zentralen Controllers kann die Kommunikation des kompletten Netzes kompromittiert werden. Dafür bietet Zigbee geringere Reaktionszeiten und ist dadurch auch für Echtzeitanwendungen geeignet.

Der Zigbee-Standard steht unter der Kontrolle der Zigbee-Allianz, die auch weitere Informationen zu diesem Thema anbietet.

Hinweis

Weitere Informationen zu diesem Thema finden Sie auf dem Web unter der URL:
http://www.zigbee.org/

3.4 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) wurde in den IEEE-Standards der 802.16-Familie definiert und parallel zu IEEE 802.11 entwickelt. Diese Technik ermöglicht eine drahtlose Breitbandtechnik für ein Metropolitan Area Network (MAN) ohne aufwändige leitungsgebundene Infrastruktur. Durch die Nutzung eines sehr breiten Frequenzspektrums im Gigahertzbereich ist WiMAX auch weltweit einsetzbar.

Anders als die WLAN-Standards kann WiMAX größere Reichweiten überbrücken, sodass auch abgelegene und ländliche Regionen mit Breitband versorgt werden können. Durch diese Eigenschaft wird WiMAX als Alternative zum Festnetz-DSL gesehen.

Die theoretische Reichweite liegt bei 50 km mit einer Übertragungsgeschwindigkeit von bis zu 75 Mbit/s. In der Praxis liegen diese Werte aber deutlich darunter.

Hinweis

Weitere Informationen zu diesem Thema finden Sie auf dem Web unter der URL:
http://www.wimax.com/

4 Topologie, Konfiguration und Organisation von IWLANs

4.1 Der Aufbau eines WLANs

4.1.1 Strukturierung durch Zelleneinteilung

Unstrukturierte Funknetze und deren Nachteile

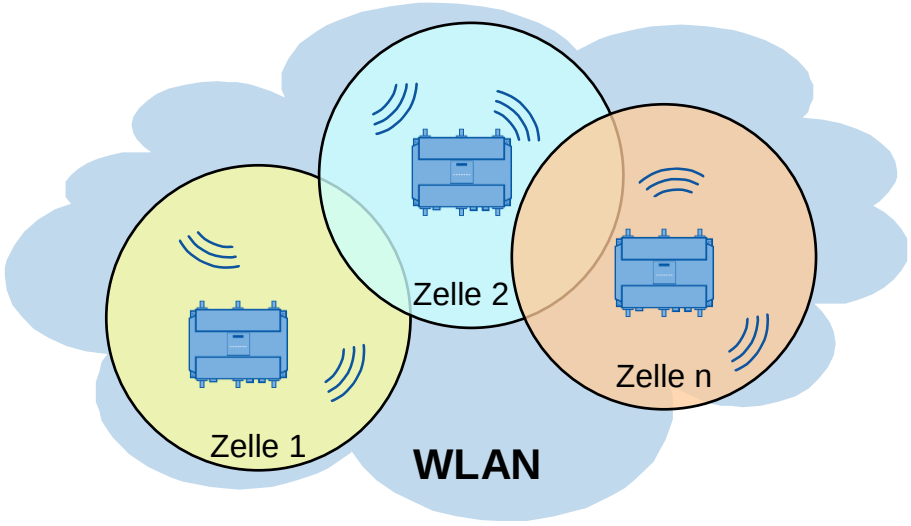
Wie in Abschnitt 1.4.3 gesehen, ist die Reichweite von Funksendern in der Praxis begrenzt. In aller Regel wird die Fläche, die durch ein LAN abgedeckt werden soll, zu groß sein, als dass sie von einem einzelnen Sender zuverlässig „ausgeleuchtet werden könnte.

Selbst wenn es technisch möglich wäre, die Sendeleistung hoch genug für alle Teilnehmer zu setzen, wäre das in vielen Fällen nicht erwünscht und nicht erlaubt. Wenn die LAN-Teilnehmer z. B. entlang einer geraden Linie angeordnet sind, würde in diesem Fall ein unnötig großes Areal zu beiden Seiten links und rechts der Linie beleuchtet, und es wäre für Dritte leicht, zusätzliche Empfänger zu installieren und den Funkverkehr unbemerkt mitzuhören.

Strukturierung von Funknetzen durch Funkzellen

Darüber hinaus ist es auch ökonomischer, das WLAN in einzelne Zellen zu unterteilen, denn zu jedem Zeitpunkt kann ja auf jedem Kanal immer nur ein Teilnehmer senden. Stehen mehrere Zellen zur Verfügung, kann sich in *jeder* Zelle ein aktiver Sender befinden, und der tatsächliche Datendurchsatz steigt an. Zudem ist durch die kurzen Distanzen nur eine vergleichsweise kleine Sendeleistung notwendig. Die folgende Abbildung zeigt die Unterteilung des WLANs in mehrere Zellen.

Abbildung 4-1



Hinweis Weitere Informationen zu diesem Thema finden Sie auf dem Web unter der URL: http://www.siemens.de/iwlan

4.1.2 Verbindung einzelner Funkzellen: „Access Points“ und „Clients“

Um die Kommunikation in einer Zelle zu steuern oder um mehrere Funkzellen miteinander zu verbinden, ist die Verwendung von „Access Points“ nötig. Diese nehmen innerhalb des WLANs eine vergleichbare Position wie Switches bei leitungsgebundenen Netzen ein.

Administrative Funktion von Access Points

Wenn es nur eine Funkzelle gibt, oder wenn die Kommunikation nur innerhalb einer Zelle stattfindet, kann der Access Point zur Koordination der Kommunikation innerhalb dieser Zelle eingesetzt werden.

Beim Einsatz von Verschlüsselungsverfahren kann er Clients den Zugang zum Netz ermöglichen oder verwehren (siehe Kapitel 5). Echtzeitanforderungen an die Kommunikation kann der Access Point erfüllen, indem er den Datenverkehr im Netz regelt und koordiniert und den einzelnen Clients regelmäßige „Zeitscheiben“ zuweist, innerhalb derer diese ungestört ihre Daten übertragen können (vgl. Abschnitt 4.4).

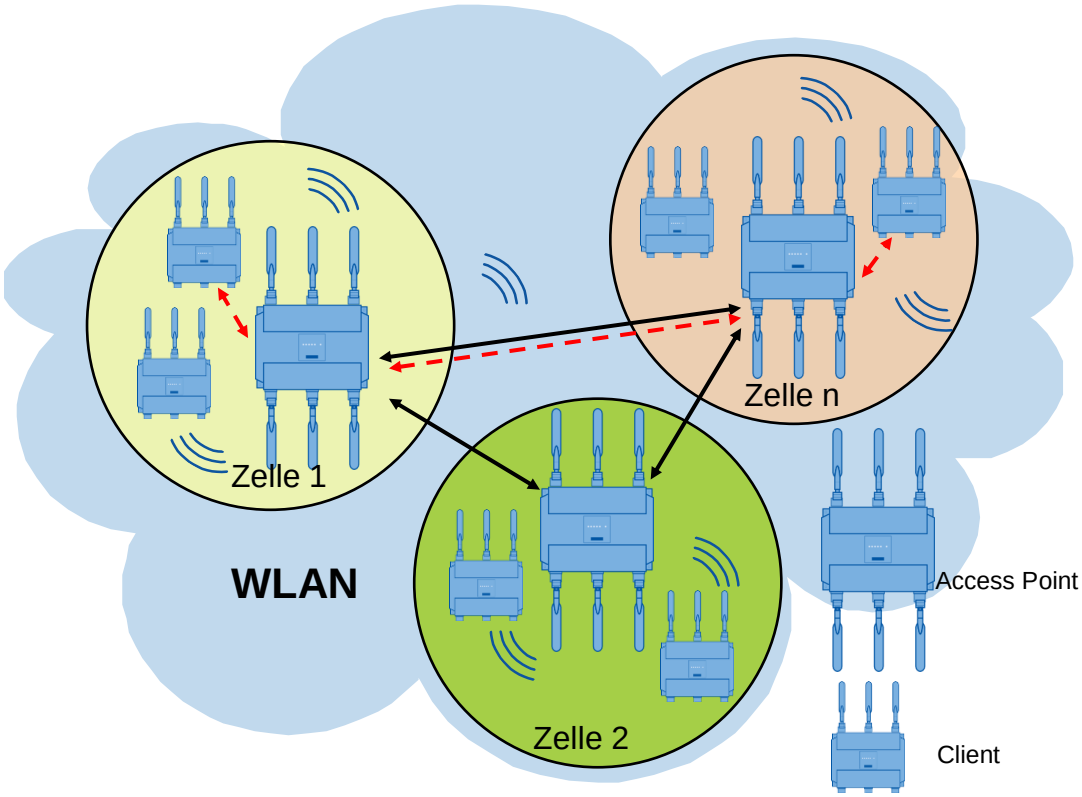
Access Points als „Backbone“ der Kommunikation

Bei einem WLAN, das aus mehreren Funkzellen besteht, kommuniziert jeder der Access Points mit allen regulären Teilnehmern seiner Zelle, den sog. „Clients“ – egal, ob diese nun stationär oder mobil sind. Zugleich halten die Access Points eines WLANs auch die Verbindung untereinander aufrecht. Dies geschieht entweder über Kabel oder mittels eines zweiten, unabhängigen Funknetzes.[14] Damit wird die Kommunikation über die Grenzen der Funkzellen hinweg ermöglicht.

Der Begriff „Backbone“ bezeichnet in diesem Fall den Zusammenschluss der verschiedenen Funkzellen bzw. Netzwerke.

[14] Dafür wird ein Access Point mit zwei oder mehr Funkinterfaces benötigt.

Abbildung 4-2



Die Illustration zeigt die Aufteilung eines WLANs in drei Funkzellen (gelb, rot, grün) mit einer Anzahl von Clients und jeweils einem Access Point. Die roten Pfeile verfolgen den Kommunikationspfad zwischen einem Client der gelben Zelle und einem Client der roten Zelle.

4.2 Das „Roaming“-Verfahren

Bewegung von Clients zwischen den Funkzellen: „Roaming“

Erstreckt sich ein WLAN über eine größere Fläche, reicht das Funkfeld eines Access Points (Funkzelle) in der Regel nicht aus. Um den gesamten Bereich funktechnisch auszuleuchten, sind mehrere Funkzellen nötig. Wenn sich die Funkbereiche der Access Points gegenseitig ein klein wenig überlappen, dann soll es den Clients erlaubt sein, sich frei zu bewegen, ohne dass die Netzwerkverbindung unterbrochen wird. Nicht nur innerhalb ihrer eigenen Funkzellen, sondern auch grenzüberschreitend in andere Funkzellen.

Die Übergabe der Teilnehmer von einem Access Point zum nächsten wird Roaming genannt. Im selben Zusammenhang wie Roaming ist auch der Begriff Hand-Over gebräuchlich.

Für den Roaming-Prozess ist es notwendig, dass die einzelnen Funkzellen einander überlappen und die aneinander angrenzenden Funkzellen auf verschiedenen Kanälen kommunizieren. Würden alle Funkzellen denselben Kanal verwenden, so würde ein Client, der sich im Überlappungsgebiet befindet, ständig einen gestörten Empfang haben. (Siehe hierzu Abschnitt 1.4.4)

Herausforderung des Roaming-Verfahrens

Durch das Roaming nach dem Standard aus IEEE 802.11 entsteht eine Verzögerungszeit von mehreren 100 ms. Diese Zeit ist nötig, um

- das Verlassen der alten Funkzelle durch einen Client zu erkennen und
- seine Verbindung mit einer neuen Funkzelle zu etablieren.

Wird diese Zeit von allen Kommunikationsteilnehmern toleriert, läuft die Kommunikation ungestört weiter.

Werden sehr schnelle Aktualisierungszeiten benötigt, z. B. für PROFINET I/O-Kommunikation, sind Access Points und Client-Module einzusetzen, die das proprietäre Verfahren iPCF (siehe Abschnitt 4.6.1) für schnelles Roaming und deterministischen Datenverkehr unterstützen.

4.3 Infrastruktur-Netzwerke

Der Betrieb von WLANs mit Hilfe von koordinierenden Access Points wird als „Infrastruktur-Modus“ bezeichnet.

Die folgenden Abschnitte zeigen mehrere Beispiele für die Topologie von Infrastruktur-Netzwerken.

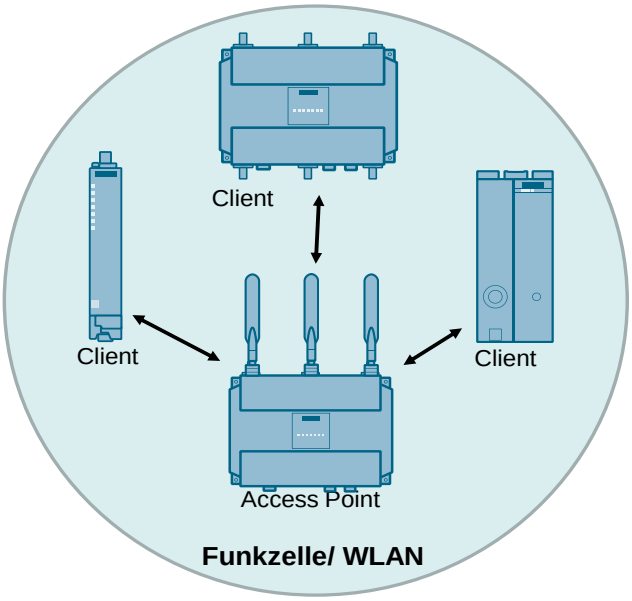
4.3.1 Standalone-Netzwerke

Beschreibung

Standalone-Netzwerke bestehen aus einer Anzahl von Clients, die sich alle in der Funkzelle eines einzigen Access Points befinden. Die Funktion des Access Points beschränkt sich hier darauf, die Kommunikation der Clients untereinander zu koordinieren.

Bildliche Darstellung

Abbildung 4-3



Oben dargestellt ist ein solches Standalone-Netz. Es gibt hierbei einen Access Point, der den Datenverkehr der anderen Busteilnehmer koordiniert und über den der gesamte Verkehr geführt wird. Der Access Point bestimmt die „SSID“ („Service Set Identifier“) des Netzes, sozusagen dessen „Namen“.

Es ist nicht notwendig, dass alle Netzwerkteilnehmer eines Standalone-Netzes direkten Kontakt zueinander haben.

Die maximale Ausdehnung eines solchen Netzwerks wird durch die Bedingung beschränkt, dass alle Clients sich noch innerhalb der Reichweite des Access Points (roter Kreis) befinden müssen.

4.3.2 Gemischte Netzwerke

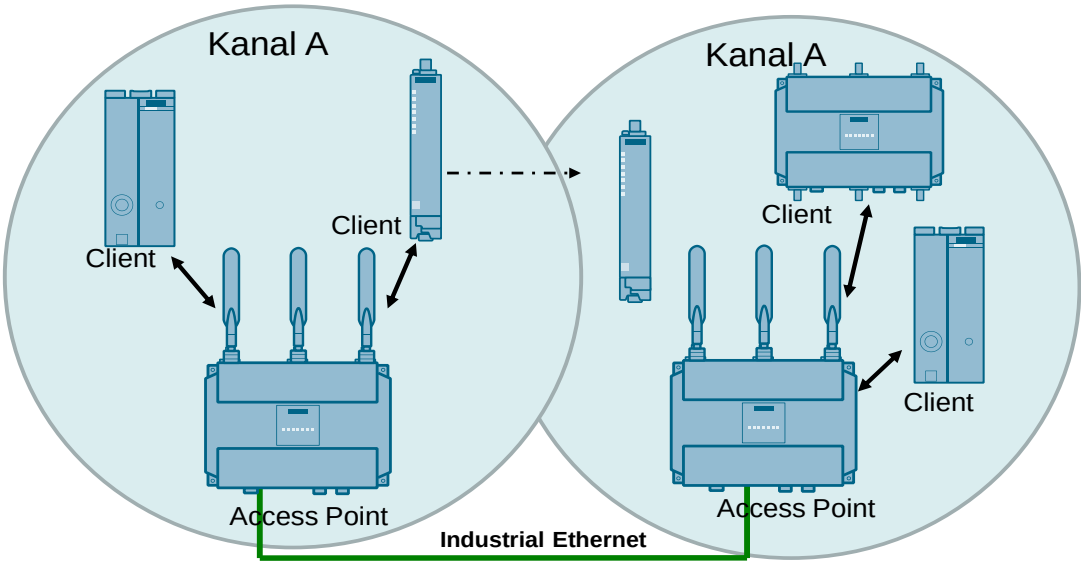
Beschreibung

Im Fall der gemischten Netzwerke dienen die Access Points nicht nur der Kommunikation der Clients untereinander, sondern sie stellen auch noch die Verbindung zu einem kabelgebundenen Netzwerk zur Verfügung. (Dieses kabelgestützte Netzwerk ist in aller Regel Industrial Ethernet.)

Es können mehrere Access Points am kabelgestützten Netz hängen. Das bedeutet wiederum, dass die Access Points mehrere Funkzellen erzeugen. Wenn diese ein bestimmtes Gebiet lückenlos abdecken, können sich die Clients darin von Funkzelle zu Funkzelle bewegen (sog. „Roaming“, siehe Kapitel 4.2).

Bildliche Darstellung

Abbildung 4-4



Eine Zahl Access Points sind untereinander durch eine drahtgebundene Ethernet-Leitung verbunden. (An das Ethernet-Segment können auch noch beliebige andere stationäre Teilnehmer angeschlossen sein.) Innerhalb des von den Access Points abgedeckten Funkfeldes (rote Kreise oben) befinden sich mehrere über WLAN angeschlossene Teilnehmer (Clients).

Gemischte Netzwerke erlauben das „Roaming“, d. h. den Wechsel eines mobilen Teilnehmers von einer Funkzelle in eine benachbarte (siehe oben, unterbrochener Pfeil).

WLANs, die auf diese Weise aufgespannt werden, können theoretisch eine beliebige Größe erreichen. Innerhalb des Überlappungsbereichs der Funkzellen kann es zu Empfangsstörungen kommen, da die Access Points auf derselben Frequenz arbeiten.

4.3.3 Mehrkanal-Konfiguration

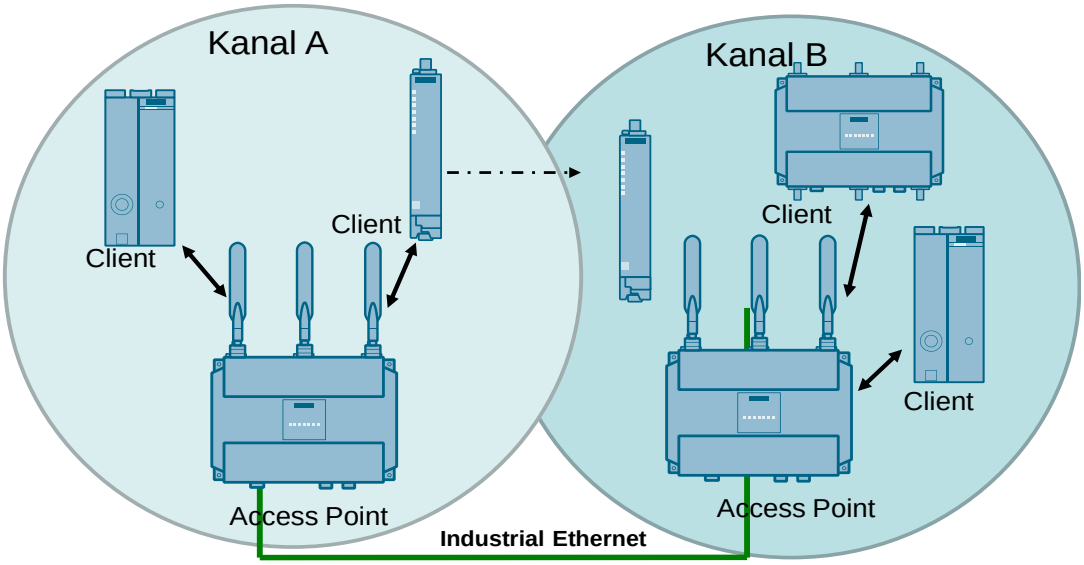
Beschreibung

Die Mehrkanal-Konfiguration entspricht dem gemischten Netzwerk (siehe Kapitel 4.3.2), allerdings arbeiten die einzelnen Access Points hierbei auf verschiedenen, einander nicht überlappenden Funkkanälen (siehe Kapitel 2.4). Auf diese Weise kommt es dort, wo die Funkzellen einander überlagern, nicht mehr zu Störungen.

Gleichzeitig wird das Roaming, also der Wechsel eines Clients von einer Zelle zur anderen, erleichtert, wobei eine deutliche Erhöhung der Performance erzielt wird.

Bildliche Darstellung

Abbildung 4-5



Bei dieser Konfiguration bilden die einzelnen Access Points einen Backbone und sind untereinander durch eine drahtgebundene Ethernet-Leitung verbunden. (An das Ethernet-Segment müssen nicht zwingend andere stationäre Teilnehmer angeschlossen sein.) Innerhalb des von den Access Points abgedeckten Funkfeldes befinden sich mehrere über WLAN angeschlossene Teilnehmer (Clients). Die verschiedenen Frequenzen, auf denen die Access Points senden, sind durch verschiedenfarbige Kreise angedeutet.

Diese Konfiguration hat in der Praxis bei WLAN die größte Verbreitung und wird im Regelfall gewählt.

4.3.4 Wireless Distribution System („WDS“)

Beschreibung

Im normalen Betrieb wird der Access Point als Schnittstelle zu einem kabelgebundenen Netz eingesetzt und kommuniziert mit Clients. Es gibt allerdings auch den Anwendungsfall, dass mehrere Access Points miteinander kommunizieren müssen, beispielsweise zum Zweck der Reichweitenvergrößerung oder zum Aufbau eines Wireless-Backbones (siehe folgendes Kapitel). Diese Betriebsart ist mit WDS (Wireless Distributed System) möglich.

Das WDS entspricht der Mehrkanal-Konfiguration (siehe Kapitel 4.3.3) bis auf einen wichtigen Unterschied: Die Access Points halten die Verbindung *untereinander* nicht über ein zweites Medium (im Falle der Mehrkanal-Konfiguration war das die Industrial Ethernet-Leitung), sondern über das Funknetz.

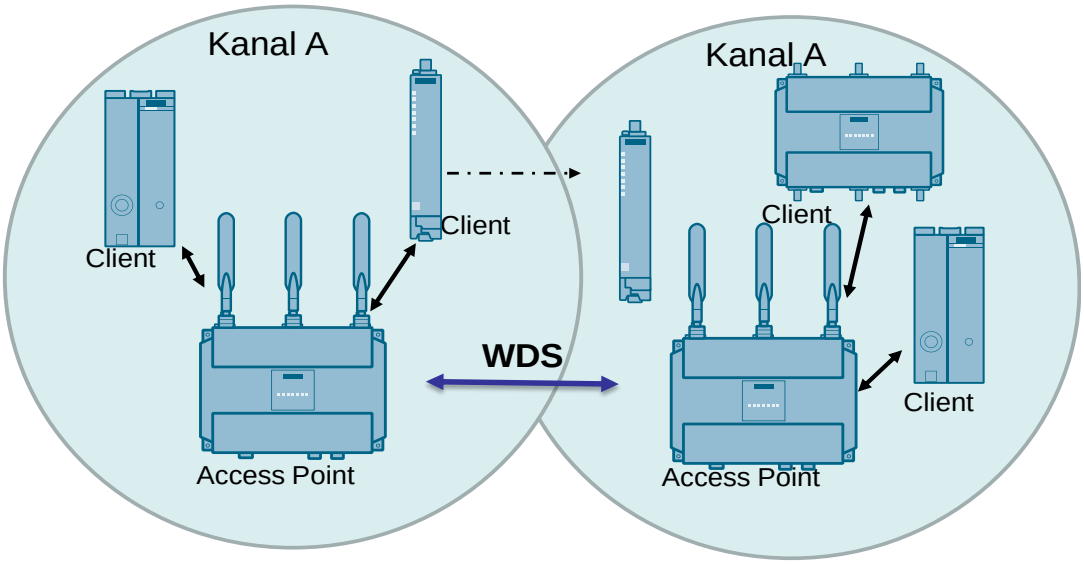
Wird nur die Kommunikation zwischen den Access Points zugelassen und der Zugriff von Clients blockiert, spricht man von einem reinen WDS.

Das WDS wird durch drei Eigenschaften charakterisiert:

- Der Abstand der Access Points zueinander muss gering genug sein, dass jeder Access Point sich innerhalb der Reichweite seines Kommunikationspartners befindet.
- Werden mehrere WDS-Verbindungen auf der gleichen Frequenz eingesetzt oder ist zusätzlich auch die Client-Access-Point-Kommunikation erlaubt, reduziert sich die effektive Datenrate des Access Points, da die Bandbreite geteilt werden muss.
- Alle Access Points, die miteinander kommunizieren sollen, müssen den gleichen Kanal benutzen.

Bildliche Darstellung

Abbildung 4-6



Die obige Illustration verdeutlicht die Funktionsweise, vgl. dazu auch Abbildung 4-4. Innerhalb des von den Access Points abgedeckten Funkfeldes (rote Kreise oben) befinden sich mehrere über WLAN angeschlossene Teilnehmer (Clients). Zusätzlich halten die Access Points untereinander eine weitere Funkverbindung.

4.3.5 Redundante Funkverbindung

Beschreibung

Zum Aufbau eines redundanten Backbones ist es notwendig, Access Points zu verwenden, die über zwei Funkschnittstellen verfügen und so gleichzeitig auf mehreren Frequenzen senden können.

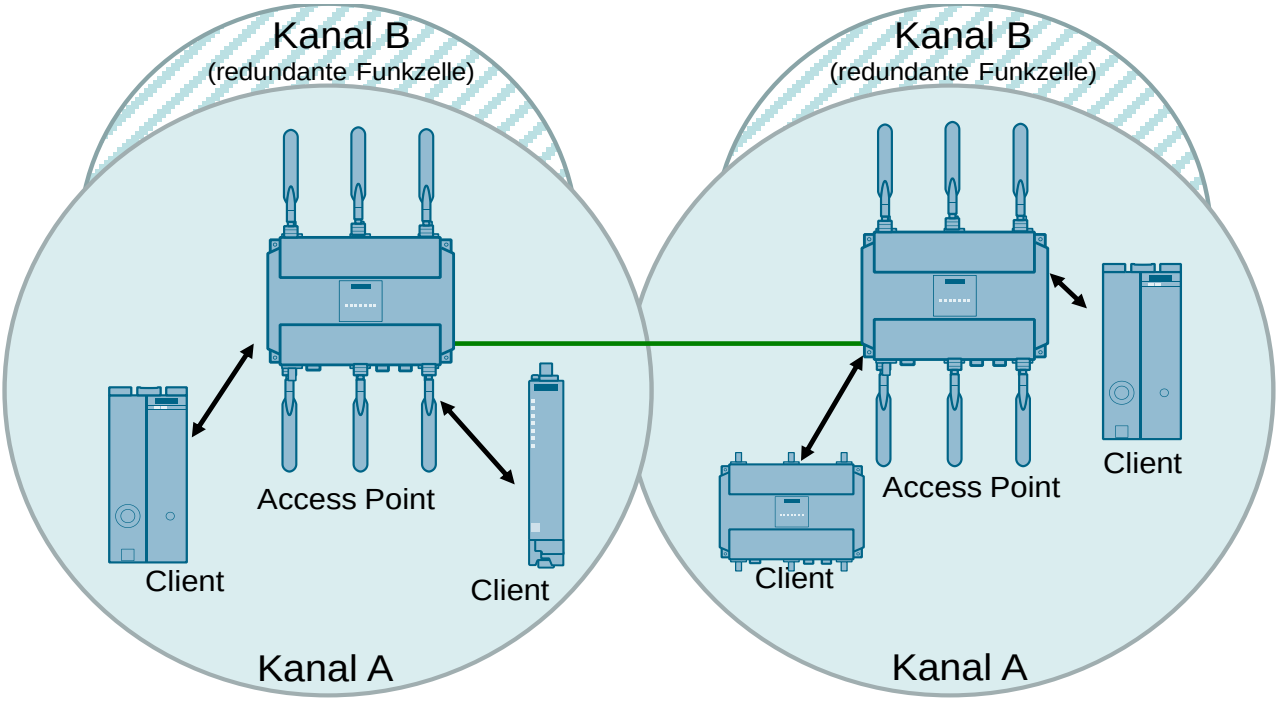
Mit dieser Voraussetzung ist es möglich:

- ein redundantes gemischtes Netzwerk oder
- ein redundantes Wireless Distribution System (siehe Kapitel 4.3.4) aufzubauen, welches aufgrund seiner Lage nicht als verkabeltes Netz aufgebaut werden kann.

Auf diese Art und Weise wird eine hohe Verbindungssicherheit in Kombination mit hohen Datenraten erreicht: Selbst wenn ein Frequenzbereich durch störende Teilnehmer oder Abschattung oder Interferenzen vorübergehend unterbrochen ist, ist mit hoher Wahrscheinlichkeit noch eine Verbindung über den anderen Kanal möglich.

Redundantes gemischtes Netzwerk

Abbildung 4-7

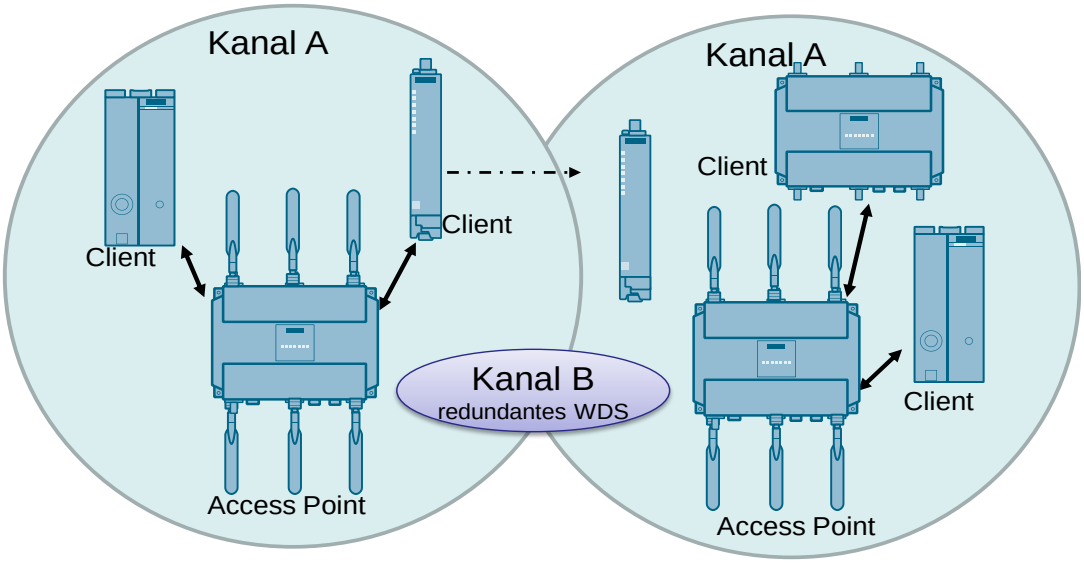


Die Access Points bauen pro Funkschnittstelle eine eigene Funkzelle auf, wobei primär nur eine Funkzelle verwendet wird.

Wenn über die Funkzelle der ersten Funkschnittstelle kein Datentransfer mit dem Access Point möglich ist, können die Clients automatisch auf die Funkzelle der zweiten Funkschnittstelle umschalten. Die Kommunikation zwischen den Access Points erfolgt kabelgebunden über Industrial Ethernet.

Redundantes WDS

Abbildung 4-8



Die Access Points kommunizieren untereinander nicht auf der primären Frequenz, sondern auf einer zweiten Frequenz mit einem zweiten Satz Antennen.

4.4 Koordinierung der Datenübertragung

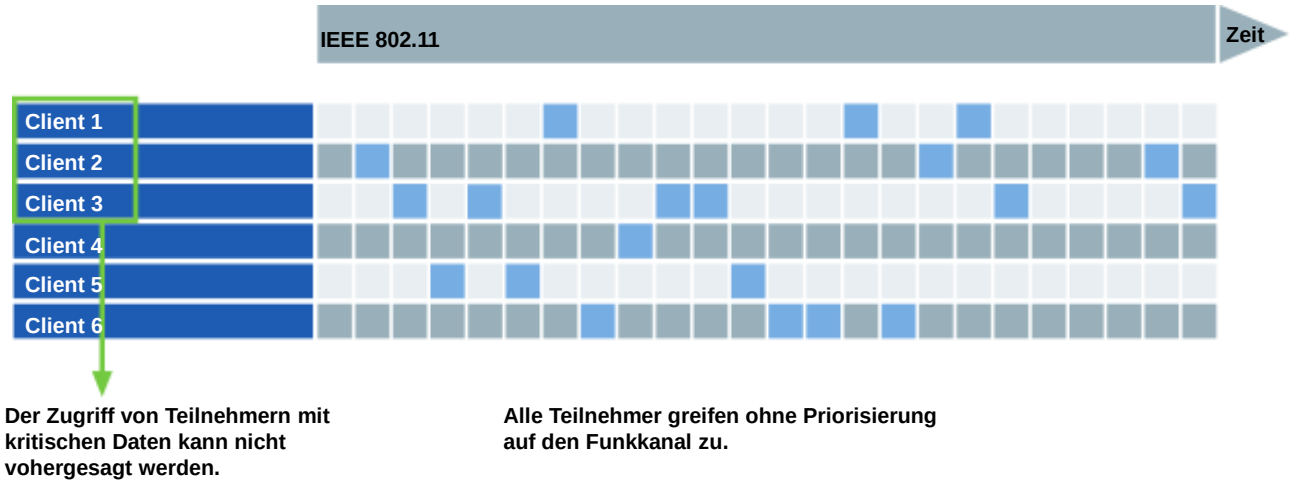
Bei einem WLAN nach dem IEEE 802.11-Standard werden zwei Ansätze unterschieden, die Kommunikation in einem Shared Medium zu koordinieren:

- die Basiszugriffsmethode mit dezentralistischem Ansatz (DCF; Distributed Coordination Function)
- die zentralistische Methode (PCF; Point Coordination Function)

4.4.1 DCF („Distributed Coordination Function“)

Bei einem WLAN nach dem IEEE 802.11-Standard sind alle Teilnehmer prinzipiell „für sich selbst verantwortlich“ und greifen unkoordiniert auf den Funkkanal zu. Der Zugriff von Teilnehmern mit kritischen Daten kann nicht vorhergesagt werden.

Abbildung 4-9



Die Datenübertragung nach dem CSMA/CA-Verfahren ist für alle Beteiligten verbindlich.

Um die Kollisionswahrscheinlichkeit zu reduzieren, hört eine sendewillige Station für eine Wartezeit, die sich aus einer konstanten Wartezeit (DIFS; Distributed Coordination Function InterFrame Space) und einer zufallsabhängigen Wartezeit zusammensetzt, das Medium ab. Ist das Medium belegt, wird bis zum Ende der Datenübertragung gewartet. Danach beginnt zunächst wieder die feste Wartezeit, die mit der reduzierten Zufallswartezeit verlängert wird. Ist das Medium noch frei, beginnt die Datenübertragung.

Der Adressat, der eine für ihn bestimmte Nachricht empfangen hat, sendet seinerseits ein Bestätigungstelegramm zurück. Auch hier muss zur Kollisionsvermeidung erst eine konstante Wartezeit (SIFS; Short Coordination Function InterFrame Space) eingehalten werden.

DCF garantiert nicht, dass eine bestimmte Datenmenge innerhalb einer maximalen Zeitspanne übertragen wird. Aus diesem Grunde ist es in erster Linie geeignet für *asynchrone* Datenübertragungen (wie E-Mail oder Webbrowser).

Für manche DCF-Netzkonfigurationen kann eine Steigerung des Datendurchsatzes durch Verwendung des RTS / CTS-Verfahrens erzielt werden.

4.4.2 “Hidden Station und RTS / CTS-Verfahren“ zur Kollisionsvermeidung

Nicht immer kann eine Station erkennen, ob das Medium frei ist. Insbesondere dann, wenn zwei Teilnehmer einer Funkzelle einander nicht „sehen“ können (d. h., sie befinden sich nicht in der gegenseitigen Reichweite). Dieses WLAN-Problem ist durch den Ausdruck „Hidden-Station“ definiert.

Wenn beide nun versuchen, mit einem dritten Teilnehmer zu kommunizieren, der sich zwischen ihnen befindet (und der mit beiden Sendern gleichzeitig Kontakt hat), kommt es zu Konflikten.

Die Lösung des „Hidden-Station“-Problems liegt im RTS / CTS-Mechanismus. Das Medium wird - um Störungen zu vermeiden - von der sendewilligen Station und der Empfangsstation durch einen Request to Send (RTS) und Clear To Send (CTS) Dialog für andere Stationen für eine Zeitdauer gesperrt. Hierbei reicht es, wenn alle Stationen im Einzugsbereich der sendenden Station eines der beiden Signale RTS / CTS mithören, um diese in den Wartezustand zu versetzen.

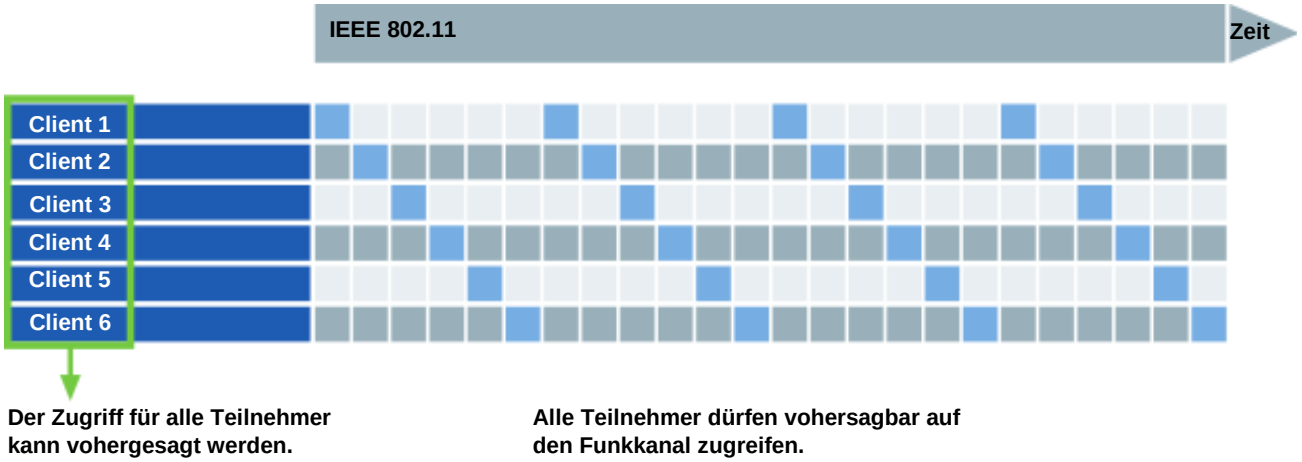
Mithilfe dieses Verfahrens reduziert sich die Zahl notwendiger Übertragungswiederholungen deutlich, weil die Kollision schon vor der Sendung längerer Datenpakete erkannt wird. Der durch die RTS / CTS-Telegramme entstehende Overhead kann jedoch den erreichbaren Datendurchsatz schmälern.

4.4.3 PCF („Point Coordination Function“)

Die Abkürzung PCF bezeichnet ein im 802.11-Standard festgelegtes Zugriffsverfahren, dessen Implementierung jedoch nicht zwingend vorgeschrieben ist. Die Methode ist geeignet, um einige der Nachteile des DCF-Verfahrens zu vermeiden.

Bei PCF sind die Netzteilnehmer nicht alle gleichberechtigt, sondern ein oder mehrere „Access Points“ fungieren als zentrale Administratoren im Netzwerk. Ein Access Point weist dann den anderen Teilnehmern, den „Clients“ Zeitslots zu: Innerhalb dieser Slots ist die Frequenz für diese Clients reserviert, und diese können ungestört senden.

Abbildung 4-10



Mit Hilfe von PCF ist es möglich, den Clients regelmäßigen Netzwerkzugriff zuzuweisen und die Übertragung von Daten innerhalb einer gewissen Frist zu garantieren. Aus diesem Grunde eignet sich PCF bevorzugt für Anwendungen, bei denen kontinuierliche Datenflüsse notwendig sind. (*Synchrone* Datenübertragung, z. B. Video- oder Audiostreams und natürlich auch Prozesswerte.) Die erzielten Übertragungsfristen liegen jedoch im Bereich mehrerer Hundert Millisekunden, und

auch die Geschwindigkeit des Wechsels von einer Funkzelle in die nächste genügt Echtzeitanforderungen nicht.

Es ist dafür möglich, Netzwerke in Intervallen zwischen DCF und PCF wechseln zu lassen, wenn die Anforderungen an die Kommunikation das erfordern.

In der Praxis wird PCF von Herstellern selten unterstützt. Mit iPCF („Industrial Point Coordination Function“) stellt SIEMENS eine proprietäre Alternative zu PCF dar (Siehe Kapitel 4.6.1).

4.5 Funktionen zum Netzwerkmanagement

4.5.1 VLANs („Virtual LANs“)

Die Segmentierung eines physikalischen Netzes in mehrere logische, „virtuelle“ Netze kann sowohl bei kabelgebundenen als auch bei Funknetzen durchgeführt werden. Die VLANs folgen heutzutage in der Regel dem IEEE 802.1Q-Standard.[15]

Segmentierung des Datenverkehrs

Bei dieser Art der Netzwerknutzung wird den einzelnen Ports eines Switches (bzw. Access Points) über die Konfiguration eine sogenannte VLAN-ID zugewiesen. Eine Kommunikation ist dann nur noch innerhalb eines VLANs (Ports mit gleicher VLAN-ID) möglich.
Dafür werden die Ethernet-Datenpakete („Frames“) um einen Datenblock (ein „Tag“) erweitert, der eine VLAN-ID beinhaltet. Die Switches (bzw. Access Points) leiten die Nachricht nur an die Mitglieder des VLANs weiter, an das die Nachricht adressiert ist.

Vorteile

Mit der Verwendung von VLANs wird eine Vielzahl von Vorteilen erzielt:

- Fehlkonfigurationen bleiben auf das VLAN, in dem sie vorgenommen wurden, beschränkt und können nicht mehr das gesamte LAN lahmlegen.
- Broadcasts, d. h. Sendungen an einen allgemeinen Empfängerkreis, werden nicht mehr über das komplette LAN, sondern nur über das betreffende VLAN vorgenommen; dadurch sinkt die Netzlast.
- Den einzelnen VLANs können verschiedene Prioritäten zugewiesen werden, durch die die Nachrichten eines hochprioren Teilnehmerkreises bevorzugt transportiert werden.
- Anders als bei der Verwendung von IP-Subnetzen können die Teilnehmer verschiedener VLANs gleiche IP-Adressen haben. Dadurch kann der beschränkte IP-Adressraum besser ausgenutzt werden, und identisch aufgebaute Produktionszellen können mit identischen IP-Adressen konfiguriert werden, wodurch der Aufwand bei Projektierung und Administration sinkt.
- Die VLAN-Konfiguration ist für die Endteilnehmer transparent, d. h., die Endteilnehmer wissen nicht, zu welchen VLANs sie gehören, und können auch deren Datenverkehr nicht mithören. Auf diese Art wird eine gewisse Sicherung des Netzes erreicht.

Hinweis Zu diesem Thema finden Sie im Siemens Industry Online Support ein animiertes Vorführsystem (Beitrags-ID 31770396):
http://support.automation.siemens.com/WW/view/de/31770396

[15] Ältere Protokolle wie ISL („Inter Switch Link“) und VLT („Virtual LAN Trunk“) spielen heute keine Rolle mehr.

4.5.2 STP („Spanning Tree Protocol“)

Beschreibung

Redundante Netze sind Netze, in denen zwischen den Endteilnehmern Nachrichten über Switche weitergeleitet werden, wobei jedes Paar von Endteilnehmern jeweils durch mehr als einen Pfad miteinander verbunden ist. Ein solches Netz kann kabelgebunden oder drahtlos sein; im letzteren Fall agieren die Access Points als Switches.

Die Nachrichten über jede mögliche Verbindung weiterzuleiten würde unnötige Netzlast erzeugen und das Netz verstopfen. Viel sinnvoller ist es, wenn die Switches bzw. Access Points die optimalen Pfade zwischen den Endteilnehmern ermitteln und die Nachrichten nur entlang dieser Route weitertransportieren. Einen alternativen Ausweichpfad verwenden sie erst, wenn die optimale Route durch Störungen oder Geräteausfall unterbrochen ist.

Zu diesem Zweck wurde das „Spanning Tree Protocol“ STP als IEEE-Standard 802.1d entwickelt.

Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzwerkstruktur und überführt sie in eine Baumtopologie (Spanning Tree).

Funktionsablauf

Zusätzlich zum regulären Datenverkehr tauschen die Switches hierbei besondere BPDUs („Bridge Protocol Data Units“) untereinander aus. In diesen BPDUs sind die MAC-Adressen des Absenders und der weiterleitenden Switches vermerkt. Indem sie diese Informationen auswerten, können die Switches selbstlernend eine „Karte“ des Netzwerks entwickeln und lernen, welche Datenpfade zur Verfügung stehen.

Welcher Pfad der optimale ist, wird anhand zweier Kriterien bestimmt:

- Prinzipiell wird der Weg bevorzugt, der die geringsten „Pfadkosten“ beinhaltet. Die Pfadkosten sind hierbei umgekehrt proportional zur Datenrate einer Verbindung.
- Sind die Pfadkosten zweier Verbindungen gleich, so wird die Route mit höherer Priorität gewählt. Diese Priorität der einzelnen Ports wird an den Switches selbst konfiguriert.

Im regulären Betrieb laufen alle Nachrichten über den optimalen Pfad.

4.5.3 RSTP („Rapid Spanning Tree Protocol“)

Ein Nachteil des STP ist, dass sich das Netz bei einer Störung oder einem Geräteausfall rekonfigurieren muss: Die Switches beginnen erst im Moment der Unterbrechung, neue Pfade auszuhandeln. Dieser Vorgang dauert bis zu 30 Sekunden; eine solche Frist ist für viele Automatisierungsvorgänge nicht akzeptabel.

Aus diesem Grunde wurde STP zum „Rapid Spanning Tree Protocol“ (RSTP, IEEE 802.1w) erweitert. Dies unterscheidet sich vom STP im Wesentlichen dadurch, dass die Switches bereits zum Zeitpunkt des ungestörten Betriebs Informationen über Alternativrouten sammeln.

Damit lässt sich die Rekonfigurationszeit für ein RSTP-gesteuertes Netz üblicherweise auf wenige Sekunden reduzieren.

Hinweis Weitere Informationen zum Thema „RSTP in Wireless LANs“ finden Sie im Siemens Industry Online Support (Beitrags-ID 30805917): http://support.automation.siemens.com/WW/view/de/30805917

4.5.4 MSTP („Multiple Spanning Tree Protocol“)

STP als auch RSTP arbeiten mit einer globalen Baumtopologie (Spanning Tree) für das gesamte Netzwerk. Zur Gewährleistung der Schleifenfreiheit werden dabei bestimmte Weg-Pfade nicht verwendet. Die vorhandenen Wege-Ressourcen werden demnach nicht effizient ausgenutzt. Zudem hat ein einzelner Spanning Tree den Nachteil, dass die Rekonfiguration bei großen Netzen relativ lange dauert.

Das Multiple Spanning Tree Protocol (MSTP) ist eine Weiterentwicklung von RSTP und oft im Zusammenhang mit VLANs anzutreffen.

MSTP arbeitet nicht nur mit einer Baumtopologie, sondern betreibt in jedem VLAN einen eigenen Spanning Tree. Lange Rekonfigurationszeiten können durch die kürzeren STP-Instanzen vermieden und die durch RSTP gesperrten Pfade innerhalb einzelner VLANs verfügbar gemacht werden.

4.6 Proprietäre Erweiterungen des IEEE 802.11-Standards: iFeatures

4.6.1 iPCF („Industrial Point Coordination Function “)

iPCF („Industrial Point Coordination Function“) stellt eine proprietäre, von SIEMENS entwickelte Alternative zu PCF dar, die mehrere der mit PCF (siehe Kapitel 4.4.3) vorhandenen Probleme löst. Zudem ermöglicht iPCF den Clients einen sehr schnellen Wechsel der Funkzelle, bei dem das Abmelden- und Neuanmelden des Clients ("Handover") so schnell vor sich geht, dass Echtzeitanforderungen der Kommunikation noch eingehalten werden.

Funktionsprinzip

Bei iPCF pollen die Access Points in regelmäßigen, sehr kurzen Abständen die Clients in ihrer Funkzelle. Diese können dabei ihren Bedarf anmelden, längere Datentelegramme zu senden, sie beginnen mit der Sendung jedoch erst, falls sie die Erlaubnis des Access Points dazu bekommen haben.

Aus diesen Eigenschaften resultieren folgende Effekte:

- Der Access Point kann dazu parametriert werden, die Pollings in sehr schneller Folge vorzunehmen. Daraus resultieren sehr geringe garantierte Antwortzeiten (deterministische Übertragung): Die Antwortzeiten können auf rund 2 ms pro Netzteilnehmer reduziert werden d. h., bei vier Clients ist eine Antwortzeit unter 10 ms garantiert.
- Die Übertragung größerer, nicht-zeitkritischer Telegramme, wird verschoben, bis freie Zykluszeit zur Verfügung steht.
- Die Abfrage eines Teilnehmers wird von allen anderen Teilnehmern in der Funkzelle gesehen. So kann ein Client die Qualität der Funkverbindung zum Access Point auch dann feststellen, wenn er selbst nicht mit dem Access Point kommuniziert.
- Durch die kurzen Polling-Zykluszeiten stellt ein Client sehr schnell fest, ob die Verbindung zu seinem Access Point noch besteht oder nicht. Ist der Kontakt verloren gegangen, kann der Client innerhalb kürzester Zeit reagieren und eine Verbindung zu einem alternativen Zugangspunkt herstellen.
- Im iPCF-Modus ist sowohl die Suche nach einem neuen Access Point als auch das Anmelden an diesem Access Point in ihrem Zeitverhalten optimiert. Es werden Handover-Zeiten von deutlich unter 50 ms erreicht.

Mit iPCF werden also insbesondere industrielle Anwendungen mit mittleren Echtzeitanforderungen im zweistelligen Millisekundenbereich WLAN-fähig. In diesen Bereich fällt unter anderem die drahtlose Anbindung von PROFINET I/O-Geräten.

Eine optimale Performance mit iPCF wird erzielt, wenn die Clients festen Bahnen folgen (z. B. bei der Verwendung von RCoax-Leitungen). Bei frei beweglichen Teilnehmern im Verkehr mit stationären Access Points wird die Verwendung von iPCF-MC (siehe 4.6.2) empfohlen.

Einschränkungen durch iPCF

iPCF kann nur allein betrieben werden. Eine Kombination mit anderen industriellen Funktionalitäten (iFeatures wie z. B. iPCF-MC, Dual Client) ist nicht möglich.

Das iPCF-Verfahren ist eine Eigenentwicklung der Fa. Siemens AG und arbeitet nur mit Teilnehmern zusammen, bei denen iPCF implementiert ist. Bei einem Access Point mit zwei WLAN-Schnittstellen ist es jedoch möglich, sowohl iPCF als auch Standard-WLAN gleichzeitig einzustellen.

Wenn der iPCF-Modus aktiviert ist, wird bei den Sicherheitseinstellungen nur Open System mit den Verschlüsselungsverfahren AES mit 128 Bit-Schlüssellänge unterstützt.

Kompatibilität mit anderen WLAN-Standards

„Gemischte Netzwerke“, bei denen ein Teil der Geräte über DCF / iPCF angebunden ist, sind mit iPCF nicht möglich.

4.6.2 iPCF-MC („iPCF – Management Channel “)

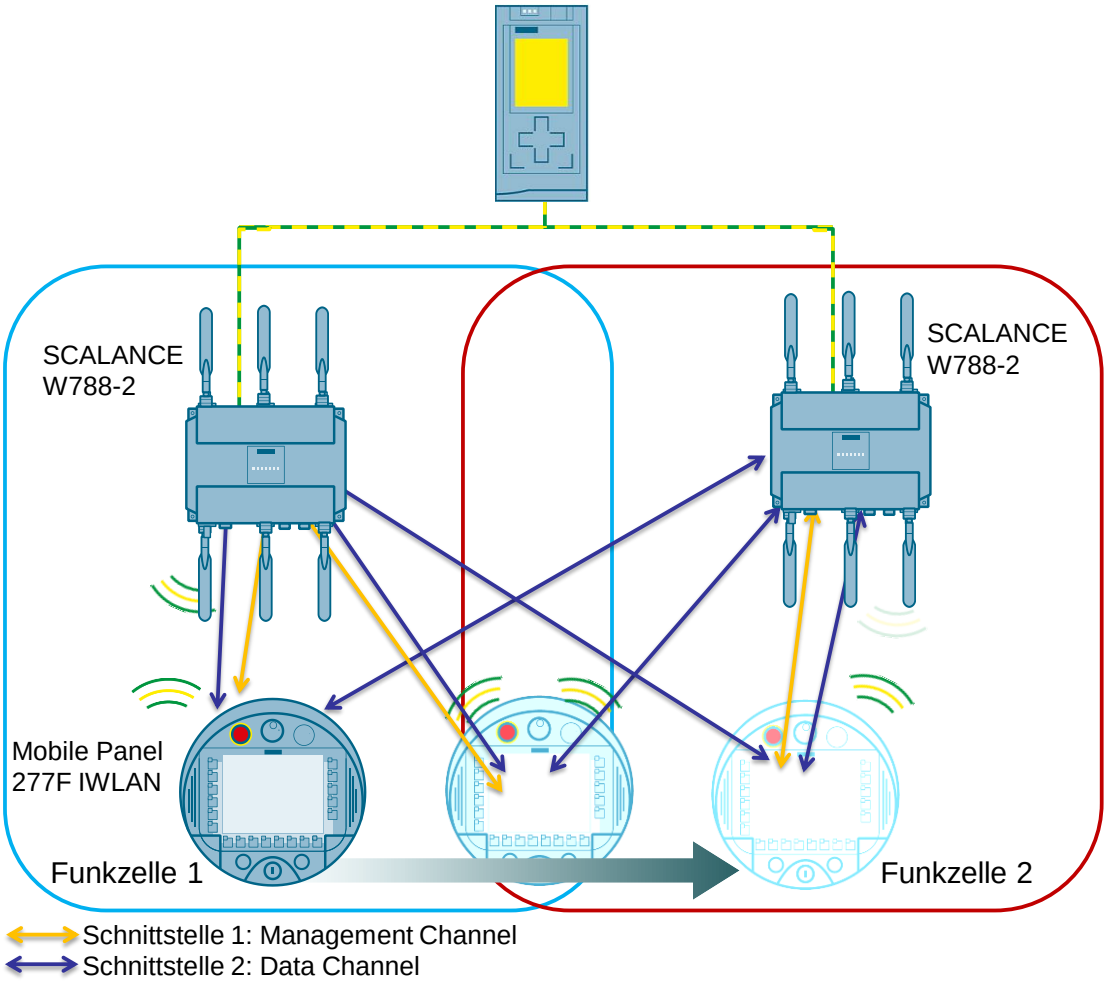
iPCF und iPCF-MC

iPCF-MC wurde entwickelt, um die durch iPCF (siehe Kapitel 4.6.1) erzielten Vorteile auch für frei bewegliche Teilnehmer nutzbar zu machen, die unabhängig von einer RCoax-Leitung oder gerichteten Antennen kommunizieren. Bei iPCF-MC sucht der Client auch dann nach potentiell geeigneten Access Points, wenn er iPCF-Abfragen des Access Points erhält und die bestehende Verbindung zu einem Access Point störungsfrei funktioniert. Dadurch kann im Bedarfsfall der Wechsel zu einem anderen Access Point sehr schnell erfolgen. Im Gegensatz zu iPCF sind bei iPCF-MC die Handover-Zeiten unabhängig von der Anzahl der verwendeten Funkkanäle.

Funktionsprinzip

Wenn iPCF-MC eingesetzt wird, ist es notwendig, einen Access Point mit zwei Funkschnittstellen zu verwenden, einen so genannten Dual Access Point. Die eine Schnittstelle arbeitet als Management Channel und sendet kurze Telegramme („Beacon“) mit administrativen Informationen (z. B. Kanaleinstellung des Data Channels und SSID). Die andere Schnittstelle (Data Channel) überträgt ausschließlich die Nutzdaten.

Abbildung 4-11



Einschränkungen durch iPCF-MC

Access Points mit einer WLAN-Schnittstelle können nicht am iPCF-MC-Verfahren teilnehmen. iPCF ist aber möglich.

iPCF und iPCF-MC sind nicht miteinander kompatibel und können nicht gleichzeitig bei einem Gerät eingesetzt werden.

Das iPCF-MC-Verfahren ist eine Eigenentwicklung der Fa. Siemens AG und arbeitet nur mit Teilnehmern zusammen, bei denen iPCF-MC implementiert ist.

Voraussetzungen

Für die Nutzung dieser Funktion sind folgende Voraussetzungen notwendig:

- iPCF-MC nutzt die beiden Funkschnittstellen des Access Point unterschiedlich: Die eine Schnittstelle arbeitet als Management-Schnittstelle. Die andere Schnittstelle überträgt die Nutzdaten. Als Access Points können somit nur SCALANCE W700-Geräte mit zwei WLAN-Schnittstellen eingesetzt werden.
- Management Channel und Data Channel müssen im gleichen Frequenzband betrieben werden und hinsichtlich ihrer Funkabdeckung übereinstimmen. iPCF-MC wird nicht funktionieren, wenn beide Funkschnittstellen mit Richtantennen ausgestattet sind, die unterschiedliche Bereiche abdecken.
- Die Management Channel aller Access Points, zwischen denen ein Client wechseln soll, müssen den gleichen Kanal verwenden. Ein Client scannt nur diesen einen Kanal, um erreichbare Access Points zu finden.
- Für den Management Channel kann nicht das Übertragungsverfahren nach IEEE 802.11h verwendet werden. Für den Data Channel ist 802.11h jedoch möglich.
- Ein Client muss dieses Feature auf seiner WLAN-Schnittstelle unterstützen.

4.6.3 iREF

Die industriespezifischen Erweiterung 'Industrial Range Extension Function' (iREF) dient zur Verbesserung der Übertragungsverhältnisse.

Durch die Minimierung der Anzahl der verwendeten Access Points entlang einer Strecke und die Vermeidung von sich überlappenden Funkkanälen entstehen weniger Interferenzen mit benachbarten Access Points, was zu einem höheren Datendurchsatz der gesamten Anlage führt.

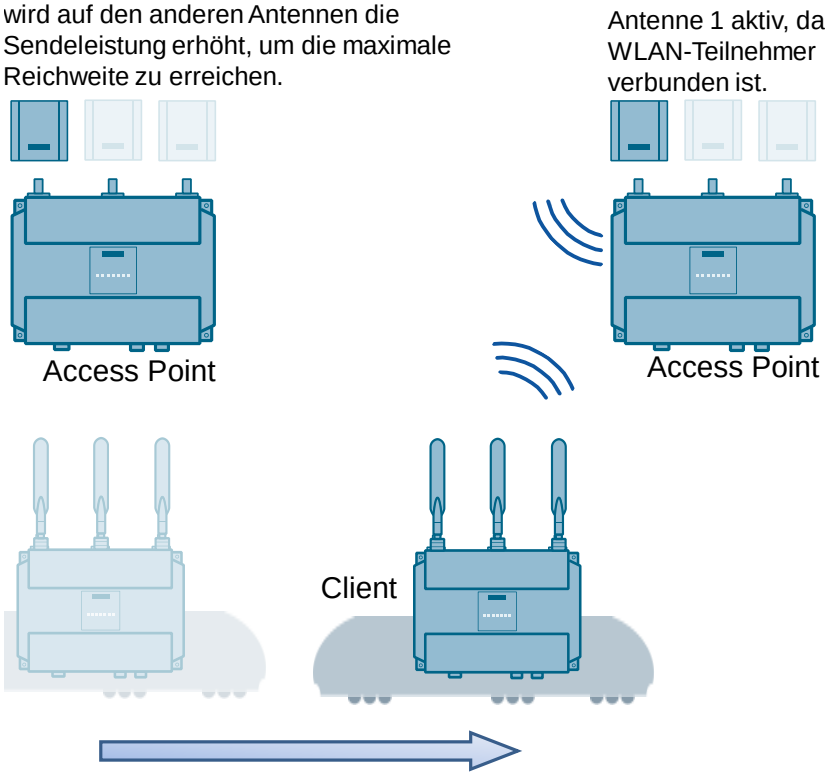
Funktionsprinzip

iREF (industrial Range Extension Function) sorgt dafür, dass der Datenverkehr vom Access Point zu jedem einzelnen Client über die jeweils am besten geeignete Antenne abläuft.

Welche Antenne am Besten geeignet ist, wird vom Access Point auf Basis der RSSI-Werte empfangener Pakete ermittelt. Unter Einbeziehung von Antennengewinn und ggf. Kabelverlusten werden Pakete jeweils nur auf denjenigen Antennen gesendet, für die clientseitig die maximale Signalstärke zu erwarten ist.

In dieser Zeit sind die anderen Antennen inaktiv und die gesetzlich zulässige Sendeleistung steht für die ausgewählte Antenne zur Verfügung.

Abbildung 4-12



Einschränkungen durch iREF

iREF kann nur allein betrieben werden. Eine Kombination mit anderen industriellen Funktionalitäten (iFeatures wie z. B. iPCF, iPCF-MC) ist nicht möglich.

Es ist nur eine maximale Datenrate von bis zu 150 Mbps möglich.

Voraussetzungen

Um die iREF-Technologie nutzen zu können, muss das Gerät über mindestens zwei aktivierte Antennen verfügen.

4.6.4 Inter AP Blocking

Die Clients, die an einem Access Point verbunden sind, können im Normalfall mit allen Geräten des Layer 2-Netzes kommunizieren.

Mit Inter AP Blocking lässt sich die Kommunikation der Clients einschränken, die mit dem Access Point verbunden sind. Nur die Geräte sind für die Clients zugänglich, deren IP-Adressen dem Access Point bekannt sind. Eine Kommunikation mit anderen sich im Netz befindlichen Teilnehmern wird damit unterbunden.

Hinweis Weitere Dokumente zum Thema „Aktuelle IWLAN-Technologien“ finden Sie auf dem SIEMENS Automatisierungsportal unter der URL:

http://www.automation.siemens.com/net/html_00/support/whitepaper.htm

4.6.5 Einsetzbare IWLAN-Geräte

Folgende Tabelle zeigt in einer Übersicht, welche iFeatures mit welchen IWLAN-Geräten kompatibel sind:[16]

Tabelle 4-1

IWLAN-Gerät	Typ	iPCF	iPCF-MC	iREF	Inter AP Blocking
SCALANCE W788-1 RJ45 / M12	AP	KEY-PLUG	- (nur als Client)	KEY-PLUG	KEY-PLUG
SCALANCE W788-2 RJ45 / M12 (EEC)			KEY-PLUG		
SCALANCE W786-1 RJ45			- (nur als Client)		
SCALANCE W786-2 RJ45 / SFP			KEY-PLUG		
SCALANCE W786-2IA RJ45					
SCALANCE W774-1 RJ45/ M12 (EEC)			- (nur als Client)		
SCALANCE W761-1 RJ45		-	-	-	-
SCALANCE W748-1 RJ45 / M12	Client	KEY-PLUG		-	-
SCALANCE W734-1 RJ45				-	-
SCALANCE W722-1 RJ45		x	x	-	-
SCALANCE W721-1 RJ45		-	-	-	-
Mobile Panel 277 IWLAN		-	x	-	-

[16] x: Die Funktion ist verfügbar
-: Die Funktion ist nicht verfügbar
KEY-PLUG: Die Funktion erfordert die Freischaltung über den entsprechenden KEY-PLUG (siehe Kapitel 9.1.1).

4.6.6 iFeatures und PROFINET I/O

PROFINET ist ein offener, herstellerübergreifender Produktstandard auf der Basis von Industrial Ethernet, der die vertikale Integration der Automatisierung, d. h. die Vernetzung aller Ebenen des Produktionsablaufs, vereinfacht. PROFINET I/O ist für den Datenaustausch in Echtzeit auslegt.

Das WLAN ist in seinem Ursprung ein Shared-Medium. Alle Teilnehmer sind prinzipiell „für sich selbst verantwortlich“ und greifen unkoordiniert auf den Funkkanal zu. Der Zugriff von Teilnehmern mit kritischen Daten kann nicht vorhergesagt werden. Unter diesen Voraussetzungen ist PROFINET I/O nur sehr bedingt bzw. unter gewissen Randbedingungen in einem Standard-WLAN einsetzbar.

Durch die proprietären iFeatures von SIEMENS

- iPCF
- iPCF-MC

wird Echtzeitkommunikation auch für ein Funknetz ermöglicht.

5 Datensicherheit und –verschlüsselung

5.1 Angriffsszenarien und Sicherheitsmechanismen

5.1.1 Grundsätzliches zur WLAN-Sicherheit

WLANs erzeugen beim Anwender leicht ein Gefühl der Unsicherheit, denn es ist für einen Eindringling nicht nötig, sich z. B. Zutritt auf ein Werksgelände zu verschaffen und sich physikalisch mit dem Netzwerk zu verbinden, um Daten mithören zu können: Prinzipiell kann jeder den Datenverkehr eines Netzes mithören, wenn er sich in dessen Funkbereich befindet. Diese Annahme ist allerdings insofern trügerisch, als es heute kaum noch kabelgebundene, isolierte LANs gibt: In Wirklichkeit sind die meisten LANs mit dem Internet verbunden und damit potenziell Angriffen von außen ausgesetzt. Sicherheit muss also sowohl bei Funknetzen als auch bei kabelgebundenen Netzen bewusst projektiert werden.

Fortschritte in Sicherheitsstandards und der Leistungsfähigkeit der Komponenten haben dazu geführt, dass Funknetze heutzutage als ebenso sicher wie drahtgebundene Netze gelten können.

Eine der einfachsten Maßnahmen, ein Funknetz zu sichern, besteht beispielsweise darin, die Access Points und ihre Sendeleistung so zu konfigurieren, dass sie tatsächlich nur den benötigen Raum abdecken und keine Überreichweiten entstehen. So ist das Funknetz auf das Firmengelände beschränkt und kann nicht von außen mitgehört werden.

Eine Reduktion der Funkleistung kann natürlich nur einen begrenzten Schutz bieten und ist nicht in beliebigem Umfang machbar. Fortgeschrittene, wirkungsvollere und sichere Methoden sind die Wahl einer geeigneten Infrastruktur sowie der Einsatz leistungsfähiger Verschlüsselungs- und Authentifizierungsprotokolle, wie sie im folgenden Kapitel beschrieben werden.

5.1.2 Angriffsszenarien

Kompromittierung des Sicherheitskonzepts

Das Sicherheitskonzept eines WLANs kann auf mehrere Arten unbeabsichtigt kompromittiert werden:

- *Fehlerhaft konfigurierte Access Points*: Access Points, die durch einen internen Anwender mit dem drahtgebundenen Netz verbunden, aber fehlerhaft konfiguriert wurden. Wenn z. B. keine Sicherheitseinstellungen vorgenommen wurden, bietet der betroffene Access Point einen freien Netzzugang für alle.
- *Ad-hoc-Wireless-Netz*: Betriebssysteme wie Windows ermöglichen es, Netze bestehend aus mehreren Wireless Clients ohne dazwischen liegenden Access Point einzurichten. Wenn einer der Computer so konfiguriert wird, dass er sowohl Teil eines Ad-hoc-Netzes bildet als auch Verbindungen zum Unternehmens-WLAN herstellt, kann er unbeabsichtigt einen Zugang für Hacker schaffen.
- *Client-Fehlverbindungen*: Wenn Unternehmen sich physikalisch in unmittelbarer Nähe befinden, nutzen die Unternehmens-WLANs höchstwahrscheinlich die gleichen Netzinformationen. In diesem Fall verbindet sich ein drahtloser Client mit dem ersten erreichbaren Access Point. Gehört dieser aber zum benachbarten WLAN, kann dies ein Sicherheitsrisiko bedeuten.

Angriffsmethoden

Böswillige Anwender können häufig von den oben beschriebenen Sicherheitslücken profitieren. Folgende Beispiele beschreiben jedoch auch Szenarien, in denen sie sich eigene Zugänge zu WLANs schaffen:

- *Rogue Access Points*: Ein illegaler Zugriffspunkt verbindet sich mit dem drahtgebundenen Netz und verschafft böswilligen oder nicht berechtigten Anwendern einen freien Zugang zum LAN.
- *Honeypot Access Points*: Einige Hacker sind in der Lage, die Konfigurationseinstellungen von WLANs zu ermitteln und setzen einen Access Point mit den gleichen Einstellungen innerhalb der Netzreichweite ein. Durch diese absichtliche Fehlverbindung stellen Clients eine Verbindung zu diesen "Honeypots" in der Annahme her, einen offiziellen Access Point zu kontaktieren. Erfahrene Hacker können dies ausnutzen, indem sie Netzressourcen mit dem AP verbinden, die als Köder agieren, so dass sich die Anwender wie gewohnt dort anmelden und den Hackern damit die Möglichkeit verschaffen, Passwörter oder vertrauliche Dokumente unberechtigt in ihr Eigentum zu bringen.
- *Access Point MAC Spoofing*: Drahtlose Client-Computer können als Access Points konfiguriert werden. Auf diese Weise kann ein Hacker einen normalen PC als Honeypot missbrauchen.

Manipulationsmöglichkeiten

Falls ein Hacker seinen Weg ins Netz gefunden hat - entweder durch eine bestehende Lücke oder durch Schaffen einer Lücke - gibt es verschiedene Möglichkeiten, um das Unternehmensnetzwerk zu manipulieren:

- *Nicht autorisierte Client-Zugriffe*: Hacker suchen permanent Zugangsmöglichkeiten in drahtlose Netze. Wenn ein Netz über eine schwache - oder nicht vorhandene - Anwenderauthentifizierung verfügt, wird der Zugang ins Unternehmensnetz sehr leicht gemacht und die Hacker können Informationen abrufen oder Ressourcen angreifen, was zu Störungen führt.
- *Denial of Service* („DoS“): Vernetzte Geräte müssen auf alle Client-Anfragen reagieren. Hacker nutzen diese Eigenschaft, indem sie eine Netzressource mit mehr Anfragen überschwemmen als sie bewältigen kann. Verteilte DoS-Angriffe verstärken die Problematik noch, indem sie eine Reihe „unwissender“ Computer mithilfe von verborgenem Code präparieren, die dann simultan DoS-Angriffe von u. U. enormen Ausmaßen vornehmen.
- *„Man in the Middle“*: Bei ungeschützten Daten können Hacker Nachrichten abfangen und Inhalte manipulieren, indem sie sich als Teilnehmer auf der Wegstrecke einer Kommunikationsverbindung tarnen.
- *IP Spoofing*: Mittels Manipulation der Quell-IP-Adresse im Paket-Header kann ein Hacker auf Verkehr von einem korrekt authentifizierten Anwender zugreifen und vortäuschen, dass der Anwender den Computer des Hackers nutzt. Infolgedessen gehen alle Daten und Nachrichten des Servers an den Hacker zurück.
- *Hijacking*: Mithilfe von Software, die heimlich auf dem PC eines Unternehmensanwenders installiert wird, kann ein Hacker die Kontrolle über den betroffenen Computer übernehmen und sich Zugang zu den Ressourcen verschaffen, die der Anwender sehen kann, oder Server oder andere Computer schädigen.

5.1.3 IEEE 802.11-Sicherheitsmechanismen

Zum Schutz vor unbefugten Zu- und Angriffen auf das Unternehmensnetzwerk ist es unerlässlich, geeignete Sicherheitsmechanismen in den WLAN-Komponenten zu aktivieren.

WEP

WEP ("Wired Equivalent Privacy") stellt das älteste und zugleich am wenigsten sichere Verschlüsselungsverfahren dar, mit dem WLAN-Übertragungen nach dem 802.11-Standard gegen unbefugte Eindringlinge geschützt werden.

Bei diesem Verfahren wird ein Passwort der Anwender als Schlüssel verwendet, mit dessen Hilfe eine Folge von Pseudo-Zufallszahlen generiert wird. Jedes Zeichen des zu übertragenden Telegramms wird dann mit der nächsten Zahl aus dieser Folge ver- bzw. beim Empfänger entschlüsselt.

Das Verfahren ist relativ schlicht und kann aus zweierlei Gründen vergleichsweise einfach kompromittiert werden. Zum einen muss beim Verbindungsaufbau ein Austausch des Schlüssels zwischen Sender und Empfänger geschehen, der natürlich unverschlüsselt abläuft.

Zum anderen können statistische Methoden angewandt werden, um aus dem übertragenen Telegrammverkehr Charakteristika zu ermitteln, die wiederum Rückschlüsse auf den verwendeten Schlüssel erlauben, aber nur solange hinreichend viele Telegramme für die Analyse vorliegen.[17]

Mit entsprechenden Tools kann der Datenverkehr in mit WEP verschlüsselten Netzwerken innerhalb weniger Minuten entschlüsselt werden. Aus diesen Gründen wird WEP heutzutage im Allgemeinen nicht mehr als hinreichend sicher erachtet.

ACL-Zugangskontrolle

Bei der Netzwerkverwaltung können Filtertabellen („Access Control List") mit IP-Adressen aufgestellt werden, die den Zugriff für bestimmte Adressen erlauben oder verbieten. Auf diese Art und Weise kann ein einfacher, wenn auch vergleichsweise unsicherer Zugriffsschutz für das Netzwerk implementiert werden.

Es ist nämlich nicht ausgeschlossen, dass IP-Adressen manipuliert werden (sog. „Spoofing"), sodass die ACL nur in Verbindung mit anderen Maßnahmen hinreichende Sicherheit für ein Netzwerk bieten.

SSID

Die SSID („Service Set Identifier") ist ein frei wählbarer Name für das WLAN und identifiziert dieses.
Ein WLAN-Access Point sendet diese SSID aus, wenn ein Client nach verfügbaren Drahtlosnetzen sucht.

Aus diesem Grund sollte - sicherheitstechnisch betrachtet - die SSID keine Rückschlüsse auf das Unternehmen, Einsatzzweck des Netzwerks oder Standort geben, da sonst eventuell die Neugier von Hackern oder anderen unbefugten Personen geweckt werden könnte.
Das Aussenden des Netzwerknamens kann aber auch unterdrückt werden. Da die Clients das Funknetz nun nicht mehr „sehen" können, muss die SSID in die Projektierung der Clients korrekt eingetragen werden, damit sich diese mit dem gewünschten WLAN verbinden können.

[17] Häufiger manueller Wechsel der Schlüssel durch den Anwender würde die Sicherheit erhöhen, wird allerdings in der Praxis selten konsequent durchgeführt.

Hinweis Da bei der SSID-Übertragung keine Verschlüsselung eingesetzt wird, kann diese Funktion nur grundlegend vor unberechtigten Zugriffen schützen. Die Nutzung einer Authentifizierungsmethode (z. B. WPA2 (RADIUS), wenn nicht möglich WPA2-PSK) bietet eine höhere Sicherheit. Es muss zudem damit gerechnet werden, dass gewisse Endgeräte Probleme mit dem Zugriff auf eine versteckte SSID haben können.

5.2 Maßnahmen zur Steigerung der WLAN-Sicherheit

5.2.1 Die IEEE 802.11i-Erweiterung

Das WEP-Verfahren verbirgt einige Schwachstellen, sodass diese Art der Verschlüsselung nicht mehr als zuverlässig betrachtet wird.

Das IEEE hat diese Sicherheitsrisiken erkannt und entsprechend reagiert. Es wurde eine neue Arbeitsgruppe für eine Erweiterung des 802.11i-Standards gegründet, die sich mit der Sicherheit der Datenübertragung über WLANs, insbesondere mit der Definition von Verschlüsselungsalgorithmen und Integritätsprüfungen[18] für die drahtlose Übertragung, befasst.
Ziel der IEEE 802.11i-Erweiterung ist die Entwicklung von standardisierten Sicherheitsverfahren für die drahtlose Datenübertragung, die den heutigen Sicherheitsansprüchen gerecht werden.

Das Ergebnis waren drei Verfahren:

- TKIP („Temporary Key Integrity Protocol“) als Übergangslösung für ältere WLAN-Geräte.
- AES-CCMP („Advanced Encryption Standard“, “CTR / CBC-MAC Protocol”) als endgültiges Verschlüsselungsverfahren, das heute von der NIST („National Institute of Standards and Technology“) empfohlen wird.
- AKM („Authentication and Key Management“) zur Sicherstellung einer eindeutigen Authentifizierung in einem WLAN.

TKIP

Mit TKIP wurde von der Arbeitsgruppe ein optionales Verschlüsselungsverfahren entwickelt, das zwar auf dem bestehenden WEP-Verfahren aufbaut, dessen Sicherheitslücken aber weitgehend behebt. Diese Übergangslösung war nötig, um den Betrieb älterer WLAN-Geräte in einem Netzwerk zu gewährleisten.

Das „Temporal Key Integrity Protocol“ benutzt zur Codierung einer Nachricht einen Schlüssel sowie einen zusätzlichen Initialisierungsvektor. Durch verschiedene Kombinationen von Ausgangsschlüssel und Initialisierungsvektor wirkt die Codierung, als werde der Schlüssel ständig gewechselt, was das Brechen des Codes erschwert.

Die Integritätsprüfung (MIC; „Message Integrity Check“) erfolgt über einen speziellen HASH-Algorithmus, der als „Michael“ bezeichnet wird.

[18] Durch eine Integritätsprüfung kann eine Datenmanipulation während der Datenübertragung ausgeschlossen werden.

AES-CCMP

AES-CCMP ist das endgültige Verfahren zur Verschlüsselung der Daten in einem WLAN.

Dieses Verfahren erfordert neue WLAN-Chipsätze und ist somit auf älteren WLAN-Produkten nicht einsetzbar.

AES-CCMP praktiziert wie WEP das „Aufaddieren“ eines Schlüssels auf die Nachricht. Zwar wird hier jeweils ein Block der Rohdaten mit jeweils demselben Schlüssel verarbeitet, dafür finden mehrere Verarbeitungsdurchgänge mit jeweils variierenden Blockgrenzen statt.

Die Berechnung der Integritätsprüfung (MIC; „Message Integrity Check“) erfolgt über temporäre Schlüssel. In diese Schlüssel ist die MAC-Adresse (d. h. die eindeutige Hardware-Identifikation) des Senders eingearbeitet, wodurch die Absender-Fälschung von Nachrichten zusätzlich erschwert wird.

Hinweis Aufgrund der steigenden Sicherheitsanforderungen wird bei iPCF und iPCF-MC nur noch das Verschlüsselungsverfahren AES unterstützt

AKM

Neben den Definitionen für eine sichere Datenübertragung und Prüfung der Frame-Integrität sieht die IEEE 802.11i-Erweiterung auch erweiterte Authentifizierungsmaßnahmen und Algorithmen für ein automatisches Schlüsselmanagement vor. Als Authentifizierungsverfahren dienen die Standards von IEEE 802.11X oder ein PSK („Pre-Shared Key“) (siehe Kapitel 5.3).

5.2.2 Sicherheitsstandard Wi-Fi Protected Access

Die Erarbeitung eines Verschlüsselungsalgorithmus, der WEP ablösen sollte, durch die IEEE-Arbeitsgruppe 802.11i verzögerte sich, sodass die „Wi-Fi-Alliance“ als Zwischenlösung die Anwendung von WPA („Wi-Fi Protected Access“) mit TKIP als einer Untermenge des 802.11i-Standards empfahl.

Als Authentifizierung lässt WPA zwei Möglichkeiten zu:

- WPA (RADIUS): Die Authentifizierung durch einen Server (RADIUS-Server) ist bei WPA (RADIUS) fest vorgeschrieben (siehe Kapitel 5.3.1). Durch den dynamischen Austausch der Schlüssel bei jedem Datenframe wird eine weitere Sicherheit eingebaut.
- WPA-PSK: Bei diesem Verfahren wird keine Authentifizierung durch einen Server durchgeführt, sondern anhand eines Passworts (siehe Kapitel 5.3.2). Dieses Passwort wird auf dem Client wie auf dem Server manuell konfiguriert.

Mit der inzwischen erfolgten Verabschiedung des 802.11i-Standards ist dies jedoch hinfällig und die Wi-Fi Alliance hat WPA2 („Wi-Fi Protected Access 2) als neuen Sicherheitsstandard ins Leben gerufen. Die Verschlüsselung bei WPA2 orientiert sich an der vollständigen Implementierung der IEEE 802.11i-Erweiterung und nutzt AES-CCMP.

Analog zu WPA kann die Authentifizierung über einen Authentifizierungsserver oder PSK erfolgen.

Hinweis Der Übertragungsstandard IEEE 802.11n mit der Einstellung „802.11n" oder „802.11n only" unterstützt bei den Sicherheitseinstellungen nur WPA2/ WPA2-PSK mit AES.

5.3 Authentifizierung und Schlüsselmanagement

5.3.1 IEEE 802.1X-Authentifizierung

Im Standard IEEE 802.1X ist nicht die Verschlüsselung des Datenverkehrs zwischen Access Point und Client definiert, sondern das Anmeldeverfahren sowie die Vergabe von Zugriffsrechten für Clients. Hierfür wird das RADIUS-Protokoll auf Basis „EAP“ („Extensible Authentication Protocol“) für größere Netze und PSK in Büronetze eingesetzt.

RADIUS-Protokoll

Das RADIUS-Protokoll („Remote Authentication Dial In User Service“) für die Authentifizierung am Netz wurde ursprünglich für kabelgebundene Systeme entwickelt, hat sich jedoch auch und besonders im Funkbereich bewährt.

Bei RADIUS existiert ein zentraler sog. RADIUS-Server, der eine Liste mit den Zugangsberechtigungen aller Teilnehmer enthält. Will sich ein Client am Netz anmelden, so leitet der Access Point die Anfrage an den RADIUS-Server weiter. Dieser reagiert darauf, indem er eine „Challenge“ generiert, d. h. eine Anfrage, zu welcher der Client nur dann die passende „Response“ senden kann, wenn er über das auf dem RADIUS-Server gespeicherte Passwort verfügt.

Dieses Verfahren hat zwei Vorteile:

- Das Passwort wird nie im Klartext über das Netz gesendet, es kann also auch nicht von einem Unbefugten abgefangen werden.
- Dadurch, dass die Zugangsberechtigungen auf einem zentralen Server gespeichert werden, ist das Verfahren besonders geeignet, wenn roamende Clients verwendet werden. Es müssen nicht alle Access Points die Zugangsdaten der Clients vorhalten, sondern sie können diese jederzeit beim RADIUS-Rechner abfragen.

EAP

Hinter der Abkürzung EAP verbirgt sich ein verbreitetes Framework für verschiedene Authentifizierungsverfahren für den Netzwerkzugang. Mit anderen Worten, EAP selbst stellt keine Authentifizierungsmethode dar, sondern beschreibt den Mechanismus, nach dem sich Client und Server auf eine Methode einigen können.

Eine der Methoden, die unter EAP eingesetzt werden können, ist „EAP-TLS“ („EAP-Transport Layer Security“), bei der die Netzwerkteilnehmer vor der Zulassung zum Netzwerkverkehr „zertifiziert“, d. h. bei einem zentralen Server beglaubigt, werden müssen. Das Verfahren ist hierbei dem aus dem Internet geläufigen SSL vergleichbar.

Daneben existiert noch eine Vielzahl anderer, teils herstellerspezifischer Protokolle, die unter EAP genutzt werden können.

5.3.2 Pre-Shared Key (PSK)

Der Pre-Shared Key ist eine Alternative zur RADIUS-Authentifizierung und wird unter anderem aus einem fest definierten Schlüssel gebildet, der vor der Kommunikation den Teilnehmern bekannt sein muss.

Weitere Parameter für die Bildung des PSK sind die SSID und die SSID-Länge.

5.4 Sicherheitsfunktionen und Datenrate

Beachten Sie, dass die Verschlüsselungsverfahren mit zunehmender Komplexität einen steigenden Overhead in der Übertragung erzeugen und mehr Rechenzeit bei den Teilnehmern verschlingen, wodurch die effektive Datenrate reduziert werden kann.

Muss ein WLAN mit sehr hoher Performanz (Datendurchsatz und Reaktionszeiten, z. B. PROFINET I/O) betrieben werden, so kann es nötig werden, auf ein weniger sicheres, aber auch ressourcenschonenderes Verschlüsselungsverfahren zurückzugreifen.

Weitere Informationen spezifisch für die SCALANCE W-Geräte finden Sie unter Kapitel 8.1.2.

Hinweis

Beachten Sie folgende Hinweise, um ihr Netz vor Angriffen zu schützen:

● Verwenden Sie eine sichere Verbindung mit HTTPS. HTTPS ermöglicht Ihnen im Gegensatz zu HTTP einen sicheren Zugang zur Konfiguration der WLAN Clients und der Access Points über das Web Based Management.

● Verwenden Sie WPA2/ WPA2-PSK mit AES um einen Passwortmissbrauch zu verhindern. WPA2 / WPA2-PSK mit AES bietet die größte Sicherheit.

● Schützen Sie ihr Netz vor Man-in-the-Middle-Angriffen durch einen Netzaufbau, der es dem Angreifer erschwert, sich in den Kommunikationsweg zwischen zwei Endgeräten einzuschalten:

- WLAN-Geräte können Sie z. B. dadurch schützen, indem der Agent IP nur über ein eigenes Management VLAN zugänglich ist.
- Eine weitere Möglichkeit besteht darin, am WLAN Client / Access Point ein eigenes HTTPS-Zertifikat zu installieren. Das HTTPS-Zertifikat überprüft die Identität des Geräts und regelt den verschlüsselten Datenaustausch. Sie können das HTTPS-Zertifikat z. B. über HTTP installieren.

● Verwenden Sie SNMPv3. SNMPv3 bietet durch Ihnen die größtmögliche Sicherheit beim Zugriff auf die WLAN-Geräte über SNMP.

6 Koexistenz von IWLANs mit anderen Funknetzen

Mögliche Störquellen des Betriebs

Im Industrieumfeld existieren prinzipiell drei Arten von Störquellen, die die Funktion eines IWLANs beeinträchtigen können:

- Eine Umgebung mit Hindernisse und Gegenstände, die die Ausbreitung der Funkwellen beeinflussen (z. B. Metall etc.),
- andere Funksender, die dasselbe Frequenzband nutzen (andere WLAN-Teilnehmer, aber auch Bluetooth, etc.),
- Geräte, die unspezifische Störimpulse senden (Schweißgeräte, Schaltgeräte).

Da das 2,4-GHz-Band von mehr Funksystemen als das 5-GHz-Band benutzt wird, ist im 2,4-GHz-Band auch mit größeren Schwierigkeiten im Betrieb zu rechnen.

Koexistenzmanagement

„Funk“ als solches ist eine knappe Ressource. Aufgrund seiner Natur als „Shared Medium“ ist es nicht möglich, die Kapazität zu erhöhen, indem z. B. einfach mehr Kabel verlegt werden. Durch ein vorausschauendes Koexistenzmanagement ist es jedoch möglich, diese Ressource optimal zu nutzen, womit in den meisten Fällen den Anforderungen industrieller Anwendung genügt wird.

Für das Koexistenzmanagement sollte immer ein Experte zurate gezogen werden.

Funkanalyse

Als erster Schritt sollte immer eine Funkanalyse der Umgebung stehen. In dieser werden die einzelnen Sender mit den verschiedenen Kriterien erfasst:

- Auf welchen Frequenzen arbeitet der Sender?
- Ist seine Anwendung zeit- oder sicherheitskritisch?
- Wie groß ist das zu übertragende Datenvolumen?
- Erfolgt die Übertragung zyklisch, sporadisch oder kontinuierlich?
- Wo sind die Teilnehmer stationiert?

Das Prinzip der Entkopplung

Die einzelnen Funkfelder werden ungestört voneinander arbeiten können, wenn sie in wenigstens einer der vier Domänen „entkoppelt“, d. h. voneinander getrennt sind:

- Raum
- Frequenz
- Zeit
- Code

Die **räumliche Entkopplung** wird erzielt, indem die Überlappung zwischen den verschiedenen Funksystemen möglichst gering gehalten wird. Dies wird erreicht, indem die Sendeleistung auf das notwendige Minimum reduziert wird (keine Überreichweiten), durch die Wahl geeigneter Antennen (Richtantennen oder omnidirektional, vgl. Kapitel 9.3), sowie eine Optimierung des Aufstellungsorts von Access Points und Clients, soweit dies im Rahmen der Funktion der Anlage möglich ist.

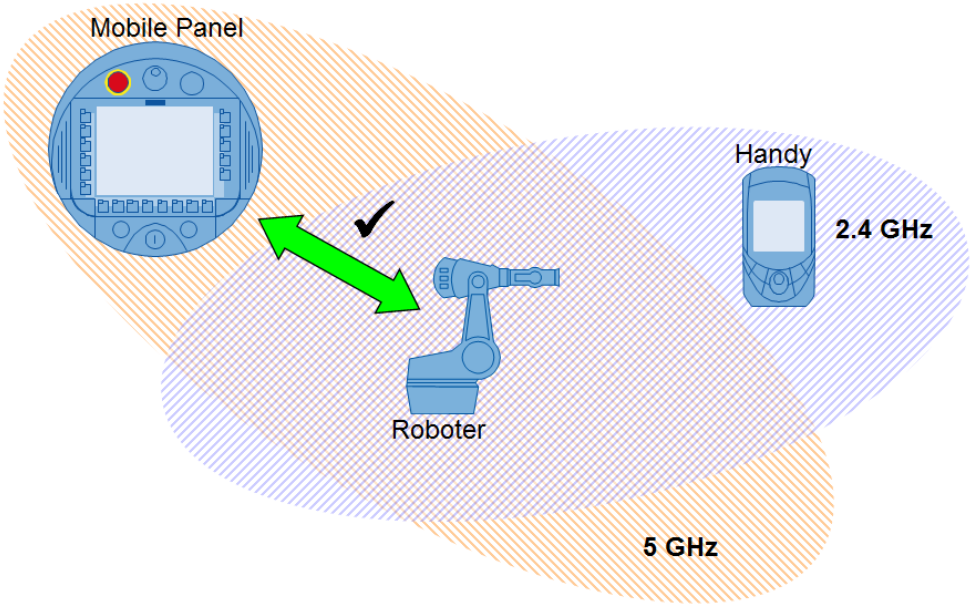
Für die **Frequenzentkopplung** ist entscheidend, dass die Frequenzbereiche der einzelnen Funksysteme sich möglichst wenig überschneiden. Im einfachsten Fall geschieht dies durch die Wahl entsprechender Funkkanäle, im fortgeschrittenen Fall wird dies durch Modulations- und Multiplexverfahren (siehe Kapitel 1.6) wie z. B. MIMO erreicht.

Für die **zeitliche Entkopplung** schließlich ist die Konfiguration der einzelnen Teilnehmer entscheidend. Diese muss so gewählt sein, dass die Wahrscheinlichkeit, dass eine zeitkritische Übertragung wie PROFINET I/O mit einer anderen Sendung zusammenfällt, möglichst gering wird. (Vorstellbar ist beispielsweise, einen Kanal ausschließlich für zeitkritische Übertragungen zu reservieren, soweit das praktisch realisierbar ist.)

Bei der **Code Entkopplung** steht die Trennung und Unterscheidung unterschiedlicher und parallel übertragener Datenströme über ein gemeinsames genutztes Frequenzband im Vordergrund. Zur Unterscheidung werden die Datenströme der Teilnehmer mit jeweils eigenen und individuellen Spreizcodes codiert (orthogonale Codes). So kann am Empfänger eindeutig ermittelt werden, welches Signal welchem Anwender gehört.

Die folgende Grafik zeigt ein Beispiel zur Entkopplung im Frequenzbereich: Das MP277 Mobile Panel kann mit dem Roboter kommunizieren, obwohl dieser sich gleichzeitig im Sendebereich des Handys befindet, da beide auf verschiedenen Frequenzen (orange: 5 GHz, lila: 2,4 GHz) kommunizieren.
Obwohl sich die Felder räumlich und zeitlich überschneiden, sind sie in der Frequenzdomäne entkoppelt.

Abbildung 6-1



Hinweis Weitere Informationen zu diesem Thema finden Sie im Web in der folgenden Broschüre, die vom „ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V“[19] herausgegeben wurde:
ZVEI_Koexistenz_von_Funksystemen_in_der_Automatisierungstechnik.
Die einzelnen Schritte des Koexistenzmanagements sind zusammengefasst in der VDI/VDE-Richtlinie 2185 (kostenpflichtiger Download)
"Funkgestützte Kommunikation in der Automatisierungstechnik"

7 Länderzulassungen

7.1 Allgemeines

Nicht alle Funkmodi sind in allen Ländern zugelassen. National unterschiedliche Beschränkungen für zugelassene Konfigurationen können sich unter anderem beziehen auf:

- Erlaubte Frequenzbänder und -kanäle,
- Maximale Sendeleistung,
- Indoor- / Outdoor-Betrieb,
- 802.11-Standards („a“, „b“, „g“, „h“, „n”, „Turbo”),
- Spezifische Verfahren zur Verbesserung der Übertragungsqualität wie DFS und TCP (Vgl. Kapitel 2.3.1)

Sind Sie bei der Projektierung Ihres Netzwerks auf eine bestimmte Konfiguration angewiesen, so ziehen Sie Ihren Siemens-Kundenbetreuer zu rate.

Betroffene Komponenten

Ein Funknetz wird als „Gesamtheit“ betrachtet, in der für alle teilnehmenden Systeme die jeweiligen Zulassungen vorliegen müssen. Primär sind das alle aktiven Komponenten, die direkten Einfluss auf das Netzwerk ausüben können, wie:

- Access Points,
- Clients (inklusive Interface-Module)
- mobile Bediengeräte (vgl. Kapitel 8.7)
- Antennen

Hinweis Passive Komponenten (z. B. Netzwerk-Sniffer-Software, Stromversorgungen) haben keine eigene Zulassung, sondern werden im System zusammen mit den Access Points und Clients zugelassen. Nähere Informationen finden Sie in der Länderliste unter http://www.siemens.de/funkzulassungen.

Verantwortlichkeit

Prinzipiell liegt die Verantwortung für den ordnungsgemäßen Betrieb einer Funkanlage beim *Betreiber*, und nicht beim Hersteller. Technisch ist es jederzeit möglich, ein Gerät, das eine Funkzulassung in einem Land besitzt, so zu konfigurieren, dass es im tatsächlichen Betrieb die Standards in diesem Land verletzt.

[19] www.zvei.org

7.2 Länderzulassungen in den SCALANCE W-Geräten

In der Firmware jedes SCALANCE W-Geräts (vgl. Kapitel 8.1.2) sind die nationalen Standards hinterlegt, die zum Zeitpunkt der Veröffentlichung der Firmware aktuell waren. Diese Standards können über das Web-Interface des Access Points oder Clients im Menü „System“ > „Load&Save“ ausgelesen werden.

Hinweis Aktuelle Beschreibungen finden Sie im Handbuch des jeweiligen Gerätes. Diese finden Sie im Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/de/ps/15853/man

Beachten Sie, dass diese Liste nur zu Ihrer Information dient, aber nicht mit einer Funktionseinschränkung des jeweiligen Geräts verbunden ist: Es ist ohne weiteres möglich, einen Access Point oder Client mit einem im jeweiligen Land nicht zugelassenen Funkmodus zu betreiben. In Ländern, die nicht in der Countrylist auftauchen, ist der Betrieb der SCALANCE W-Geräte prinzipiell nicht erlaubt.

Der folgende Screenshot zeigt eine mögliche Länderzulassungsliste aus einem Access Point. Hier ein Auszug mit den Einträgen der in Italien zugelassenen Funkmodi.

Abbildung 7-1

	DFS+TPC	136	5680	1000mW	Indoor+Outdoor
	DFS+TPC	140	5700	1000mW	Indoor+Outdoor
COUNTRY	MODE	CH	MHz	PWR(EIRP)	USAGE
ITALY	11b 11g g-Turbo				
		1	2412	100mW	Indoor+Outdoor
		2	2417	100mW	Indoor+Outdoor
		3	2422	100mW	Indoor+Outdoor
		4	2427	100mW	Indoor+Outdoor
		5	2432	100mW	Indoor+Outdoor
		6	2437	100mW	Indoor+Outdoor
		7	2442	100mW	Indoor+Outdoor
		8	2447	100mW	Indoor+Outdoor
		9	2452	100mW	Indoor+Outdoor
		10	2457	100mW	Indoor+Outdoor
		11	2462	100mW	Indoor+Outdoor
		12	2467	100mW	Indoor+Outdoor
		13	2472	100mW	Indoor+Outdoor
	11a				
	TPC	36	5180	60mW	Indoor Only
	TPC	40	5200	60mW	Indoor Only
	TPC	44	5220	60mW	Indoor Only
	TPC	48	5240	60mW	Indoor Only
	11h				
	DFS+TPC	36	5180	200mW	Indoor Only
	DFS+TPC	40	5200	200mW	Indoor Only
	DFS+TPC	44	5220	200mW	Indoor Only
	DFS+TPC	48	5240	200mW	Indoor Only
	DFS+TPC	52	5260	200mW	Indoor Only
	DFS+TPC	56	5280	200mW	Indoor Only
	DFS+TPC	60	5300	200mW	Indoor Only
	DFS+TPC	64	5320	200mW	Indoor Only
	DFS+TPC	100	5500	1000mW	Indoor+Outdoor
	DFS+TPC	104	5520	1000mW	Indoor+Outdoor
	DFS+TPC	108	5540	1000mW	Indoor+Outdoor
	DFS+TPC	112	5560	1000mW	Indoor+Outdoor
	DFS+TPC	116	5580	1000mW	Indoor+Outdoor
	DFS+TPC	120	5600	1000mW	Indoor+Outdoor
	DFS+TPC	124	5620	1000mW	Indoor+Outdoor
	DFS+TPC	128	5640	1000mW	Indoor+Outdoor
	DFS+TPC	132	5660	1000mW	Indoor+Outdoor
	DFS+TPC	136	5680	1000mW	Indoor+Outdoor
	DFS+TPC	140	5700	1000mW	Indoor+Outdoor
COUNTRY	MODE	CH	MHz	PWR(EIRP)	USAGE
JAPAN	11b 11g				
		1	2412	100mW	Indoor+Outdoor
		2	2417	100mW	Indoor+Outdoor

Hinweis Aktualisierte Listen mit Länderzulassungen für die einzelnen SCALANCE W-Produkte finden Sie im Handbuch „SIMATIC NET Industrial Wireless LAN Zulassungen SCALANCE W700 802.11n“ unter der Beitrags-ID: 109476834.

8 SIMATIC NET-Produkte für den Aufbau eines IWLANs

8.1 Allgemeine Informationen

8.1.1 Übersicht der Produktpalette

Für den Aufbau eines sicheren und zuverlässigen WLANs bietet SIEMENS eine breite Produktpalette an. Die nächsten Kapitel stellen diese mit ihren Eigenschaften vor und zeigen die Anwendung und den praktischen Nutzen.

Das folgende Bild zeigt eine Auswahl von SIMATIC-Wireless-Produkte.

Abbildung 8-1

Hinweis Weitere ständig aktualisierte Informationen zu SCALANCE W-Produkten finden Sie unter: http://www.siemens.de/iwlan

8.1.2 Einteilung der SCALANCE W-Produkte

Bei der SCALANCE W-Produktreihe („Wireless“) handelt es sich um Komponenten für die Verbindung von Industrial Ethernet und WLAN in industriellen Umgebungen.

Die Familie der SCALANCE W-Geräte umfasst die Produkte:

- IWLAN-Controller,
- Access Points und
- Client-Module.

Der IWLAN-Controller

Der IWLAN-Controller SCALANCE WLC711 ist ein Netzwerkgerät für das zentrale Management eines Wireless LAN im industriellen Umfeld. Er unterstützt bei der Inbetriebnahme, der Diagnose, der Zugangskontrolle und den Sicherheitseinstellungen des Drahtlosnetzwerkes sowie bei Firmwareupdates der Access Points.

Hinweis Weitere und detailliertere Informationen zum SCALANCE WLC711 finden Sie im Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/de/ps/15870/man

Die Access Points

Die W78x-, W77x- und W76x-Baugruppen sind dabei Access Points, die als Netzwerk-Switches der einzelnen Funkzellen sowie als Übergänge zwischen Industrial Ethernet- und WLAN-Abschnitten dienen. Zu den Baugruppen gehören zwei unterschiedliche Varianten von Access Points:

- Standalone Access Points
- Controller-basierte Access Points

Hinweis Handbücher zu den SCALANCE Access Points finden Sie im Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/de/ps/15860/man

Die Client-Module

Die Client-Baugruppen tragen die Bezeichnung „W74x“, „W78x“ und „W73x“. Sie werden über Ethernet an mobile Endteilnehmer angeschlossen und kommunizieren über die Access Points miteinander.

Hinweis Handbücher zu den SCALANCE Clients finden Sie im Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/de/ps/15882/man

8.2 IWLAN-Controller SCALANCE WLC711

Der SCALANCE WLC711 ist eine Netzwerkinstanz für das zentrale Management eines Wireless LAN im industriellen Umfeld. Er unterstützt bei der Inbetriebnahme, der Diagnose, der Zugangskontrolle und den Sicherheitseinstellungen des Drahtlosnetzwerkes sowie bei Firmwareupdates der Access Points.

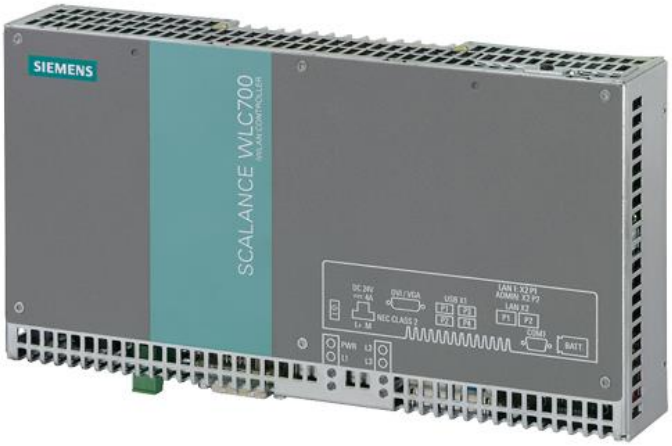
Am SCALANCE WLC711 können ausschließlich Controller-basierte Access Points betrieben werden.

Allgemeines

Die Anforderungen an WLAN im industriellen Bereich, sowie die Vielfalt der möglichen Applikationen und Anwendungen sind in den letzten Jahren ständig gestiegen. Aspekte wie höhere Leistungsfähigkeit und Datenrate sowie geringerer Managementaufwand des Netzes stellen heute neue Herausforderungen. Als Antwort hat sich eine weitere Architektur in WLAN-Netzen im Office Bereich seit Jahren etabliert: die Controller-basierte Architektur.
Bei dieser Architektur werden die Access Points nicht mehr als Standalone betrieben, sondern von einem IWLAN-Controller gesteuert. Über den Controller können die Managementdaten sowie die Nutzdaten an und von den einzelnen Access Points übertragen werden.

Mit dem SCALANCE WLC711 bietet das Portfolio von SIMATIC NET die Möglichkeit eines Controller-basierten IWLANs.

Abbildung 8-2



Hardware-Basis

Die Hardwarebasis ist ein lüfterloser Industrie-PC mit zwei getrennten Gigabit-Ethernet-Schnittstellen:

- Management-Port: Über diesen Port wird der Controller konfiguriert.
- Daten-Port: An diesem werden die Daten übermittelt.

Merkmale

Der SCALANCE WLC711 zeichnet sich durch folgende Merkmale aus:

- Zentrale Konfiguration und Firmware-Hochrüsten der Access Points über ein User-Interface im Controller.
- Überwachung größerer WLAN-Netze: Der IWLAN-Controller bietet über das „Wireless Assistant Home Screen“ die Möglichkeit, das Netzwerk in Echtzeit im Bildschirm zu überwachen.
- Zuweisen von Eigenschaften an Gruppen von Anwendern, Geräten und Diensten.
- Rollenbasierte Sicherheitsfunktionen (Authentifizierung, Intrusion Detection, Rogue AP Detection, Firewalls, usw.).
- Schnelles Layer2 und Layer3-Roaming (z. B. für Logistik-Scanner und VoIP).
- Erweiterte QoS-Funktionen gewährleisten IP-Priorisierung Ende-zu-Ende für Voice, Video & Data.
- RF-Management (automatisches Einstellen von Kanälen und Sendeleistung).
- Zuverlässiges Meshed-WLAN durch redundante Pfade: Bei dem Ausfall einer Verbindung oder eines Access Points werden das Netzwerk und die Paket-Route automatisch neu konfiguriert.
- Internes und externes Captive Portal (Gästeportal): Der Gast wird automatisch zu einer Login Website weitergeleitet, wo er seine Login-Daten eingeben muss.

Hinweis Weitere und detailliertere Informationen zum SCALANCE WLC711 finden Sie im Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/de/ps/15870/man

8.3 Standalone SCALANCE W Access Points

Standalone bedeutet, dass die Access Points einzeln konfiguriert werden und es keine höhere Instanz gibt, die das Netzwerk steuern kann.
Die Access Points nach IEEE 802.11n können sowohl im 2,4-GHz-Band als auch im 5-GHz-Band arbeiten (siehe Kapitel 2.2.4).
Durch den Einsatz spezieller Mechanismen und neuer Technologien sind hier ein Datendurchsatz bis zu 450 Mbit/s (brutto) und eine bessere Funkabdeckung möglich.

Pro Funkmodul können bis zu drei Antennen angeschlossen werden. Damit wird der Datenstrom auf bis zu drei Sendeantennen verteilt (spatial multiplexing).

Hinweis

Mit der Umsetzung des neuen WLAN-Standard 802.11n in den SCALANCE W-Produkten wurden die Baugruppen komplett innoviert und alle alten Geräte abgekündigt. Die neuen Geräte können nicht als Ersatzteil für die alten Geräte eingesetzt werden.

Der folgende FAQ zeigt, welche SCALANCE W-Produkte mit Standard 802.11n die alten Geräte ohne Standard 802.11n ablösen.
https://support.industry.siemens.com/cs/ww/de/view/109479635

Access Points SCALANCE W788-x RJ45

Die SCALANCE W788-x RJ45-Module sind nach Schutzklasse IP30 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Die Ethernet-Schnittstelle ist elektrisch (RJ45) ausgeführt, Gigabit-fähig und ermöglicht Power-over-Ethernet.

Für den Anschluss der externen Antennen sind R-SMA Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-3

Der SCALANCE W788-x RJ45 ist in folgenden Varianten bestellbar:

- W788-1 RJ45 mit einer Funkschnittstelle
  - MLFB: 6GK5788-1FC00-0AA0 bzw.
  - MLFB: 6GK5788-1FC00-0AB0 (US-Variante)
- W788-2 RJ45 mit zwei voneinander unabhängigen Funkschnittstellen
  - MLFB: 6GK5788-2FC00-0AA0 bzw.
  - MLFB: 6GK5788-2FC00-0AB0 (US-Variante)

Access Points SCALANCE W788-x M12 (EEC)

Der SCALANCE W788-x M12 ist in zwei Ausführungen erhältlich:

- Die Standard-Variante W788-x M12
- Die EEC-Variante W788-x M12 EEC (Enhanced Environment Conditions)

Beide Access Points verfügen über die IP65 Schutzklasse und eignen sich für die Montage in Innenbereichen innerhalb von Industrieumgebungen mit besonders anspruchsvollen Umgebungsbedingungen.

Zusätzlich kann die EEC-Variante in hochperformanten Anlagennetzen und Applikationen mit hohen Temperatur- oder EMV-Anforderungen eingesetzt werden.

Die Ethernet-Schnittstelle ist elektrisch (M12) ausgeführt. Für den Anschluss der externen Antennen sind robuste N-Connect Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-4

Der SCALANCE W788-x M12 ist in folgenden Varianten bestellbar:

- W788-1 M12 mit einer Funkschnittstelle
  - MLFB: 6GK5788-1GD00-0AA0 bzw.
  - MLFB: 6GK5788-1GD00-0AB0 (US-Variante)
- W788-2 M12 mit zwei voneinander unabhängigen Funkschnittstellen
  - MLFB: 6GK5788-2GD00-0AA0 bzw.
  - MLFB: 6GK5788-2GD00-0AB0 (US-Variante)
- W788-2 M12 EEC mit zwei voneinander unabhängigen Funkschnittstellen
  - MLFB: 6GK5788-2GD00-0TA0 bzw.
  - MLFB: 6GK5788-2GD00-0TB0 (US-Variante)

Access Points SCALANCE W786-x RJ45/SFP

Die SCALANCE W786-x RJ45/SFP Access Points sind durch die Schutzklasse IP65 konzipiert für den Einsatz innerhalb von Industrieumgebungen mit besonders anspruchsvollen Umgebungsbedingungen, in öffentlichen Räumen oder außerhalb von Gebäuden. Zu den wichtigen Eigenschaften zählen die Unempfindlichkeit gegen extreme Witterungseinflüsse wie Salzwassersprühnebel, aber auch die robuste Bauweise im schlag- und stoßfesten Kunststoffgehäuse ohne nach außen durchgeführte zerstörbare Teile.

Die Ethernet-Schnittstelle ist dabei entweder als RJ45 oder SFP ausgeführt.

SFP-Interface-Module (Small Form-Factor Pluggable) sind kleine kompakte und steckbare Transceiver-Module und bilden die physikalische Schnittstelle zwischen dem Übertragungsmedium und Gigabit-Ethernet. SPF-Module werden für verschiedene Lichtwellenleiter angeboten.

Hinweis Weitere Informationen zu SFP finden Sie in der Betriebsanleitung zum SCALANCE W786 im Siemens Industry Online Support (Beitrags-ID:62521860): http://support.automation.siemens.com/WW/view/de/62521860

Für den Anschluss der externen Antennen sind R-SMA Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-5

Der SCALANCE W786-x RJ45/SFP ist in folgenden Varianten bestellbar:

- W786-1 RJ45 mit einer Funkschnittstelle und externen Antennen
  - MLFB: 6GK5786-1FC00-0AA0 bzw.
  - MLFB: 6GK5786-1FC00-0AB0 (US-Variante)
- W786-2 RJ45 mit zwei voneinander unabhängigen Funkschnittstellen und externen Antennen
  - MLFB: 6GK5786-2FC00-0AA0 bzw.
  - MLFB: 6GK5786-2FC00-0AB0 (US-Variante)
- W786-2IA RJ45 mit zwei voneinander unabhängigen Funkschnittstellen und internen Antennen
  - MLFB: 6GK5786-2HC00-0AA0 bzw.
  - MLFB: 6GK5786-2HC00-0AB0 (US-Variante)
- W786-2 SFP mit zwei voneinander unabhängigen Funkschnittstellen und externen Antennen
  - MLFB: 6GK5786-2FE00-0AA0
  - MLFB: 6GK5786-2FE00-0AB0 (US-Variante)

Access Points SCALANCE W774-1 RJ45

Die SCALANCE W774-1 RJ45-Module sind nach Schutzklasse IP30 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Durch das abgestimmte Gehäusedesign sind sie optimal kombinierbar mit bestehenden SIMATIC-Produkten im Schaltschrank
(z.B. ET200SP, ET200MP, …).

Die beiden Ethernet-Schnittstellen sind elektrisch (RJ45) ausgeführt, wovon eine geeignet ist für die Einspeisung über Power-over-Ethernet.

Für den Anschluss der beiden externen Antennen sind R-SMA Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-6

Der SCALANCE W774-1 RJ45 ist in folgenden Varianten bestellbar:

- MLFB: 6GK5774-1FX00-0AA0 bzw.
- MLFB: 6GK5774-1FX00-0AB0 (US-Variante)

Access Points SCALANCE W774-1 M12 EEC

Der SCALANCE W774-1 M12 EEC (Extended Environmental Conditions) verfügt über die IP30 Schutzklasse und eignet sich für den Einsatz in Umgebungen mit erweiterten Umgebungsbedingungen.

Aufgrund des robusten Gehäusematerials (Aluminium) sowie der kompakten Bauform, sind die SCALANCE W774-1 M12 EEC Produkte besonders für den Einsatz im Fahrzeug oder Schaltschrank geeignet. Sie erfüllen die Zulassung EN 50155 für Bahnanwendungen und die Zulassung E1 für die Verwendung in Kraftfahrzeugen.

Durch das abgestimmte Gehäusedesign sind sie optimal kombinierbar mit bestehenden SIMATIC-Produkten.

Die Ethernet-Schnittstelle ist elektrisch (M12) ausgeführt. Für den Anschluss der externen Antennen sind zwei Antennen-Anschlüsse vom Typ R-SMA vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-7

Der SCALANCE W774-1 M12 EEC ist in folgenden Varianten bestellbar:

- MLFB: 6GK5774-1FY00-0TA0 bzw.
- MLFB: 6GK5774-1FY00-0TB0 (US-Variante)

Access Points SCALANCE W761-1 RJ45

Die SCALANCE W761-1 RJ45-Module sind nach Schutzklasse IP20 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Durch das abgestimmte Gehäusedesign sind sie optimal kombinierbar mit bestehenden SIMATIC-Produkten im Schaltschrank
(z.B. ET200SP, ET200MP, …).

Die Ethernet-Schnittstelle ist elektrisch (RJ45) ausgeführt. Für den Anschluss der externen Antenne ist eine R-SMA Buchse vorgesehen.

Abbildung 8-8

Der SCALANCE W761-1 RJ45 ist in folgenden Varianten bestellbar:

- MLFB: 6GK5761-1FC00-0AA0 bzw.
- MLFB: 6GK5761-1FC00-0AB0 (US-Variante)

8.4 Controller-basierte SCALANCE W Access Points

Controller-basierte Access Points können nur in einem Netzwerk mit einem IWLAN-Controller eingesetzt werden, da sie dessen zentrale Managementfunktionen benötigen.

Die Controller-basierten Access Points nach dem IEEE 802.11n-Standard arbeiten sowohl im 2,4-GHz-Band als auch im 5-GHz-Band.

Sie sind hinsichtlich Bauform und Funktionalität identisch mit den Standalone Access Points für IEEE 802.11n (siehe Kapitel 0). Im Gegensatz zu diesen können die Controller-basierten Access Points nur in Verbindung mit einem Controller eingesetzt werden.

Folgende Controller-basierte Access Points sind aus dem Produktportfolio bestellbar:

- SCALANCE W788C-2 RJ45 mit zwei voneinander unabhängigen Funkschnittstellen:
  - MLFB 6GK5788-2FC00-1AA0
- SCALANCE W788C-2 M12 mit zwei voneinander unabhängigen Funkschnittstellen:
  - MLFB 6GK5788-2GD00-1AA0
- SCALANCE W788C-2 M12 EEC mit zwei voneinander unabhängigen Funkschnittstellen:
  - MLFB 6GK5788-2GD00-1TA0
- SCALANCE W786C-2x RJ45 in folgenden Varianten:
  - W786C-2 RJ45 mit zwei voneinander unabhängigen Funkschnittstellen und externen Antennen:
    - MLFB 6GK5786-2FC00-1AA0.
  - W786C-2IA RJ45 mit zwei voneinander unabhängigen Funkschnittstellen und internen Antennen
    - MLFB 6GK5786-2HC00-1AA0
- W786C-2 SFP mit zwei voneinander unabhängigen Funkschnittstellen und externen Antennen:
  - MLFB: 6GK5786-2FE00-1AA0

8.5 SCALANCE W-Clients

Die SCALANCE W-Clients können sowohl an Standalone Access Points, als auch an Controller-basierten Access Points betrieben werden.

Die Module sind baugleich mit den korrespondierenden Access Points (siehe Kapitel 8.3). Allerdings unterscheidet sich die Software in den Funktionalitäten, sodass diese Geräte nicht für das Netzwerk-Management wie die Access Points, sondern für eine Kommunikation untereinander und mit anderen Netzwerkgeräten vorgesehen sind.

Die Clients stellen zudem die Schnittstelle zwischen Ethernet-angebundenen Geräten und dem WLAN dar. Dabei übertragen sie aber nicht den kompletten Netzwerkverkehr, sondern nur die Telegramme einer begrenzten Zahl von Ethernet-Teilnehmern.

Die Client Module nach dem IEEE 802.11n-Standard können sowohl im 2,4-GHz-Band als auch im 5-GHz-Band arbeiten.

Durch den Einsatz spezieller Mechanismen und neuer Technologien sind hier ein Datendurchsatz bis zu 450 Mbit/s (brutto) und eine bessere Funkabdeckung möglich.

Die Clients verfügen über ein Funkmodul. Hier können bis zu drei Antennen angeschlossen werden. Damit kann der Datenstrom auf bis zu drei Sendeantennen verteilen werden (spatial multiplexing).

Hinweis

Mit der Umsetzung des neuen WLAN-Standard 802.11n in den SCALANCE W-Produkten wurden die Baugruppen komplett innoviert und alle alten Geräte abgekündigt. Die neuen Geräte können nicht als Ersatzteil für die alten Geräte eingesetzt werden.

Der folgende FAQ zeigt, welche SCALANCE W-Produkte mit Standard 802.11n die alten Geräte ohne Standard 802.11n ablösen.
https://support.industry.siemens.com/cs/ww/de/view/109479635

Clients SCALANCE W748-1 RJ45

Die SCALANCE W748-1-Module sind nach Schutzklasse IP30 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Die Ethernet-Schnittstelle ist elektrisch (RJ45) ausgeführt, Gigabit-fähig und ermöglicht Power-over-Ethernet.

Für den Anschluss der drei externen Antennen sind R-SMA Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-9

Der SCALANCE W748-1 RJ45 ist in folgenden Varianten bestellbar:

- MLFB: 6GK5748-1FC00-0AA0 bzw.
- MLFB: 6GK5748-1FC00-0AB0 (US-Variante)

Clients SCALANCE W748-1 M12

Diese Clients verfügen über die IP65 Schutzklasse und eignen sich für die Montage in Innenbereichen in Industrieumgebungen.

Die Ethernet-Schnittstelle ist elektrisch (M12) ausgeführt, Gigabit-fähig und ermöglicht Power-over-Ethernet.

Für den Anschluss der drei externen Antennen sind robuste N-Connect Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-10

Der SCALANCE W748-1 M12 ist in folgenden Varianten bestellbar:

- MLFB: 6GK5748-1GD00-0AA0 bzw.
- MLFB: 6GK5748-1GD00-0AB0 (US-Variante)

Clients SCALANCE W734-1 RJ45

Die SCALANCE W734-1 RJ45-Module sind nach Schutzklasse IP30 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Durch das abgestimmte Gehäusedesign sind sie optimal kombinierbar mit bestehenden SIMATIC-Produkten im Schaltschrank
(z.B. ET200SP, ET200MP, …).

Die beiden Ethernet-Schnittstellen sind elektrisch (RJ45) ausgeführt, wovon eine geeignet ist für die Einspeisung über Power-over-Ethernet.

Für den Anschluss der beiden externen Antennen sind R-SMA Buchsen vorgesehen.

Die Baugruppe verfügt über einen PLUG-Schacht zum Stecken eines C-PLUGs bzw. KEY-PLUGs.

Abbildung 8-11

Der SCALANCE W734-1 RJ45 ist in folgenden Varianten bestellbar:

- MLFB: 6GK5734-1FX00-0AA0 bzw.
- MLFB: 6GK5734-1FX00-0AB0 (US-Variante)

Clients SCALANCE W72x-1 RJ45

Der SCALANCE W72x-1 RJ45 ist in zwei Ausführungen erhältlich:

- Die Basis-Version SCALANCE W721-1 RJ45
- Der SCALANCE W722-1 RJ45 mit Unterstützung von iPCF und NAT.

Beide Module sind nach Schutzklasse IP20 gebaut und eignen sich unter anderem sehr gut für den Schaltschrank in industriellen Umgebungen.

Der SCALANCE W722-1 ist durch die Unterstützung von iPCF zudem geeignet für drahtlose PROFINET IO Kommunikation.

Durch das abgestimmte Gehäusedesign sind sie optimal kombinierbar mit bestehenden SIMATIC-Produkten im Schaltschrank (z.B. ET200SP, ET200MP, …).

Die Ethernet-Schnittstelle ist elektrisch (RJ45) ausgeführt. Für den Anschluss der externen Antenne ist eine R-SMA Buchse vorgesehen.

Abbildung 8-12

Der SCALANCE W72x-1 RJ45 ist in folgenden Varianten bestellbar:

- W721-1 RJ45 mit Basis-Funktion
  - MLFB: 6GK5721-1FC00-0AA0 bzw.
  - MLFB: 6GK5721-1FC00-0AB0 (US-Variante)
- W722-1 RJ45 mit zusätzlicher iPCF- und NAT-Funktion
  - MLFB: 6GK5722-1FC00-0AA0 bzw.
  - MLFB: 6GK5722-1FC00-0AB0 (US-Variante)

8.6 Konfiguration der SCALANCE W-Geräte

Die SCALANCE W700 Access Points, Client-Module sowie Controller können mittels „Web Based Management“ (WBM) oder mittels Telnet über die Kommandozeile („Command Line Interface“, CLI) konfiguriert werden.

Bei WBM erfolgt der Zugriff auf die Konfigurationsdaten des SCALANCE W über die Ethernet-Schnittstelle oder eine existierende WLAN-Verbindung. Ein Web-Browser auf dem PC des Konfigurators kommuniziert dabei mit einem HTTP-Server, der auf dem SCALANCE W läuft. Mithilfe des HTTP-Servers können die Konfigurationsdaten mit Formularen, wie man sie von gewöhnlichen Webseiten kennt, gelesen und geändert werden.

Für die benutzerfreundliche Installation und Konfiguration sowohl der Access Points als auch der Client-Module stehen eine Reihe von Wizards im Web Based Management zur Verfügung. Mit diesen können die Baugruppen optimal an die Kommunikationsaufgabe angepasst werden. Sowohl der Netzwerk-Betriebsmodus als auch die benötigte Sicherheitsstufe des WLAN lassen sich hier mit wenig Aufwand einstellen.

Hinweis

Im Siemens Industry Online Support stehen eine Reihe von Projektierungshandbüchern zur Verfügung. Eine Auswahl finden Sie unter folgenden Links:

- Projektierung der SCALANCE W780/ W740 über WBM: http://support.automation.siemens.com/WW/view/de/62516763
- Projektierung der SCALANCE W770/ W730 über WBM: https://support.industry.siemens.com/cs/de/de/view/109480849
- Projektierung der SCALANCE W760/ W720 über das WBM: https://support.industry.siemens.com/cs/de/de/view/109480845
- Getting Started für den IWLAN-Controller WLC711: http://support.autIWLAN-Controlleromation.siemens.com/WW/view/de/62523066

8.7 SIMATIC Mobile Panels 277(F) IWLAN V2

SIEMENS bietet für die Automatisierung ein breites Spektrum von HMI-Geräten („Panels“), mit denen komplette Anlagen oder einzelne Geräte innerhalb der Linie beobachtet, überwacht und bedient werden können. Darunter befinden sich auch „Mobile Panels“ mit integrierten Funkschnittstellen, die im Rahmen eines IWLANs eingesetzt werden. Diese Panels sind insbesondere nicht mehr stationär eingebaut, sondern können durch die Anlage bewegt und an dem Ort, an dem sie benötigt werden, zum Einsatz kommen.

Sie kombinieren die Fähigkeiten eines IWLAN-Clients mit dem Funktionsumfang eines HMI-Panels wie

- Archive (Speicherung von Messwerten und Eingaben im zeitlichen Kontext),
- Rezepturen (Sätze von zusammengehörigen Prozessdaten, die „als Ganzes“ verwaltet werden)
- ein hochentwickeltes Melde-, Protokoll- und Alarmsystem.

Die Bedienung erfolgt über den Touchscreen, die konfigurierbaren Funktionstasten oder mittels Handrad, Schlüsselschalter und Leuchtdrucktaster. Die SIMATIC

8.7 SIMATIC Mobile Panels 277(F) IWLAN V2

Mobile Panels 277(F) IWLAN V2 sind nach Schutzart IP 65 gebaut und kommunizieren über den WLAN-Standard IEEE 802.11a/b/g/h über PROFINET.

Abbildung 8-13

Hinweis Weitere Informationen zu diesem Produkt finden Sie in der SIEMENS Industry Mall unter: http://www.automation.siemens.com/panels

Hinweis Ein Applikationsbeispiel inkl. Safety finden Sie im Siemens Industry Online Support unter:
http://support.automation.siemens.com/WW/view/de/25702331

9 Zubehör für drahtlose Netzwerke (WLANs)

9.1 Optionale Speichermedien

Bei einem KEY-PLUG bzw. C-PLUG („Configuration Plug“) handelt es sich um ein Wechselspeichermedium, das in einen entsprechenden Slot der Hardware gesteckt wird.
C- und KEY-PLUG sind vom Aufbau her ähnlich, unterscheiden sich aber in Funktion und Farbe.

Abbildung 9-1

9.1.1 KEY-PLUG

Mit Hilfe unterschiedlicher KEY-PLUGs werden in verschiedenen industriellen Netzwerkkomponenten der Siemens AG Zusatzfunktionen verfügbar gemacht.

In Verbindung mit den SCALANCE W7xx für IEEE 802.11a/g/n werden mit dem KEY-PLUG W780 bzw. W740 die iFeatures (siehe Kapitel 4.6) aktiviert:

- der KEY-PLUG W780 iFeatures schaltet die iFeatures im Access Point-Mode und im Client-Mode frei,
- der KEY-PLUG W740 iFeatures schaltet die iFeatures nur im Client-Mode frei.
- der KEY-PLUG W700 Security schaltet weitere Sicherheitsfunktionen im Access Point frei.

Damit kann jedes SCALANCE W 11n-Standardgerät mit weiteren Funktionen erweitert/ hochgerüstet werden, ohne dass ein Austausch der Hardware nötig ist.

Zusätzlich beinhaltet der KEY-PLUG dieselben Funktionen wie der C-PLUG.

9.1.2 C-PLUG

Die SCALANCE W700-Geräte nach dem IEEE 802.11a/b/g/n-Standard besitzen zur Aufnahme der Projektierdaten einen internen Flash-Speicher sowie einen C-PLUG-Steckplatz.

Wenn ein C-PLUG gesteckt ist, werden Projektierdaten und deren Änderungen immer auf diesem gespeichert. Dadurch wird der Ersatzteilfall vereinfacht. Durch einfachen C-PLUG-Austausch können alle Daten ohne Programmiergerät in ein Ersatzgerät übernommen werden.

Hinweis Weitere Informationen zum Einsatz von C-PLUG mit SCALANCE W-Geräten finden Sie im Siemens Industry Online Support (Beitrags-ID 29823212):

http://support.automation.siemens.com/WW/view/de/29823212

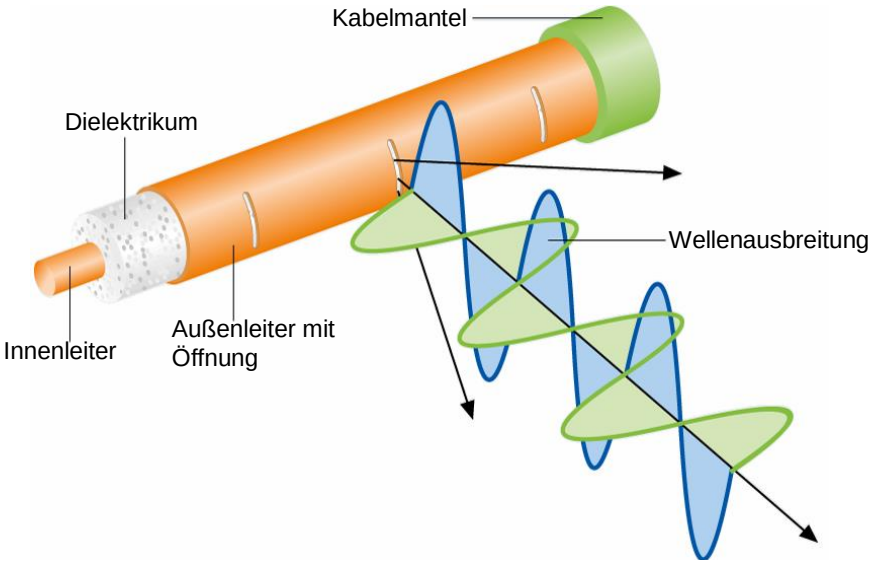
9.2 RCoax-Leckwellenleiter

Beschreibung

Die RCoax-Leitungen sind Leckwellenleiter, die in funktechnisch anspruchsvollen Umgebungen als Spezialantennen für die Access Points SCALANCE W fungieren.

Bei Leckwellenleiter handelt es sich um Koaxialleitungen, deren äußere Abschirmung definiert unterbrochen ist. Dieser konstruktive Aufbau bewirkt, dass sich entlang der RCoax-Leitung ein definiertes, kegelförmiges Funkfeld entwickelt.

Abbildung 9-2



Die RCoax-Leitung

Die RCoax-Leitungen ersetzen die üblichen Funkantennen an ausgewählten Access Points durch ein Antennensegment in frei konfektionierbarer Länge. Sie senden und empfangen im 2,4-GHz- oder im 5-GHz-Band. Dabei werden sie bevorzugt in Umgebungen eingesetzt, in denen sich die Teilnehmer in begrenzten Bereichen oder ausschließlich auf vorgegebenen Bahnen bewegen (Einschienenhängebahnen, Hochregallager) und wo viele Abschattungen oder Reflexionen zu erwarten sind.

Die RCoax-Leitung lässt sich bei der Installation der Anlage biegen und damit den örtlichen Gegebenheiten anpassen: So kann es zum Beispiel dem Verlauf einer Einschienenhängebahn unmittelbar folgen. Damit gibt es die Möglichkeit, bei anspruchsvollen Umgebungen auch schwer erreichbare Abschnitte der Funkzelle zuverlässig auszuleuchten. Wartungsintensive Schleifkontakte bzw. Schleppkabel können so eingespart werden.

iPCF und PROFINET I/O

Das IEEE 802.11-Protokoll des Access Points wird durch die Verwendung der RCoax-Leitung nicht beeinflusst, insbesondere bleiben die Datenraten und die

Protokolle zur Datensicherung erhalten. Auch iPCF und die Kommunikation über PROFINET I/O sind – die entsprechenden Access Points und Clients vorausgesetzt – wie zuvor möglich.

Hinweis Ein Anwendungsbeispiel für die Verwendung von RCoax-Leitungen in einer PROFINET I/O-Umgebung finden Sie im Siemens Industry Online Support (Beitrags-ID 23488061): http://support.automation.siemens.com/WW/view/de/23488061

Datenrate und Segmentlänge

Jeder SCALANCE W Access Point kann mit einer RCoax-Leitung ausgerüstet werden.
Um längere, lückenlose Funkbereiche zu erzeugen, können mehrere Leckwellenleitersegmente (mit jeweils einem zugeordneten Access Point) nacheinander angeordnet werden.

Mit der Länge der RCoax-Leitung steigt die Dämpfung entlang des Leckwellenleiters und die Signalstärke reduziert sich. Mit zunehmender Leitungslänge und steigendem Abstand von der Leitung sinkt also die erreichbare Datenrate.

Hinweis Weitere Informationen zu diesem Thema und Leistungsdaten finden Sie im „Systemhandbuch RCoax“ im Siemens Industry Online Support (Beitrags-ID 21286952): http://support.automation.siemens.com/WW/view/de/21286952

Anschluss von mobilen Teilnehmern

In einem RCoax-Netz wird die RCoax-Leitung von einem Access Point gespeist. Die RCoax-Leitung wirkt als Antenne zu mobilen Partnerstationen (z. B. SCALANCE W Clients), die sich längs der RCoax-Leitung bewegen und die Information über ihre Antenne aus dieser Leitung empfangen bzw. in dieses einkoppeln.

Der Anschluss an das drahtlose RCoax-Netzwerk erfolgt über Antennen, die mittels der flexiblen Anschlussleitung in unmittelbarer Umgebung der RCoax-Leitung montiert werden sollen.

Hinweis Aktualisierte Produktinformationen zu RCoax-Leitungen finden Sie auf dem Web unter der URL:
http://www.automation.siemens.com/mcms/industrial-communication/de/industrial-wireless-communication/netzkomponenten-iwlan/iwlan-rcoax/Seiten/rcoax.aspx

9.3 Antennen

9.3.1 Übersicht der WLAN-Antennen

Für eine optimale Funkfeldarchitektur steht neben der Auswahl der Geräte die der Antennen an oberster Stelle. Entscheidend sind vor allem diese Punkte:

- Charakteristik der Antenne (Funkausleuchtung)
- Einsatzort (Innen- oder Außenbereich)
- Benötigte Datenraten

Im SIMATIC-Portfolio stehen eine Reihe omnidirektionaler Antennen und Richtantennen zur Verfügung (grundlegende Informationen zu Antennen siehe auch Kapitel 1.5). Diese können direkt montiert oder abgesetzt vom Gerät z. B. an einem Mast oder einer Wand befestigt werden, um eine optimale Ausleuchtung des zu erfassenden Raums zu erzielen.

Antennen mit zwei (Dual Slant) oder drei Anschlüssen (MIMO) erhöhen den Datendurchsatz und die Zuverlässigkeit durch gezielte Nutzung der Mehrwegeausbreitung.

Eine Übersicht der WLAN-Antennen zeigt das folgende Bild:

Abbildung 9-3

9.3 Antennen

Die Eigenschaften der wichtigsten Antennentypen können der folgenden Tabelle entnommen werden:

Tabelle 9-1

Typ	Montage	Charakter-istik	Antennen-gewinn	SCALANCE W780/ W740	SCALANCE W770/ W730	SCALANCE W760/ W720
ANT795-4MC	Direkt am Gerät	Omnidir.	2,4 GHz: 3,0 dB 5,0 GHz: 5,0 dB	x	-	-
ANT795-4MD				x	-	-
ANT795-4MA				x	x	x
ANT795-4MX			2,4 GHz: 2,0 dB 5,0 GHz: 2,5 dB	x	-	-
ANT792-6MN	Wand oder Mast		2,4 GHz: 6,0 dB	x	x	x
ANT793-6MN			5,0 GHz: 5,0 dB	x	x	x
ANT795-6MP			2,4 GHz: 5,0 dB 5,0 GHz: 7,0 dB	x	x	x
ANT795-6MN	Decke		2,4 GHz: 6,0 dB 5,0 GHz: 8,0 dB	x	x	x
ANT795-6MT			2,4 GHz: 4,0 dB 5,0 GHz: 6,0 dB	x	-	-
ANT795-6DC	Wand oder Mast	Gerichtet	2,4 GHz: 9,0 dB 5,0 GHz: 9,0 dB	x	x	-
ANT793-6DG			5,0 GHz: 9,0 dB	x	x	-
ANT793-6DT			5,0 GHz: 8,0 dB	x	-	-
ANT792-8DN			2,4 GHz: 14,0 dB	x	-	-
ANT793-8DP			5,0 GHz: 13,5 dB	x	-	-
ANT793-8DJ			5,0 GHz: 18,0 dB	x	-	-
ANT793-8DK			5,0 GHz: 23,0 dB	x	-	-
ANT793-8DL			5,0 GHz: 14,0 dB	x	x	x
ANT793-4MN	RCoax	Omnidir.	5,0 GHz: 6,0 dB	x	x	x
ANT792-4DN		Gerichtet	2,4 GHz: 4,0 dB	x	x	x

Hinweis zur Namenskonvention bei IWLAN-Antennen

In der Bezeichnung der Antennen-Typen sind die wichtigsten Funktionsmerkmale codiert hinterlegt:

ANT79w-xyz

w = 2 / 3 / 5: Frequenzbereich 2,4 GHz / 5 GHz / Dualband (2,4 und 5 GHz)

x = 4 / 6 / 8: Maß für die passive Verstärkung

y = M / D: Omni (Rundstrahl) / gerichtet

Beispiel: ANT792-8DN (2 GHz, hohe Verstärkung, gerichtet, N-Connect)

9.3.2 Antennen mit omnidirektionaler Charakteristik

SIMATIC NET bietet ein abgestimmtes Sortiment von Antennen mit einer omnidirektionalen Charakteristik für unterschiedliche Anwendungsfälle sowohl im Innenbereich, als auch im Außenbereich an. Die Antennen unterscheiden sich hinsichtlich des Montageorts, der Anschlüsse, der Schutzklasse und des Frequenzbereichs.

Antenne ANT795-4Mx

Die Antennen vom Typ ANT795-4Mx eignen sich für die Montage direkt am Access Point oder Client.

Abbildung 9-4

ANT795-4MC ANT795-4MD ANT795-4MA ANT795-4MX

Die folgende Tabelle stellt die Varianten dar:

Tabelle 9-2

Antenne	Anschluss	Schutz-klasse	Bemerkung
ANT795-4MC	1 x N-Connect male	IP65	gerade
ANT795-4MD	1 x N-Connect male	IP65	Fester 90° Winkel
ANT795-4MA	1 x R-SMA male	IP30	Mit zusätzlichem Gelenk; schwenkbar um einen Winkel zwischen 0° und 90°.
ANT795-4MX	1 x N-Connect male	IP68	gerade

Antenne ANT79x-6MN / ANT795-6MP

Die Antennen vom Typ ANT79x-6Mx können sowohl an einer Wand als auch an einem Mast montiert werden.

Abbildung 9-5

ANT79x-6MN ANT795-6MP

Die folgende Tabelle stellt die Varianten dar:

Tabelle 9-3

Antenne	Anschluss	Schutz-klasse	Bemerkung
ANT792-6MN	1 x N-Connect female	IP65	Im Bild oben dargestellt.
ANT793-6MN	1 x N-Connect female	IP65	
ANT795-6MP	1 x N-Connect female	IP67	

Antenne ANT795-6Mx

Die Montage der Antennen vom Typ ANT795-6Mx kann direkt an einer Wand, Decke oder einem Dach erfolgen.

Abbildung 9-6

ANT795-6MN

ANT795-6MT

Die folgende Tabelle stellt die Varianten dar:

Tabelle 9-4

Antenne	Anschluss	Schutz-klasse	Bemerkung
ANT795-6MN	1 x N-Connect female	IP65	
ANT795-6MT	3 x QMA female	IP65	MIMO-Antenne;

9.3.3 Antennen mit Richtwirkung

Die Produktpalette von SIMATIC NET bietet auch eine große Auswahl an Richtantennen an. Die Antennen unterscheiden sich hinsichtlich der Anschlüsse, der Schutzklasse und des Frequenzbereichs.

Die Antennen vom Typ ANT79x-xDx sind für die Wand- oder Mastmontage konzipiert.

Abbildung 9-7

ANT795-6DC ANT793-6DG ANT793-6DT ANT793-8DP

ANT792-8DN ANT793-8DJ ANT793-8DK

ANT793-8DL

Die folgende Tabelle stellt die Varianten dar:

Tabelle 9-5

Antenne	Anschluss	Schutz-klasse	Bemerkung
ANT795-6DC	1 x N-Connect female	IP67	
ANT793-6DG	2 x N-Connect female	IP67	Dual Slant
ANT793-6DT	3 x QMA female	IP67	MIMO-Antenne
ANT793-8DN	1 x N-Connect female	IP65	
ANT793-8DP	1 x N-Connect female	IP67	
ANT793-8DJ	2 x N-Connect female	IP67	Dual Slant
ANT793-8DK	2 x N-Connect female	IP67	Dual Slant
ANT793-8DL	2 x N-Connect female	IP67	Dual Slant

9.3.4 Antennen für RCoax

Beim Einsatz eines RCoax-Systems bietet das Portfolio zwei Antennen an, die sich nur im Frequenzbereich unterscheiden.

Abbildung 9-8

ANT792-4DN ANT793-4MN

Die folgende Tabelle stellt die Varianten dar:

Tabelle 9-6

Antenne	Anschluss	Schutz-klasse	Bemerkung
ANT793-4MN	1 x N-Connect female	IP66	
ANT792-4DN	1 x N-Connect female	IP65	

Hinweis

Weitere Produktinformationen zu Antennen finden Sie unter der URL:

http://www.automation.siemens.com/mcms/industrial-communication/de/industrial-wireless-communication/netzkomponenten-iwlan/zubehoer/Seiten/zubehoer.aspx.

Informationen zu RCoax-Antennen finden Sie im „Systemhandbuch RCoax“ im Siemens Industry Online Support (Beitrags-ID 21286952): http://support.automation.siemens.com/WW/view/de/21286952

9.4 Anschlüsse und Verkabelung

In der Industrie kommen je nach Anwendungsfall verschiedene Antennenstecker zum Einsatz. Sie unterscheiden sich in der Größe, mechanischen Eigenschaften und dem Einsatzgebiet.

Die SCALANCE W Access Points und -Clients haben je nach Modell N-Connect oder R-SMA-Anschlüsse, die Antennen zusätzlich noch QMA-Anschlüsse. Diese Anschlüsse zeichnen sich durch hochklassige Übertragung, zuverlässige Verbindungen durch die Verwendung von Überwurfmuttern und einen geringen Formfaktor aus.

N-Connect-Anschluss

Der N-Stecker ist für alle Koaxialkabeltypen ausgelegt. Durch eine mechanische Fixierung weist er eine hohe Robustheit auf und ist durch einen zusätzlichen Dichtungsring gut für den Außenbereich geeignet.

SMA-Anschluss

Der SMA-Anschluss ist ein Miniatur-Koaxial-Stecker bzw. –Buchse und besteht aus einem Gewinde und Innenkontakt. Er wird in zwei Ausführungen angeboten:

- SMA-Variante
- Reverse-(R-)SMA-Variante.

Die Unterschiede zeigt die folgende Tabelle:

Tabelle 9-7

Stecker-/Buchse Variante	Merkmal
SMA-Stecker	Innengewinde und Innenkontakt als Stift
SMA-Buchse	Außengewinde und Innenkontakt als Kelch
R-SMA-Stecker	Innengewinde und Innenkontakt als Kelch
R-SMA-Buchse	Außengewinde und Innenkontakt als Stift

Bei SCALANCE W-Geräten mit Anschlüssen dieser Baugröße kommt die R-SMA-Variante zum Einsatz.

QMA-Anschluss

QMA-Anschlüsse haben die gleiche hohe elektrische Leistung wie die SMA-Serie mit einer einfacheren und schnelleren Montage. QMA-Anschlüsse werden vor allem für die neue Generation von SCALANCE W-Antennen (IEEE 802.11n) verwendet, bei denen mehrere Anschlüsse auf sehr engem Raum platziert sind.

9.5 Weiteres Zubehör

Für eine flexible Kombination und Installation der einzelnen IWLAN-Komponenten im Innen- wie auch Außenbereich wird ein umfangreiches, aufeinander abgestimmtes Sortiment an koaxialen Zubehörteilen angeboten. Es umfasst sowohl Antennen-Anschlussleitungen als auch diverse Steckverbinder, Blitzschutzelemente, einen Power Splitter und ein Dämpfungsglied.

Hinweis Welche Verbindungskabel und Zusatzgeräte zum Anschluss einer externen Antenne an den SCALANCE W eingesetzt werden können, zeigen mehrere FAQs im Siemens Industry Online Support (Beitrags-ID:22167025):

http://support.automation.siemens.com/WW/view/de/22167025

Blitzschutzelement

Das Blitzschutzelement LP798-2N erweitert die Einsatzmöglichkeit der SCALANCE W700-Produkte mit abgesetzten Antennen besonders für den Außenbereich.

Abbildung 9-9

Ein Blitzschutzelement sichert das aktive Gerät gegen zerstörende Überspannung (z.B. Blitzschlag) über die Antennenanschlüsse. Tritt ein Überspannungsereignis ein, so werden entsprechende Ströme über die Erdung abgeleitet.

Das Blitzschutzelement sollte möglichst in der Nähe des aktiven Gerätes (z.B. an der Schaltschrankwand) installiert und großflächig geerdet werden. Über Antennen-Anschlussleitungen wird es mit der Antenne und dem aktiven Gerät verbunden.

Es stehen unterschiedliche Varianten des Blitzschutzelements zur Verfügung.

Abschlusswiderstand

Der Abschlusswiderstand TI795-1R (siehe Abbildung) bzw. TI795-1N muss bei SCALANCE W700-Produkten für jeden nicht verwendeten Antennenanschluss eingesetzt werden, um diesen hochfrequenztechnisch abzuschließen.

Abbildung 9-10

Flexible Verbindungsleitungen

Die flexiblen IWLAN RCoax/Antenna-Anschlussleitungen werden zur Verbindung von RCoax-Segmenten oder Antennen mit aktiven Geräten benötigt. Außerdem können sie als Adapterleitungen verwendet werden, wenn die Antenne und die WLAN-Baugruppe unterschiedliche Anschlüsse aufweisen. Sie sind in verschiedenen Längen (0,3 m bis 10 m) und Anschlusskombinationen (N-Connect, R-SMA, SMA, QMA) erhältlich.

Das folgende Bild zeigt ein QMA/N-Connect male/female Verbindungskabel:

Abbildung 9-11

Das nächste Bild zeigt eine Verbindungsleitung, die zwischen einem SCALANCE W78x RJ45 und z. B. einer abgesetzten Antenne oder einer anderen Komponente mit N-Connect Anschluss eingesetzt wird:

Abbildung 9-12

Hinweis Weitere Informationen sowie Anwendungsbeispiele finden Sie im FAQ „Welche Verbindungskabel und IWLAN Geräte können Sie einsetzen, um eine externe Antenne an den SCALANCE W anzuschließen?“ (Beitrags-ID 43895062)

http://support.automation.siemens.com/WW/view/de/43895062

Die Leitungen bieten eine geringe Dämpfung, sodass die Qualität des Funksignals nur minimal beeinträchtigt wird. Alle Antennenleitungen bieten Flammschutz, sind chemisch beständig und silikonfrei.

Power Splitter

Abbildung 9-13

Mit Hilfe des Power Splitters wird die Sendeleistung eines Access Points auf zwei RCoax- oder Antennensegmente verteilt. Dies ermöglicht eine Funkabdeckung in zwei unterschiedlichen Bereichen mit nur einem Access Point.

Stromversorgung SITOP PS307

Die SITOP PowerSupply ist eine hochqualitative Gleichspannungsversorgung für den Einsatz im industriellen Umfeld mit Schutzart IP20. Über spezielle Zusatzmodulen schützt die Stromversorgung vor Störungen auf der Netz- sowie auf der Gleichspannungsseite und sorgt für die nötige Versorgungssicherheit.

Abbildung 9-14

Hinweis Bei Nutzung der SITOP PS307 für die SCALANCE W788 M12-Geräte muss die Stromversorgung in einen Schaltkasten montiert werden.

Wechselspannungsnetzteil mit IP65

Über das Netzteil PS791-1PRO können die SCALANCE W- Baugruppen (IEEE 802.11 a/b/g) in Schutzart IP65 direkt aus der Steckdose mit Spannung versorgt werden. Durch den weiten Netzeingangsspannungsbereich (Eingangsspannungen von AC 90 bis 265 V) ist ein weltweiter Einsatz möglich.

Abbildung 9-15

Das Netzteil selbst verfügt über ein robustes Metallgehäuse mit Schutz vor Wasser und Staub in Schutzklasse IP65. Die Kurzschlussfestigkeit, Leerlaufsicherheit und die Überbrückung kurzer Netzstörungen garantieren eine hohe Betriebssicherheit.

Dämpfungsglied

Das Dämpfungsglied kommt immer dann zum Einsatz, wenn die übertragene Leistung sowohl in Sende- als auch in Empfangsrichtung reduziert werden muss. Typische Anwendungsgebiete sind kurze RCoax-Segmente oder Richtfunkstrecken, die in der Ausdehnung begrenzt werden sollen. Die Einfügedämpfung des Dämpfungsglieds beträgt 10 dB.

Abbildung 9-16

Schaltschrankdurchführungen

Die Schaltschrankdurchführungen ermöglichen zusammen mit den Antennen-Anschlussleitungen eine einfache Verbindung abgesetzt montierter Antennen mit den im Schaltschrank / -kasten befindlichen aktiven Komponenten. Die Schrankdurchführung gibt es mit den Anschlusskombinationen:

- SMA-female / N-female für Wandstärken bis max. 4,5 mm
- N-Connect female / N-Connect female für Wandstärken bis max. 4,5 mm

Abbildung 9-17

Hinweis Weitere Produktinformationen zu passiven Netzkomponenten finden Sie im „Systemhandbuch zu den Industrial Wireless LAN Passive Netzkomponenten“ im Siemens Industry Online Support (Beitrags-ID 67701823): http://support.automation.siemens.com/WW/view/de/67701823

9.6 TIA Selection Tool

Allgemeines

Die Auswahl- und Bestellhilfe TIA Selection Tool unterstützt bei der Auswahl von Industrial Ethernet Switches und Komponenten für Industrial Wireless Communication.

Primär soll das Tool den Bestellvorgang vereinfachen und dem Kunden bei der Auswahl der Produkte unterstützen.

Beschreibung

Das TIA Selection Tool ist der Nachfolger des SIMATIC Selection Tools und vereint bereits bekannte Konfiguratoren für die Automatisierungstechnik in einem Werkzeug mit deutlich mehr Produkte als der Vorgänger.

Es bietet mehrere Assistenten zur Auswahl der gewünschten Geräte und Netzwerke an. Zudem gibt es Konfiguratoren zur Selektion von Modulen und Zubehör sowie dem Überprüfen der korrekten Funktionsweise.

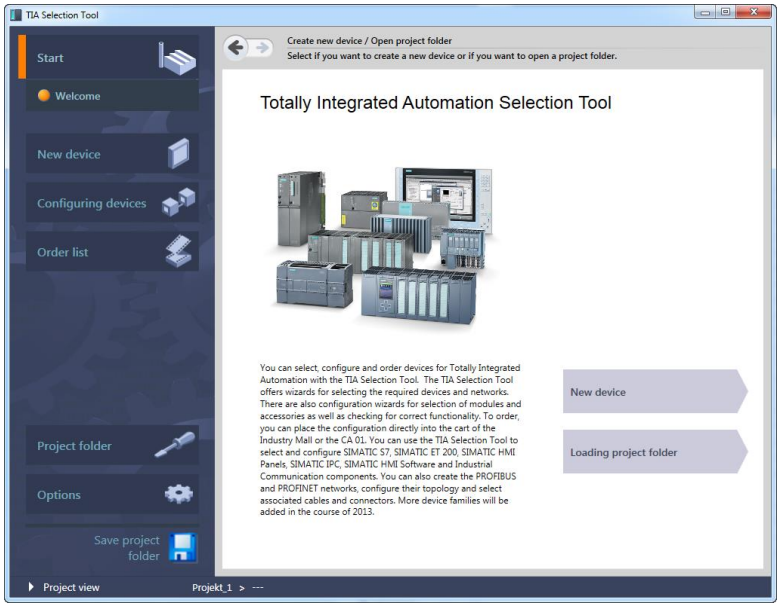
Aus der Produktauswahl oder der Produktkonfiguration kann eine vollständige Bestellliste generiert werden. Diese können Sie direkt in den Warenkorb der Industry Mall oder des CA 01 exportieren.

Bedienoberfläche

Die Bedienoberfläche des TIA Selection Tools ähnelt der Engineeringsoftware des TIA Portals.

Das Tool besitzt eine javabasierte, grafische Oberfläche. Die einzelnen Auswahlmöglichkeiten und Produkte sind als Reiter dargestellt. Es ist möglich, direkt den Reiter zu wählen oder mithilfe des Tools Schritt für Schritt geleitet zu werden.

Abbildung 9-18



Unterstützte Komponenten

Mit dem TIA Selection Tool können folgende Produkte ausgewählt und konfiguriert werden:

- SIMATIC S7,
- SIMATIC ET 200,
- SIMATIC HMI Panels,
- SIMATIC IPC, SIMATIC
- HMI Software
- Industrial Communication Komponenten

Zudem können PROFIBUS- und PROFINET-Netzwerke erstellt, deren Topologie konfiguriert sowie zugehörige Kabel und Stecker auswählt werden.

Installation

Das TIA Selection Tool kann direkt in der Siemens Industry Mall gestartet oder als Datei heruntergeladen werden.

Hinweis Weitere Informationen finden Sie unter der URL: http://www.siemens.de/tia-selection-tool

10 IWLAN im Einsatz

Durch die Anwendung von drahtlosen Datennetzen können Prozesse erheblich effizienter gestaltet werden. Der Vorteil drahtloser Lösungen ist vor allem die einfache und flexible Erreichbarkeit mobiler oder schwer zugänglicher Teilnehmer.

Durch die drahtlose Kommunikation zu Automatisierungsgeräten und industriellen Endgeräten wird eine höhere Flexibilität erreicht, Wartungsarbeiten werden vereinfacht, Servicekosten und Stillstandzeiten reduziert und das Personal optimal eingesetzt.

Mit Industrial Wireless LAN (IWLAN) sind auch anspruchsvolle Anwendungen mit Echtzeit- und Redundanzanforderungen in der Industrie realisierbar.

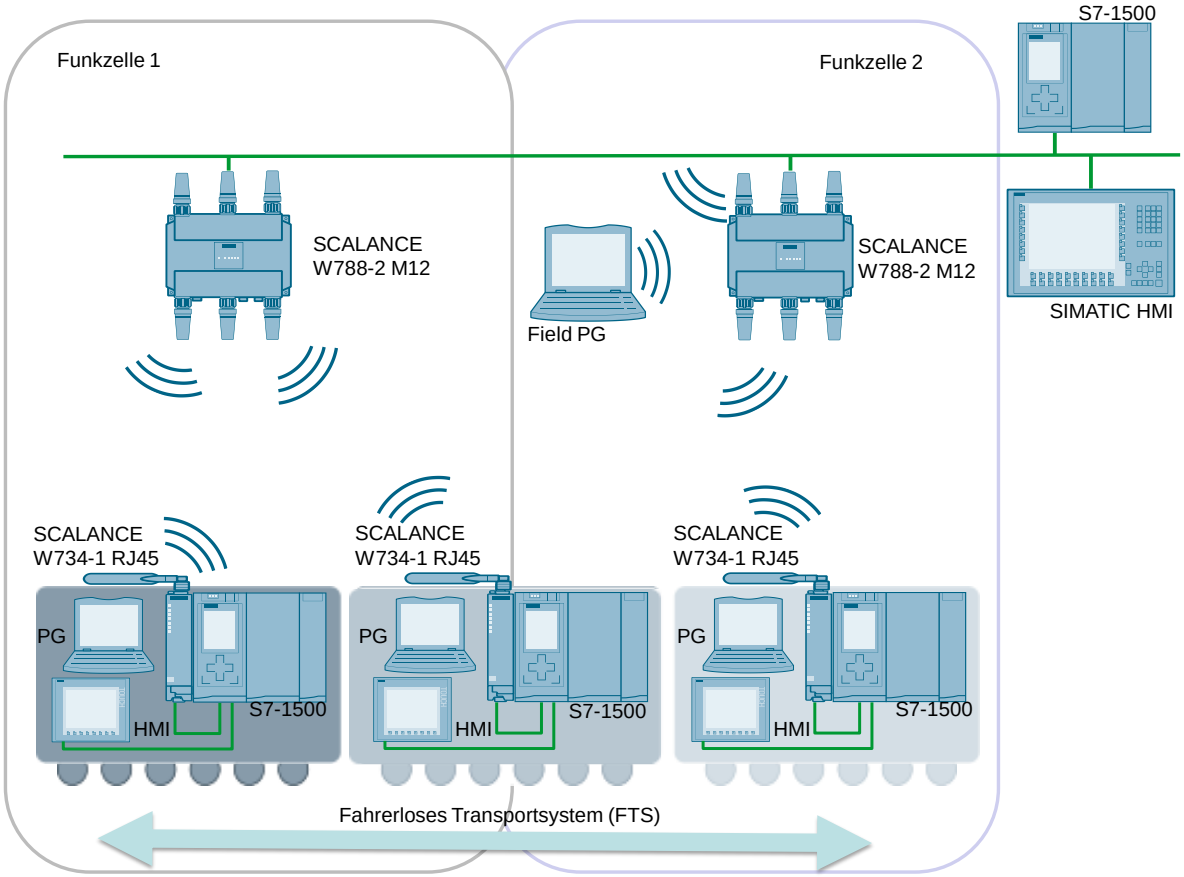
Anhand ausgewählter Einsatzorte und Applikationsbeispiele wird der Einsatz von IWLAN im Folgenden kurz demonstriert.

Fahrerloses Transportsystem: Roaming von bewegten Geräten

Unten dargestellt ist ein Beispiel aus der Intralogistik, bei dem einzelne W788-2-Access Points mehrere benachbarte Funkzellen aufspannen. Untereinander verbunden über einen kabelgestützten Ethernet-Strang vermitteln sie die Kommunikation zwischen dem fahrerlosen Transportsystem, auf dem sich ein Client-Modul W734-1 und eine mobile S7-1500 CPU befinden, einerseits und einer stationären S7-1500 CPU sowie einem HMI-Panel andererseits.

Diese Konfiguration ermöglicht es dem fahrerlosen Transportsystem, von Funkzelle zu Funkzelle zu wechseln („Roaming“), ohne den Kontakt zu verlieren.

Abbildung 10-1

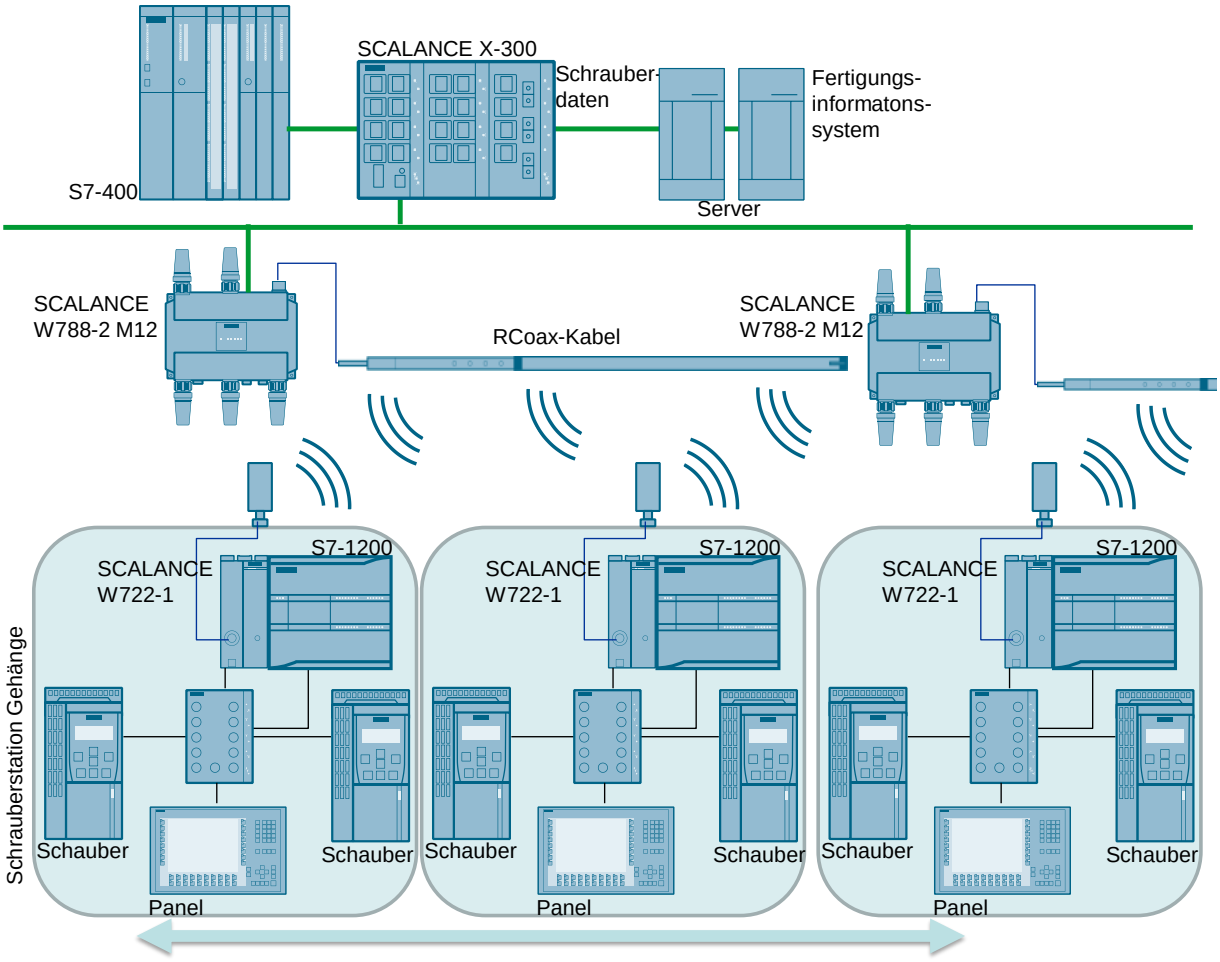


Einhängeschienenbahn: Einsatz von RCoax

Im folgenden Beispiel aus der Automobilindustrie wird für den Aufbau der drahtlosen Datenübertragung der Leckwellenleiter IWLAN RCoax entlang der Codierschiene eingesetzt. Er erzeugt ein definiertes und zuverlässiges Funkfeld. Als Einspeisestation für die RCoax-Leitung werden die Access Points W788-2 eingesetzt.

Die mobilen Schrauberstationen – jeweils bestückt mit einem Client-Modul W722-1, einer SIMATIC S7-1200, zwei Schraubern und einem Panel – bewegen sich entlang des Pfades der Einhängeschienenbahn und können über ihr Client-Modul und den Access Point mit dem kabelgebundenen Netzwerk kommunizieren.

Abbildung 10-2



Controller-basiertes WLAN: Einsatz des SCALANCE WLC711

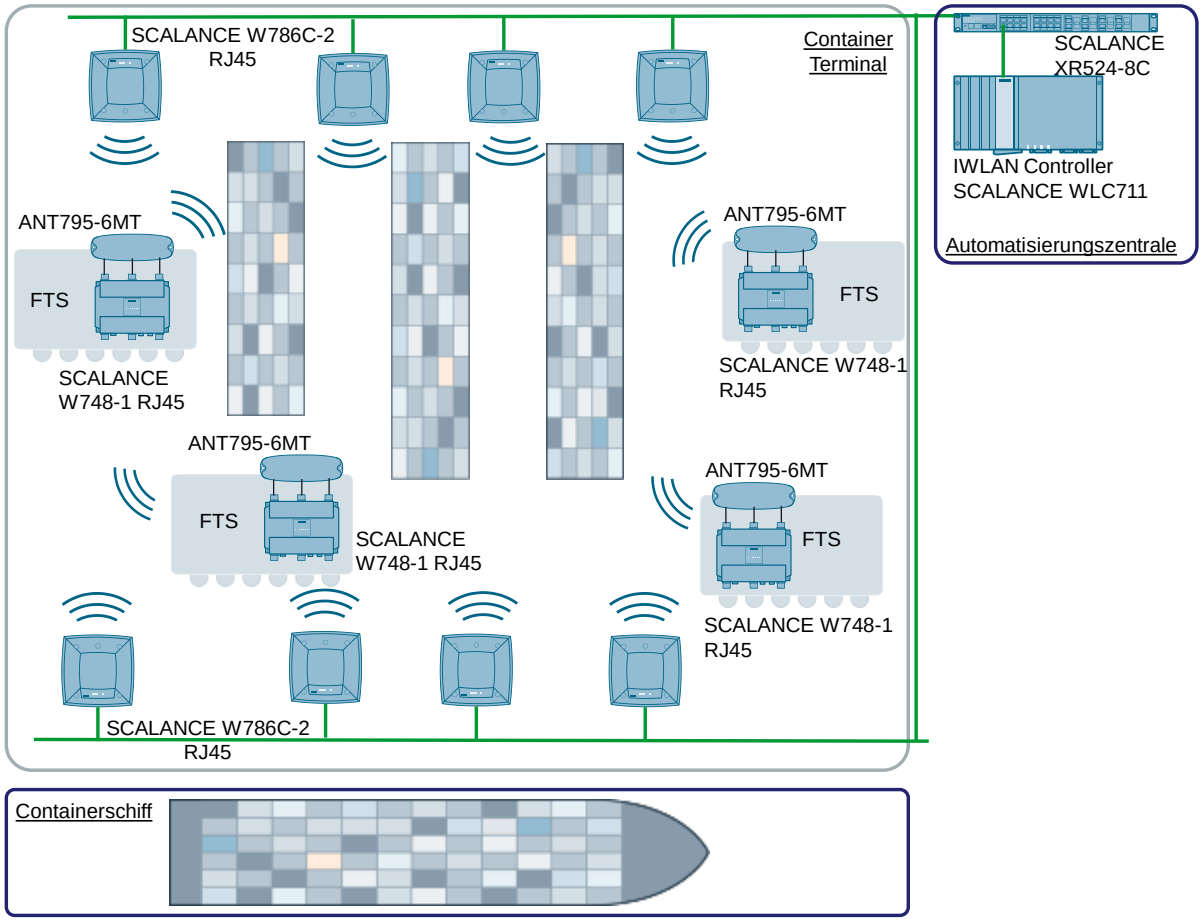
Der Einsatz eines Controller-basierten WLANs wird beispielhaft an einer Container-Umschlaganlage gezeigt. Für ein effizientes Umladen der Container werden fahrerlose Transportsysteme (FTS) eingesetzt, die sich in dem großen Areal des Terminals frei bewegen können.

Da sich die FTSs im Außenbereich bewegen, ist es wichtig, dass eine robuste und Outdoor-taugliche Verbindung aufgebaut wird, damit die Positionsdaten und Fahrbefehle sicher und zuverlässig übertragen werden können.

Eine geeignete Lösung kann mit den verschiedenen Produkten des SCALANCE W-Portofolios aufgebaut werden. Die FTSs werden mit W748-1 RJ45 Client-Modulen ausgestattet. Die Kommunikation zwischen den FTSs wird dann von den Controller-basierten SCALANCE W786-2C-Access Points gesteuert.

Durch den Einsatz des SCALANCE WLC 711 können die Access Points W786-2C zentral konfiguriert und betrieben werden. Außerdem liefert der Controller zusätzliche Features, um die Qualität der Lösung noch mal zu steigern. So kann z. B. mittels Load Balancing eine gleichmäßige Verteilung der Clients auf die einzelnen Access Points erreicht werden.

Abbildung 10-3



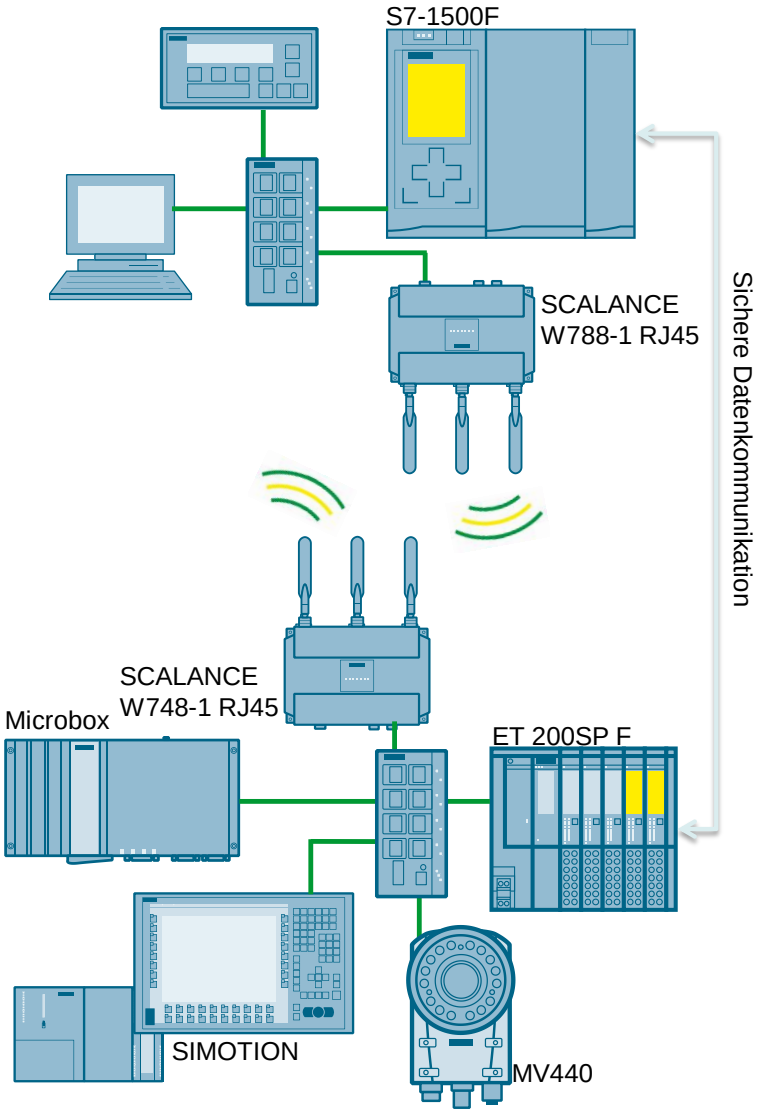
Safety over Wireless: PROFIsafe mit SCALANCE W

PROFIsafe ist eine Protokollerweiterung von PROFIBUS / PROFINET für die sicherheitsgerichtete Kommunikation.

Im nachfolgenden Beispiel wird das sicherheitsgerichtete Bedienen eines Roboters demonstriert.

Da PROFIsafe eine Protokollerweiterung darstellt, kann ein gemischter Verkehr von „gesicherten“ und Standard-Nachrichten auf demselben Netz stattfinden.

Abbildung 10-4



11 Glossar

802.11

Eine Reihe von durch die → IEEE entwickelten Standards für drahtlose Netzwerkprotokolle.

Access Point

„Zugangspunkt“, ein Teilnehmer eines → WLANs, der gleichzeitig administrative Funktionen im Netzwerk erfüllt und z.B. für → Clients die Verbindung zu drahtgebundenen Netzwerken, anderen Clients in derselben Funkzelle oder in anderen Funkzellen bereitstellt. Siehe Kapitel 4.1.2

***Ad-hoc*-Netzwerk**

Ein unstrukturiertes → WLAN, bei dem es keine → Access Points gibt. Die → Clients kommunizieren „auf eigene Verantwortung“ ohne übergeordnete Koordination miteinander. Der Gegensatz dazu ist ein Netz im → Infrastrukturmodus.

AES

„Advanced Encryption Standard“, ein Verschlüsselungsverfahren, siehe Kapitel 5.2.2.

Antennen-Diagramm

Eine grafische Darstellung der Strahlungscharakteristik einer Antenne zur Abschätzung der Leistungsfähigkeit. Die Werte für das Antennen-Diagramm werden messtechnisch aufgenommen oder durch Simulationsprogramme generiert.

Antennen-Diversity

Die gleichzeitige Verfügbarkeit zweier Funkschnittstellen an einem Gerät. In funktechnisch schwierigen Umgebungen kann dynamisch auf die Schnittstelle mit der Frequenz gewechselt werden, die momentan die besten Empfangsbedingungen gewährleistet.

Antennengewinn

Durch geeignete Bauform erzielte Konzentration des Funkfeldes einer Antenne in eine begrenzte Raumrichtung. Dadurch wird eine (passive!) Verstärkung in dieser Raumrichtung im Vergleich zu einem isotropen Strahler erreicht. Andere Raumrichtungen werden dafür abgeschwächt. Die Form des Funkfeldes wird in dem → Antennendiagramm näher spezifiziert.

Bandbreite

Soviel wie „maximal nutzbare Datenrate“. Der Begriff leitet sich ab von der Tatsache, dass durch die Übertragung mit einer bestimmten Datenrate ein proportional breiter Abschnitt des Funkspektrums belegt wird. Siehe hierzu auch Kapitel 1.4.4.

Bluetooth

Ein Funkstandard mit kurzer Reichweite für die Kommunikation von Bürogeräten und Mobiltelefonen untereinander, siehe Kapitel 3.

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, ein Verschlüsselungsalgorithmus, der im Rahmen von → WPA2 eingesetzt wird, siehe Kapitel 5.2.2.

Client

Hier: Ein Teilnehmer eines → WLANs, der keine eigenen Infrastruktur-Fähigkeiten besitzt, sondern über einen → Access Point auf ein Funknetz zugreift.

CSMA/CA

“Carrier Sense Multiple Access with Collision Avoidance”, ein Verfahren zur Erkennung von “Kollisionen”, d. h. dem Versuch mehrerer Sender, gleichzeitig auf einer Frequenz ihre Übertragung zu beginnen. Wenn das passiert, brechen beide Sender ihre Übertragung ab und warten eine mehr oder minder zufällige Frist ab. Nur, wenn der andere innerhalb dieser Frist nicht wieder zu senden begonnen hat, beginnen sie ihre Wiederholung. So kommt es nur dann zu einer zweiten Kollision, wenn beide zufällig gewählten Verzögerungen identisch sind.

DCF

„Distributed Coordination Function“, ein Organisationsmodell für Funknetze (siehe Kapitel 4.4.1).

DFS

„Dynamic Frequency Selection“, svw. Dynamische Frequenzwahl, eine Erweiterung des → 802.11h-Standards. Wird während des Betriebes auf einem Kanal ein anderer (netzfremder) Nutzer entdeckt, so wechselt der → Access Point den benutzten Kanal. Dadurch soll eine Beeinflussung durch andere Systeme, die im 5-GHz-Band arbeiten (Radar, Satellitenfunk und –navigation), vermieden werden.

DoS

„Denial of Service“, eine Angriffsmethode gegen ein Netzwerk.

DSSS

“Direct Sequence Spread Spectrum“, ein Spreizbandübertragungsverfahren bei IEEE 802.11b.

EAP

„Extensible Authentication Protocol“, eine Methode im Rahmen des → RADIUS-Protokolls, mit deren Hilfe Server und Client sich vor der eigentlichen Authentifizierung auf ein *Verfahren* für die Authentifizierung einigen können.

GFSK

„Gaussian Phase Shift Keying“, ein Modulationsverfahren bei IEEE 802.11.

GPRS

„General Packet Radio Service", ein Datenübertragungsdienst, der für die Kommunikation von Mobiltelefonen verwendet wird.

Handover

Der Übergang eines mobilen Clients von einem Access Point und dessen Funkzelle zum nächsten (→ Roaming); insbesondere die Re-Integration ins Netzwerk.

Hidden-Node-Problem

Svw. → Hidden-Station-Problem

Hidden-Station-Problem

Ein Verbindungsproblem, das auftritt, wenn ein Empfänger gleichzeitig von zwei Sendern angesprochen wird, die einander nicht hören können, wodurch es beim Empfänger zu Kollisionen kommt.

HMI

„Human Machine Interface“, Anzeige- und Bediengeräte für die Anlagensteuerung, wie z. B. die SIMATIC Mobile Panels

IEEE

„Institute of Electrics and Electronics Engineers“ (ausgesprochen „I – Triple E“), eine US-amerikanische Vereinigung die unter anderem Richtlinien und technische Empfehlungen erarbeitet; im weiteren Sinne vergleichbar mit dem DIN.

.

Infrastrukturmodus

Die Organisation eines Funknetzwerkes dergestalt, dass ein oder mehrere → Access Points Zellen bilden, durch die das Netz eine „Struktur“ erhält. Der Gegensatz dazu ist ein → *Ad-hoc*-Netzwerk.

IP 30

Eine Schutzart, die besagt, dass das solchermaßen kategorisierte Bauteil vor dem Eintritt grober Fremdkörper (ab 2,5 mm Durchmesser), aber nicht vor Wassereintritt geschützt ist. Dies entspricht einem gewöhnlichen elektrischen Haushaltsgerät.

IP 65

Eine Schutzart, die besagt, dass das solchermaßen kategorisierte Bauteil komplett vor Staub und vor Strahlwasser geschützt ist. Dies entspricht einer fast luftdichten Kapselung.

iPCF

„Industrial Point Coordination Function“, ein proprietäres, von SIEMENS unterstütztes Netzwerkprotokoll, das geringe → Handover-Zeiten (in der Größenordnung von 30 ms) beim → Roaming der beweglichen Teilnehmer ermöglicht. iPCF ist mit → iQoS nicht kompatibel.

iQoS

„Industrial Quality of Service“, ein Verfahren, bei dem für einzelne → Clients eine bestimmte → Bandbreite reserviert wird. Das Resultat ist eine mit hoher Wahrscheinlichkeit, jedoch nicht mit Bestimmtheit eingehaltene Antwortzeit. iQoS erfüllt also weniger scharfe Echtzeitanforderungen als → iPCF; es ist mit → iPCF nicht kompatibel.

ISM

„Industrial, Scientific and Medical“, ein Band des Funkspektrums, das unter anderem auch den 2,4- GHz-Frequenzabschnitt umfasst, der vom → 802.11-Protokoll verwendet wird.

LAN

„Local Area Network“, örtlich abgegrenztes Netzwerk im Gegensatz z. B. zum Internet.

Leckwellenleiter

Ein Koaxialkabel, dessen äußere Abschirmung in definierten Abständen unterbrochen ist. Als Konsequenz daraus erzeugt das Kabel ein räumlich begrenztes Funkfeld, das „formbar“ ist, da es der Krümmung des Kabels folgt.

Link Check

Eine Access Point-Funktionalität zur Überwachung der Verbindung mit den Clients. Verschiedene Ereignisse (An-, Abmelden der Clients, etc.) können automatisierte Reaktionen des APs (Versenden von Mails / Traps, Einschalten der *Fault*-LED, etc.) auslösen. Alle SCALANCE W Access Points unterstützen Link Check.

MAC

„Media Access Control“, ein Protokoll, mit dem der Zugriff auf ein Übertragungsmedium (Kabel, Funk) gesteuert wird, das nicht von allen Teilnehmern gleichzeitig benutzt werden kann.

MAC-Adresse

Eine weltweit eindeutige Identifikationsnummer für jede Hardware-Komponente, die in einem Netzwerk eine Rolle spielt. → MAC

Middleware

Software, die eine vermittelnde Funktion zwischen Betriebssystemen und Treibern einerseits und Anwender-Applikationen andererseits einnimmt.

MIMO

"Multiple Inputs, Multiple Outputs", ein Verfahren, bei dem jeder Funkteilnehmer gleichzeitig mit mehreren Antennen sendet bzw. empfängt. MIMO ist Teil des → IEEE → 802.11n-Standards.

MPI

„Multi-Point Interface“, ein Siemens-proprietärer RS 485-basierter Bus für die serielle → PROFIBUS-Kommunikation mit einer größeren Anzahl von Teilnehmern.

N-Connect

Ein Anschlusssystem für IWLAN-Antennen.

OFDM

„Orthogonal Frequency Division Multiplex“, ein Modulationsverfahren bei IEEE 802.11a und g.

PCF

„Point Coordination Function“, ein Organisationsmodell für Funknetze.

PoE

„Power over Ethernet“, Spannungsversorgung von Busteilnehmern über das Industrial Ethernet-Kabel.

Polling

Das regelmäßige Abfragen von Zustandsdaten oder Variablen von einer Datenquelle („Server“) durch einen Klienten. (Dieser Klient ist nicht notwendigerweise der Client eines WLANs.) Die Alternative dazu ist die eventgesteuerte Übertragung. Hier überträgt der Server von sich aus Daten zu den Klienten, sobald Änderungen in den Daten auftreten.

PROFIBUS

Ein Feldbussystem zur seriellen Datenübertragung im Automatisierungsbereich, das auf den → MPI-Hardwarespezifikationen basiert.

PROFINET

Eine Erweiterung der Ethernet-Kommunikationsstandards, um den Anforderungen des „Industrial Ethernet“, d. h. dem Einsatz in einer Industrieumgebung, gerecht zu werden. Neue Eigenschaften sind die Maßnahmen zur Steigerung der Übertragungssicherheit und Ausfallsicherheit sowie die Verwendung robuster Komponenten etc. Die SCALANCE-Produktgeneration wurde für den Einsatz mit PROFINET entworfen.

PROFIsafe

Eine Protokollerweiterung für → PROFIBUS und → PROFINET, mit deren Hilfe die Übertragungssicherheit und -zuverlässigkeit deutlich erhöht wird.

PSK

„Pre-Shared Key“, ein Verfahren zur Authentifizierung im Rahmen der → WPA/WPA2-Protokolle.

Quality of Service

Eine im Rahmen eines Netzwerks garantierte Übertragungsqualität.

RADIUS

„Remote Authentification Dial In User Service“, ein Zugangskontrollverfahren, bei dem die Authentifizierung zwischen Client und Access Point über einen dritten, separaten Server abgewickelt wird, auf dem die Zugangsdaten gespeichert sind.

Rapid Spanning Tree

Ein Verfahren zur Optimierung der Datenpfade in Netzwerken, ähnlich dem → Spanning Tree. Rapid SpanningTree wurde jedoch dahin gehend optimiert, beim Ausfall eines Access Points die Rekonfigurationszeit möglichst gering zu halten.

RC4

Ein Verschlüsselungsalgorithmus, der im Rahmen der Standards → WEP und → WPA eingesetzt wird.

RCoax

Ein → Leckwellenleiter, mit dessen Hilfe echtzeitfähige Funknetze begrenzter Reichweite aufgebaut werden können, die sich besonders für → Clients mit festen Bewegungspfaden (z. B. fahrerlose Transportsysteme) oder in stark abgeschatteten Umgebungen (z. B. Tunnels) eignen.

RFID

„Radio Frequency IDentification“, ein Verfahren, bei dem Gegenstände (z. B. Bücher einer Bibliothek) mit passiven Funk-Transpondern ausgerüstet werden. Die Transponder antworten auf Anfrage eines Senders (z. B. eines Lesegeräts an der Ausgabestelle der Bibliothek) mit einer ID, anhand derer sie nachverfolgt werden können. Die Transponder sind klein, billig und werden durch die Energie des Lesegeräts gespeist. Reichweite und Datenkapazität sind jedoch gering.

Roaming

Die Bewegung eines → WLAN-Teilnehmers von einer Funkzelle zur nächsten.

R/SMA

„Reverse (Polarity) SubMiniature (version) A (Connector)“, ein Anschlusssystem für WLAN-Antennen.

RSTP

„Rapid Spannung Tree Protocol“, ein Algorithmus, mit dessen Hilfe Switches in einem Netzwerk selbsttätig die optimalen Wege zur Datenübertragung zwischen zwei Endteilnehmern ermitteln und beim Ausfall einer Übertragungsstelle auch Alternativen ermitteln. Siehe Kapitel 4.5.3.

RTS / CTS

„Read-to-Send / Clear-to-Send“, ein Verfahren zur Vermeidung von Netzwerkkollisionen und zur Vermeidung des → Hidden-Station-Problems.

Spanning Tree

Ein Verfahren zur Optimierung der Datenwege in (Funk-) Netzen. Das Spanning Tree-Verfahren ermittelt physikalisch redundante Netzwerkstrukturen und verhindert Schleifenbildung durch Abschalten redundanter Wege. Der Datenverkehr erfolgt dann ausschließlich auf den verbleibenden Verbindungswegen. Wenn der bevorzugte Datenweg ausfällt, sucht der Spanning Tree-Algorithmus den effizientesten Weg, der mit den verbliebenen Netzteilnehmern möglich ist. Siehe auch → Rapid Spanning Tree

Spoofing

Svw. „Parodie, Schwindel“, ein Sammelbegriff für Angriffe auf Netzwerke, bei denen der Angreifer seine eigene IP- oder MAC-Adresse („IP-Spoofing“, „MAC-Spoofing“) verschleiert und damit die „Identität“ eines (rechtmäßigen) Netzteilnehmers vorgaukelt.

SSID

„Service Set Identifier“, im Rahmen eines → “Wi-Fi”-WLANs der Name eines Netzwerks, der gleichzeitig allen seinen Netzteilnehmern bekannt sein muss und der Teil jeder übertragenen Nachricht ist. SSIDs alleine bieten nur einen extrem schwachen Zugriffsschutz gegenüber Dritten und sollten auf jeden Fall durch andere Verschlüsselungsverfahren ergänzt werden.

SSL

„Secure Sockets Layer“, ein Protokoll zur verschlüsselten Datenübertragung im Internet, das seine Sicherheit durch die Verwendung von „Public Key“-Algorithmen erhält.

TKIP

„Temporary Key Integrity Protocol“, ein Verfahren zum dynamischen Wechsel der Schlüssel in einem → WLAN.

TPC

„Transmit Power Control“, eine Erweiterung des → 802.11h-Standards, bei dem nur die Sendeleistung abgestrahlt wird, die für den störungsfreien Empfang der bekannten Clients benötigt wird. Dadurch wird die Generierung von Überreichweiten verhindert.

UMTS

„Universal Mobile Telecommunications System“, ein Mobilfunkstandard für Datenübertragungen mit hoher Kapazität.

VLAN

„Virtual LAN“, eine Protokollerweiterung für drahtgebundene und drahtlose Netze, mit denen ein physikalisches Netz in mehrere logische Subnetze unterteilt werden kann. → VPN

VNS

„Virtual Network Services“, die Organisation logischer Netzwerke innerhalb eines oder mehrere physikalischer Netzwerke.

VoIP

„Voice over IP“, die Übertragung von Telefongesprächen über das Internet oder andere IP-basierte Netzwerke.

VPN

„Virtual Private Network“, eine mit → VLANs eng verwandte Protokollerweiterung, bei der der Datenverkehr eines (virtuellen) Subnetzes innerhalb eines größeren Netzes „getunnelt“, d. h. für die anderen Teilnehmer unsichtbar geführt wird. Diese Eigenschaft macht VPNs geeignet zur Erhöhung der Sicherheit eines Netzes.

WAN

„Wide Area Network“, ein begrenztes, aber weiter als ein → LAN ausgedehntes Netzwerk.

WBM

„Web Based Management“, Konfiguration eines Access Points oder Clients über ein Web-Interface.

WDS

„Wireless Distribution System“, ein → Infrastrukturmodus für → WLANs, bei dem die → Access Points ein redundantes Netz aufbauen.

WEP

„Wire Equivalent Protocol“, ein Verschlüsselungsverfahren im drahtlosen Datenverkehr.

Wi-Fi

Von der Herstellervereinigung „WiFi-Alliance“ eingeführte Bezeichnung für→ WLAN-Produkte, die kompatibel mit einem bestimmten Subset des → 802.11-Standards sind; gelegentlich auch (inkorrekterweise) als Synonym für „WLAN“ im Allgemeinen gebraucht.

Wireless HART

(„Highway Addressable Remote Transducer“), die drahtlose Variante eines Feldbus-Standards.

WLAN

„Wireless Local Area Network“, soviel wie „lokales Funknetz“, also ein funkbasiertes → LAN.

WMM

„Wireless Multimedia Extensions“, ein Subset des → IEEE → 802.11e-Standards.

WPA, WPA2

„Wi-Fi Protected Access“, zwei Verschlüsselungsverfahren im drahtlosen Datenverkehr.

Zigbee

Ein dem → WirelessHART ähnlicher Funkstandard, der allerdings für den Betrieb in der Heim- und Gebäudeautomatisierung vorgesehen ist.

Zustimmtaster

Beim Umgang in gefährdeten Umgebungen können durch das Personal handgehaltene Zustimmtaster verwendet werden, die drei Tasterpositionen besitzen. Ein Betrieb des durch die Zustimmtaster kontrollierten Geräts ist nur in der mittleren Position mit einem mäßig festen Handgriff möglich. Wird der Zustimmtaster ganz losgelassen oder sehr fest gehalten („Panikschaltung“), so wird der Not-Halt des Geräts ausgelöst.

12 Literaturhinweise

Hinweis Webseiten mit relevantem Material sind - soweit sinnvoll - bereits direkt im Text verlinkt.

Tabelle 12-1

	Thema
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	https://support.industry.siemens.com/cs/ww/de/view/22681042
\3\	

13 Historie

Tabelle 13-1

Version	Datum	Änderung
V1.0	01.04.2006	Erste Ausgabe
V2.0	01.01.2010	Diverse Aktualisierungen
V2.1	08.02.2011	Diverse Aktualisierungen
V3.0	04/2013	Komplette Überarbeitung der Struktur und Erweiterung mit den neuen Funktionen / Geräte für IEEE 802.11n
V4.0	01/2016	Einfügen der neusten Geräte/ Antennen. Entfernung alter Geräte nach Standard IEEE 802.11a/b/g; Aktualisierung der Bilder