

.steute

// DAS FUNKBUCH
EVOLUTION UND KOMMUNIKATION



// DAS FUNKBUCH

EVOLUTION UND KOMMUNIKATION

// Inhalt

009	Vorwort der Geschäftsleitung
011	Einleitung
015	Allgemeines zum Thema Funk
023	Historie Funk
039	Eigenschaften der Funkwellen
049	Grundlagen der Funktechnik: Frequenzen
061	Das Funkfeld
073	Der Funk-Kanal
087	Funk in der industriellen Automation
095	Grundlagen der Funktechnik: Technologien und Standards
139	Koexistenz und Sicherheit
169	Antennentechnik
181	Wireless-Technologien und -Produkte von steute für die Medizintechnik
193	Wireless-Technologien und -Produkte von steute für die Industrie
205	Ausblick
209	Anhang

// Vorwort der Geschäftsleitung

Kommunikation über elektromagnetische Wellen – kurz als Funk bezeichnet – hat eine spannende Geschichte hinter sich. Von den ersten Versuchen, mit einem Lichtbogen elektromagnetische Wellen zu erzeugen, bis zum modernsten Low-power-ASIC Sender ist vieles entdeckt, geforscht und letztendlich in brauchbare Lösungen überführt worden. Das gilt vor allem für den Bereich der »Consumer Electronics«: Vom Radio über das Mobiltelefon bis zum Funk-Thermometer sind wir heute von Funk-Geräten umgeben.

Auch in der Industrie ist Funk keineswegs ein neues Thema. Aber für viele Ingenieure ist z. B. der Aufbau von Funk-Topologien oder die Integration von Funk-Endgeräten in die Steuerung von Industrieanlagen kein vertrautes Gebiet. Es fehlt an technischer Information über die Theorie und Praxis von drahtloser Kommunikation in einem industriellen Umfeld. Und oft fehlt auch das Vertrauen, dass »Wireless«-Lösungen unter den nicht immer günstigen industriellen Umgebungsbedingungen die gewünschte Verfügbarkeit erreichen.

Diese Befürchtungen sind unbegründet, wie die umfassenden Erfahrungen von steute mit »Wireless Automation« auch in explosionsgefährdeten Bereichen sowie mit kabellosen Bediensystemen im mindestens ebenso anspruchsvollen Anwendungsfeld der Medizintechnik zeigen.

Dennoch: In der Industrie herrscht nach wie vor Informationsbedarf zum Thema Funk. Das vorliegende Buch möchte einen Beitrag dazu leisten, diese Informationslücke zu schließen – auf ganz grundlegende, dabei immer praxisorientierte, aber auch unterhaltsame Art und Weise.

Mit diesem Buch erfüllen wir uns aber auch selbst einen Wunsch. Denn die Neugier bei steute, tiefer in die grundlegenden Themengebiete unserer täglichen Entwicklungsarbeit einzudringen, kennt kaum Grenzen. Unsere Hauptaufgabe besteht darin, dieses Wissen und die daraus entstehenden Ideen in kluge, sinnvolle und praxisgerechte Produkte umzusetzen. Genau das streben wir mit unserem Programm an Funk-Lösungen für den Maschinen- und Anlagenbau sowie für die Medizintechnik an. Auf welchen Grundlagen wir dabei aufbauen, erläutern wir mit diesem »Funkbuch«.

Wir freuen uns, dass wir für dieses Vorhaben mit Dipl.-Ing. Wolfram Gebhardt und Prof. Dr.-Ing. Jörg Wollert zwei ausgewiesene Funk-Experten gewinnen konnten, die die Hauptlast des Schreibens übernommen haben und denen wir ausdrücklich danken. Ihrem beeindruckenden Fachwissen und – was mindestens ebenso wichtig ist – der seltenen Gabe, dieses Wissen zu teilen und zu vermitteln, verdankt dieses Buch seine Existenz.

Wir wünschen Ihnen eine informative und anregende Lektüre!

Marc Stanesby
Geschäftsführer, steute Schaltgeräte GmbH & Co. KG

// Einleitung

Funk – eine Trendtechnologie

Die kulturelle Entwicklung der Menschheit ist wesentlich durch die Kommunikation bestimmt. Ein wesentliches Problem der sprachlichen Kommunikation liegt jedoch in der geringen Reichweite der Schallwellen. Erst mit der Entwicklung der funkgestützten Kommunikation wurde eine fast unbegrenzte Reichweite möglich sowie eine Vielfalt der Informationsübertragung mit Ton, Bild und Daten und zusätzlich eine hohe Flächendeckung: der Rundfunk.

Albert Einstein sagte in seiner Festrede zur Eröffnung der Funkausstellung 1930 in Berlin: »Wenn Ihr den Rundfunk hört, so denkt daran, wie die Menschen in den Besitz dieses wunderbaren Werkzeuges der Mitteilungen gekommen sind. Denkt an Maxwell, der die Existenz elektrischer Wellen auf mathematischem Wege aufzeigte, und an Hertz, der sie zuerst mit Hilfe des Funkens erzeugte und nachwies.«

Heute ist Funk eine Trendtechnologie, die weite Verbreitung findet – von der Mobiltelefonie über kabelfreie Internetzugänge bis zur Kfz-Funkfernbedienung. Mit dem Erfolg der vielen kleinen Funkgeräte im Consumer-Markt und der Telekommunikation ist es nur zu verständlich, dass in den letzten zehn Jahren auch in der industriellen Kommunikation immer wieder neue Anwendungsbereiche erschlossen wurden.

Kaum ein Anbieter von Feldbustechnik oder intelligenten Komponenten konnte sich dem allgemeinen Trend in Hinblick auf die Befreiung vom Kabel entziehen. Dies verwundert kaum, da die Notwendigkeit von Funkstandards in der IT-Welt anerkannt ist und die Automatisierungstechnik immer stärkeren Wert auf Mobilität und Flexibilität legt.

Funk in der Industrie-Automation – Chancen und Risiken

Doch gerade in der Automation bringt die Freiheit von Stecker und Kabel nicht nur Vorteile, sondern auch Risiken mit, die oft nicht bekannt sind oder nicht beachtet werden. Dass die neuen Technologien dennoch einen vehementen Zuspruch erreichen, liegt am deutlichen Zuwachs an Komfort, Flexibilität und Mobilität. Dieser Zuwachs ermöglicht einen Innovationsschub für die Mensch-Maschine-Schnittstelle, und vollkommen neue Ansätze in der Bedienung von Geräten, Maschinen und Anlagen werden möglich.

Doch der Einsatz von Funktechnik will besonnen geplant werden. Zu unterschiedlich sind die Anwendungsfälle und damit die möglichen Realisierungen. Eine einzige, universelle Funktechnik für alle Anwendungen kann es nicht geben und der einfache Ersatz eines Kabels durch eine Funkstrecke wird in vielen Fällen ein Projekt zum Scheitern bringen – aus Unkenntnis und überzogener Erwartungshaltung.

Ziel: Die richtige Funk-Technologie für die jeweilige Anwendung

Daher sind Verunsicherungen in der Praxis an der Tagesordnung. Welche der vielen Technologien von Bluetooth über EnOcean, Nanonet, WIMAX und WLAN bis hin zu Z-Wave und ZigBee schließlich die Gunst des Kunden finden werden, hängt nicht nur von einer qualifizierten Beratung, sondern auch von umfassenden technischen Kenntnissen des Anwenders selbst ab. Nicht jede Technik wird jeder Anforderung gerecht.

Und hier liegt dann auch das Erfolgspotential verborgen – das Finden der richtigen Technologie für die richtige Anwendung. Für den Endanwender ist es zunächst nebensächlich, wie diese Technik heißt und wie sie im Detail funktioniert – er möchte nur ein zuverlässig funktionierendes Gerät besitzen, das seinen Zuverlässigkeits- und Leistungsanforderungen gerecht wird. Der Markt der Anbieter hat das bereits erkannt und darauf reagiert.

Große Kreativität der Anwender

Doch bei aller Kreativität der Hersteller: Häufig sind die Anwender nochmals kreativer. Systeme werden in Applikationen eingesetzt, von denen der Hersteller nicht einmal zu träumen gewagt hätte – aber dennoch erwartet der Anwender eine zuverlässige Funktionalität.

Zusammenfassend kann man feststellen, dass aus technischer Sicht fast für jede Fragestellung eine kabellose Lösung gefunden werden kann. Für einen erfolgreichen Einsatz ist jedoch ein verantwortungsvoller Umgang mit den Funktechnologien notwendig. Denn auch eine noch so große Kreativität kann physikalische Gesetzmäßigkeiten nicht aufheben. Auch wenn man von Funktechnik in der Automation und Consumer-Technik begeistert ist, gilt nach wie vor der Grundsatz: »Wo ein Kabel möglich ist, sollte es auch verwendet werden«. Funk einzusetzen, nur weil es Funk gibt, ist nicht sinnvoll. Vielmehr muss der Nutzen unmittelbar vorhanden sein. In diesem Werk soll daher ein kleiner Überblick zu den technologischen Chancen und Grenzen gegeben werden.

// Allgemeines zum Thema Funk

01

Evolution und Kommunikation

// Evolution und Kommunikation

Die Natur hat eine Vielfalt von Verfahren zur Informationsübertragung oder Kommunikation entwickelt. Die hoch differenzierte Silbensprache des Menschen hat eine grundlegende Voraussetzung für den Aufbau von Hochkulturen geschaffen.

In beiden Fällen kam es zu spannenden Wechselwirkungen zwischen den Kommunikationspartnern und ihren Kommunikationsverfahren. Während die natürlichen Informationsübertragungen mechanische, chemische, akustische und optische Verfahren nutzen, hat der Mensch mit der Erfindung der elektrischen Verfahren und besonders der Funkverfahren für die Kommunikation eine eigene Größe in der Entwicklung der Menschheit und ihrer Kultur geschaffen. Dies wird deutlich, wenn man sich die verschiedenen Kommunikationsverfahren vergegenwärtigt.

Mechanische Kommunikation

Der vermutlich älteste Sinn ist der Tastsinn. Ihn nutzen Seeanemonen, Korallen, Spinnen und andere einfache Lebewesen zum Erfassen von Beute. Durch die mechanische Berührung oder das Spüren von Erschütterungen werden Informationssignale übertragen. Viele Tiere spüren vor einer Naturkatastrophe feinste Erdbebenwellen und ergreifen Sicherheitsvorkehrungen. Der Mensch nutzt den Tastsinn ebenfalls, z. B. in der Blindenschrift oder als Körperkontakt zwischen Mutter und Kind. Die mechanische Kommunikation kann keine oder nur sehr kurze Entfernungen überbrücken.

Chemische Kommunikation

Signale können auch als Düfte oder Geschmack übertragen werden. Pflanzen »schreien« mit Düften um Hilfe, wenn sie von Fressfeinden angegriffen werden, und rufen so deren natürlichen Gegner herbei. Oder sie verändern ihren Geschmack so, dass die Fressfeinde von ihnen ablassen. Bie-

nen und Kolibris orientieren sich bei der Futtersuche an Düften. Tiere und Menschen nutzen Duft und Geschmack von Futter und Lebensmitteln, um Nahrung zu finden oder auf Bekömmlichkeit zu prüfen. Berühmt sind Pheromone als duftenden Lockstoffe zur Partnerfindung über einige Entfernung und in unübersichtlicher Umgebung. Nicht nur Tiermütter können ihre Kinder am Geruch sicher erkennen – auch beim Menschen ist dieses Phänomen nachgewiesen.

Wichtig ist, dass die chemische Kommunikation im Unterschied zur mechanischen Kommunikation abstandsfähig ist – von nahen Entfernungen bis zu einigen hundert Metern.

Akustische Kommunikation

Die akustische Kommunikation hat sich artspezifisch ausdifferenziert und in ihrem Informationsumfang (ihrer »Intelligenz«) flexibel angepasst. Tiere übertragen durch arteigene Laute durchaus komplexe Inhalte. Schon durch die Wahl der Tonfrequenzen können manche Tierarten wie Elefanten und Wale per Infraschall große Entfernungen von bis zu 40 km überbrücken, um sozialen Zusammenhalt zu pflegen.

Für den Menschen hat die Erfindung der Sprache den größten Entwicklungsschub auf dem Weg zum Homo sapiens gebracht. Daneben haben die Menschen aber noch andere akustische Verfahren für Übermittlung von Informationen entwickelt – zum Beispiel das Jodeln, das in einem durch die Echowirkung gestörten Umfeld bei Entfernungen bis etwa 1000 Metern durchaus sinnvoll ist, wenn auch mit eingeschränkter Informationsdichte.

Einen deutlichen Entwicklungsschub in der akustischen Kommunikation gab die Verwendung von Trommeln, Sprachrohren, Trompeten, Signalhörnern und anderen Geräten. Sie erlauben die Informationsübermittlung über größere Entfernungen oder in lärmgefüllter Umgebung (z. B. in





Stadien oder im Kampflärm) ausreichend zuverlässig zu kommunizieren.

Zudem nutzt der Mensch heute die akustische Kommunikation für seine Kunst (Musik) und für medizinische (Ultraschall) oder therapeutische (psychosomatische) Behandlung.

Die akustische Kommunikation hat drei wesentliche Vorzüge:

- gute Abstandsfähigkeit bzw. Reichweite
- gute Raumabdeckung (Ortsreichbarkeit in Luft und Wasser) und ein mäßiges Durchsetzungsvermögen (Lautstärke)
- flexibel anpassungsfähig an die Nutzer und deren unterschiedlich differenzierte Sprachen und Anwendungen.

Daher ist die akustische Kommunikation eine bedeutende »Erfindung« auf dem Wege zur Menschheit und zur kulturellen Entfaltung des Menschen.

Optische Kommunikation

Die Entwicklung des Lebens fand unter ständigem Sonnenlicht statt. Daher reagieren fast alle Pflanzen und Tiere und auch Menschen auf optische Informationen. Die meisten Lebewesen sind sogar existenziell vom Licht abhängig.

Pflanzen rufen z. B. durch ihre Form und Farbe aktive Helfer zur Erhaltung der Art herbei (Blütenbestäubung). Tiere erkennen ihre Umwelt und ihre Artgenossen mit dem Gesichtssinn. Manche Arten verändern ihre Färbung zur Tarnung oder mit dem Ziel der Kommunikation bei der Partnersuche, einige wie die Glühwürmchen können sogar aktiv leuchten.

Tiere und Mensch nutzen das Licht zur sozialen Kommunikation durch ihre Körpersprache. Wenn der Hund mit dem Schwanz wedelt, freut er sich. Wenn die Katze das Gleiche tut, ist sie aufgeregt oder missgestimmt. Daher kommt es zwischen

den beiden häufig zu Missverständnissen. Nur der Mensch – wenn er mit der visuellen Sprache von Hund und Katze vertraut ist – versteht beide richtig. Alle geselligen Tiere pflegen eine recht differenzierte Körpersprache. Bei den Primaten ist das Mienenspiel besonders gut entwickelt, Affen sagen mehr durch Mimik als durch Töne.

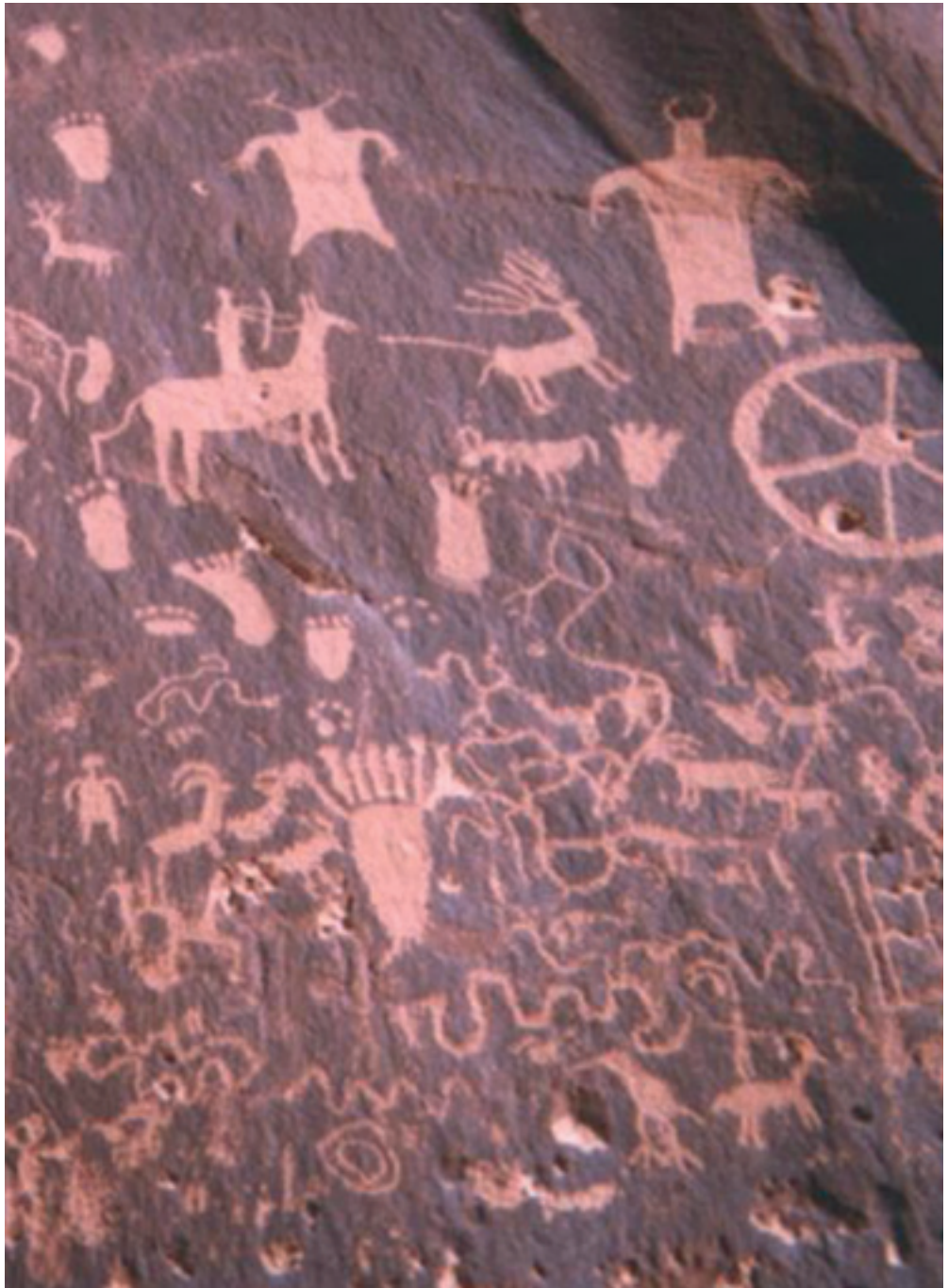
Optische Kommunikation war für den Menschen anfangs entscheidend für das Überleben, denn der aufrechte Gang sorgte für bessere Sicht und durch Zeichensprache konnte er z. B. bei der Jagd über mittlere Entfernungen je nach Sichtweite kommunizieren.

Er erfand Lichtzeichen, wobei Feuersignale besonders nachts und Rauchsignale am Tage auch große Entfernungen überbrückten, sofern die Bedeutung der Signale vorher vereinbart, also kodifiziert war. Auch in der Seefahrt war optische Kommunikation das Mittel der Wahl über Entfernungen bis zu 40 Seemeilen (75 km). Leuchtfeuer auf Türmen und Flaggensignale wurden genutzt. Auch die Römer setzten die optische Kommunikation am Limes von Wachturm zu Wachturm ein.

Ein Höhepunkt dieser Entwicklung war die Entfaltung der darstellenden Kunst zur bildlichen Kommunikation abstrakter Sachverhalte von der Jagd bis hin zur Religion.

Der wichtigste evolutionäre Schub war die Erfindung der Schrift – zunächst als reine Bilderschrift, später als Silbenschrift (Hieroglyphen) und Buchstabenschrift. Damit wurde Dokumentation möglich und die Kommunikation konnte von der Echtzeit (»online«) zur versetzten Zeit (»offline«) verlagert werden.

Die schriftliche Kommunikation als eine Ausprägung der optischen Kommunikation mit den Vorteilen der Dokumentation und Speicherung, der Überwindung beliebiger Entfernungen (ggf. mit



Zeitverlust) und der Darstellung konkreter und abstrakter Sachverhalte wurde nun das Kernstück der menschlichen Kommunikation.

Die Vorteile der optischen Kommunikation sind also:

- große Reichweite (bei Sichtverbindung)
- hohe Raumabdeckung, allerdings begrenzt auf hindernisfreie Sicht
- Durchsetzungsvermögen und Diskretion (Richtwirkungsmöglichkeit)
- in schriftlicher Form dokumentierbar und lang-lebig
- neue Perspektiven für Kunst, Kultur und Wissenschaft (z. B. Astronomie)

Zusammenfassende Bedeutung der Kommunikation für die Menschheit

- Die im Verlauf der Evolution entwickelten Kommunikationsverfahren verliefen parallel zu den Entwicklungsstufen des Lebens.
- Ältere Kommunikationsverfahren werden von den höher entwickelten Verfahren nicht abgelöst, sondern erweitert.
- Alle Kommunikationsverfahren bilden gemeinsam ein System, das an die jeweilige Lebensform der Arten angepasst ist.
- Die akustische und die optische Kommunikation schaffen die Voraussetzung für die Entfaltung der Menschheit hinsichtlich Kunst, Kultur und Wissenschaft.
- Die Menschheit wird auch zukünftig alle gewachsenen evolutionären Kommunikationsverfahren nutzen.
- Eine Erweiterung der Kommunikation ist möglich, aber nur hinsichtlich bestimmter Eigenschaften wie Reichweite, Raumabdeckung, Diskretion und Durchsetzungsvermögen gegen Umwelteinflüsse.
- Technische Kommunikationsverfahren, vor allem Funk, befreien die natürlichen Verfahren von bisherigen Fesseln und bringen so einen neuen wesentlichen Entwicklungsschub.

// Historie Funk

02

Die Entdeckung der Funkwellen

Die ersten Funkanwendungen

Meilensteine der Funkentwicklung

Maxwellgleichungen im gaußschen cgs-System

$$\text{Ampèresches Gesetz} \quad \nabla \cdot \mathbf{H} = 4\pi \frac{\mathbf{j}}{c} + \frac{1}{c} \frac{\partial \mathbf{D}}{\partial t}$$

$$\text{Induktionsgesetz} \quad \nabla \cdot \mathbf{E} = -\frac{1}{c} \frac{\partial \mathbf{B}}{\partial t}$$

$$\text{Coulombsches Gesetz} \quad \nabla \cdot \mathbf{D} = 4\pi \rho$$

$$\text{Gaußsches Gesetz des Magnetismus} \quad \nabla \cdot \mathbf{B} = 0$$

Die Maxwellschen Gleichungen in moderner Schreibweise

// Die Entdeckung der Funkwellen

Die Menschen entdeckten die Elektrizität erst relativ spät – was darin begründet ist, dass der Mensch keinen Sinn, d. h. kein eigenes Sinnesorgan für die Wahrnehmung der Elektrizität hat. Im antiken Griechenland stellte man erstmals fest, dass ein mit organischen Stoffen (Tücher, Katzenfell) geriebener Bernstein nichtmetallische Teilchen wie Staub oder Papyrusstückchen ansaugt. Heute wissen wir, dass sich der Bernstein dabei elektrisch auflädt. Bernstein heißt altgriechisch »Elektron«; daher kommt der Name für das elektrisch geladene Elementarteilchen.

Die Entdeckung des Magnetismus reicht vermutlich in die Zeit des Übergangs von der Antike zum Mittelalter zurück. So soll ein frei aufgehängtes Stück Magneteisenerz als nordweisender Kompass bereits vor der Wikingerzeit im 7./8. Jahrhundert von Seefahrern genutzt worden sein. Solche Erzbrocken waren selten, einige wurden auf der Babilonie gefunden, einer germanischen Burgan-

lage am Nordrand des Wiehengebirges (also unweit des steute-Firmensitzes), wo bereits in der La-Tène-Zeit Eisenverhüttung betrieben wurde.

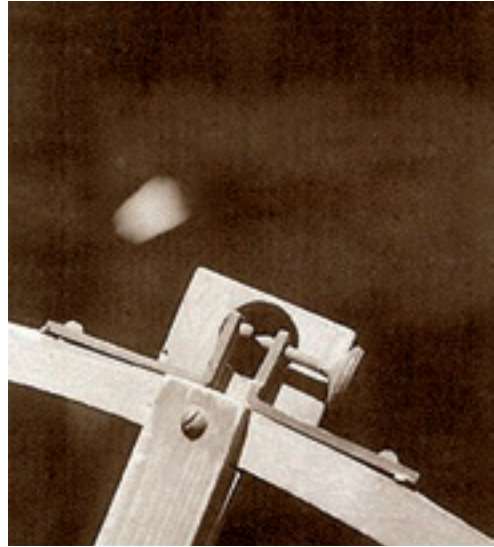
Mit dem Engländer Michael Faraday begann die systematische Erforschung des Elektromagnetismus. Er entdeckte 1814 die elektromagnetische Induktion und wies so einen Weg zur Erzeugung von Strom. 1836/37 entwickelte er daraus die Theorie des elektrischen und magnetischen Feldes, die auch nichtmetallische Materie und den freien Raum durchdringen müssten. Da er seine Theorie nicht mathematisch nachweisen konnte, glaubte ihm die Wissenschaft zunächst nicht.

Die Maxwellschen Gleichungen

Erst als 30 Jahre später (1864/1865) der schottische Mathematiker und Physiker James Clark Maxwell seine bedeutenden Differentialgleichungen, die »Maxwellschen Gleichungen« entwickelte, konnte das Zusammenwirken von elektrischen und magnetischen Feldern nachgewiesen werden. Aus seinen Gleichungen ließ sich schon 1866 rein mathematisch ableiten, dass es



Heinrich Hertz



Versuchsanordnung zum experimentellen Nachweis elektromagnetischer Wellen

elektromagnetische Wechselfelder und Wellen geben müsste, die sich mit Lichtgeschwindigkeit ausbreiten.

Heinrich Hertz

Der tatsächliche Nachweis der vorausgesagten Wellen war 22 Jahre später, im Jahr 1888, Heinrich Hertz vorbehalten.

Hertz studierte in Berlin bei berühmten Gelehrten wie Herrmann von Helmholtz und Robert Kirchhoff und promovierte bereits mit 23 Jahren. Helmholtz, der die Begabung seines Doktoranden erkannte, war begeisterter Anhänger der Maxwell'schen Theorie und seiner Feldgleichungen. Er gewann Heinrich Hertz für das Vorhaben, die elektromagnetischen Wellen experimentell nachzuweisen.

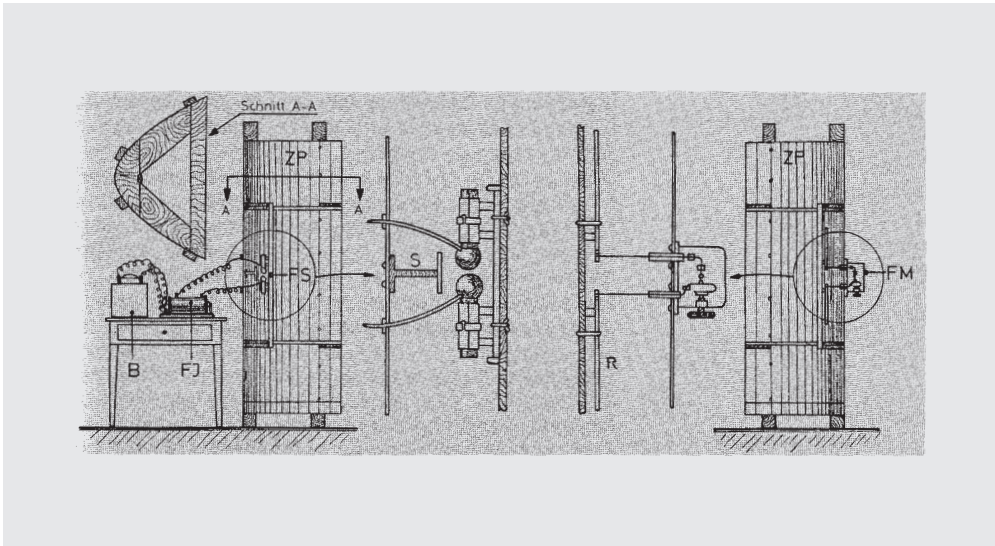
Hertz, der mit 26 Jahren zum ordentlichen Professor für Experimentalphysik an der Karlsruher Technischen Hochschule berufen worden war, begann 1887 im Alter von 30 Jahren mit seinen For-

schungsarbeiten. Damals war bereits bekannt, dass elektrische Entladungen über eine Spule, die durch eine Funkenstrecke unterbrochen ist, elektrische Schwingungen ausführen und an der Funkenstrecke elektrische Funken zeigen. Als er bei seinen ersten Versuchen die Funken untersuchte, entdeckte er zufällig, dass eine zweite Spule in der Nähe, die nicht elektrisch leitend mit der ersten Spule verbunden war, auch Funken zeigte.

Ausgangspunkt: Ein Zufallsfund

Aus diesem Zufallsfund musste Hertz schließen, dass von der Funkenstrecke und der Spule eine Energie in Form von Schwingungen oder Strahlungen durch den Raum zur zweiten Spule übertragen worden sein musste und dort zu den winzigen Funken führte. Heute wissen wir, dass dies die erste »Funkverbindung« war, wobei unsicher ist, ob Hertz schon erkannte, dass er damit elektromagnetische Wellen bereits entdeckt hatte.

Jedenfalls forschte Hertz nun gezielt weiter. Zur Vereinfachung nahm er statt der zweiten Spule



Die erste Richtfunkstrecke: Versuchsaufbau von Heinrich Hertz

Erste Untersuchungen der Eigenschaften von Funkwellen

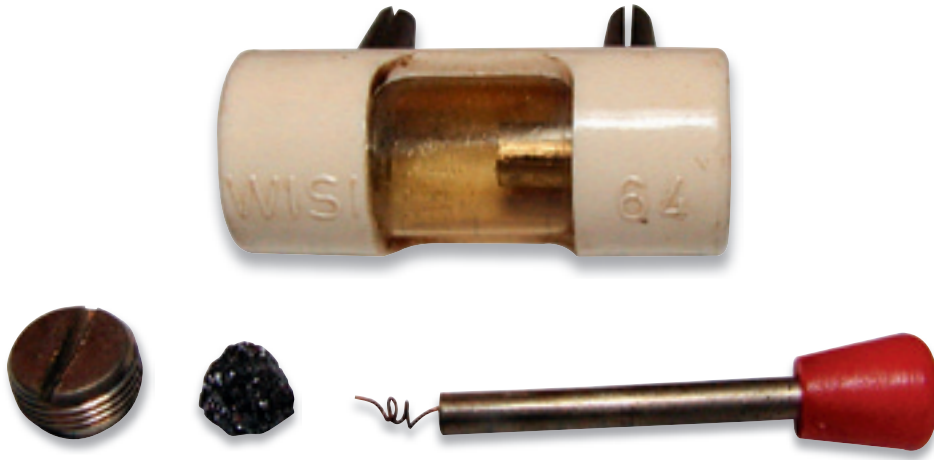
In einem weiteren Versuch nutzte Heinrich Hertz einen 2×2 m großen rechteckigen Holzrahmen, in den er parallele Drähte spannte. Hielt er diese Drähte parallel zu den sendenden Drähten (Antenne), so gab es keine Funken. Hielt er den Rahmen aber um 90 Grad gedreht, so war die Funkenbildung wieder da. Damit hatte er erkannt, dass es sich um Quer-/Transversalwellen handelt, die zudem noch polarisiert sind, wie Lichtwellen.

Nun prüfte er, ob sich diese Wellen ähnlich wie Licht beugen lassen. Dazu stellte er in den Ausbreitungsweg ein großes Prisma aus Hartpech mit der Grundfläche eines regelmäßigen Dreiecks bei einer Seitenlänge von 1,3 Metern und ca. 65 cm Höhe. Dieses Teil wog allein rund 600 kg. Es zeigte sich, dass die Funkwellen genau wie Lichtwellen am Glasprisma gebeugt werden und etwa den vorausberechneten Beugungswinkel hatten.

Zuletzt brachte er den Sendedipol in die Brennpunktlinie eines zylindrischen Parabolspiegels aus Zink und einen Empfangsdipol in einen gleichen Reflektor mit 1,5 m Öffnungsweite. Hierbei hatte er rechnerisch die Abmessungen der Reflektoren mit der Länge der Dipole abgestimmt. Diese Anlage arbeitete nun auf 66 cm Wellenlänge.

Innerhalb des gebündelten Funkwegs waren die gemessenen Funkenwerte hoch, außerhalb waren keine Funken nachzuweisen. Damit war die zum Licht analoge Bündelung bewiesen und die erste Richtfunkstrecke erfunden, wenn auch nur mit einer Reichweite von immerhin 16 Metern.

Durch seine gezielte Forschung hatte Hertz nicht nur die elektromagnetischen Wellen nachgewiesen, sondern zugleich auch deren Eigenschaften umfassend erforscht. Dabei hat er die gleichen Eigenschaften wie bei Lichtwellen gefunden und erkannt: »Das Licht ist eine elektrische Erscheinung ...«. Das war revolutionär. Eine praktische



Steckbarer Kristalldetektor mit Pyritkristall und Spitze

Anwendung seiner Funkwellen konnte sich Heinrich Hertz allerdings nicht vorstellen. Die diesbezügliche Anfrage eines Ingenieurs im Jahre 1889 hat er ausdrücklich verneint. Zu seinen Ehren wird die Einheit der Frequenz mit Hertz (Hz) bezeichnet.

// Die ersten Funkanwendungen

Die Hertzschen Versuche lösten in Europa eine Welle von Experimenten aus, die u. a. zum Ziel hatten, die Reichweite dieser Funkwellen zu vergrößern. Die bisherige Funkenstrecke im Empfangsring mit Lupe war viel zu unempfindlich und erforderte sehr hohe Sendeleistungen.

In Paris nutzte Edouard Branley 1890 einen Detektor zur Steigerung der Empfängerempfindlichkeit, der als Radioconducteur, Kohärer oder Fritter bezeichnet wurde. Branley erkannte auch die Bedeutung der Antenne: Er nannte sie Luftdraht. Der Engländer Oliver Joseph Lodge erhöhte die Empfindlichkeit weiter durch Einführung eines

Resonanzschwingkreises. Im Jahre 1894 steigerte der Russe Alexander Stepanowitsch Popow in Petersburg die Empfindlichkeit der Empfangsschaltung durch Einfügen eines empfindlichen Relais, das eine elektrische Klingel einschaltete bzw. einen aus der bisherigen drahtgebundenen Telegraphietechnik bekannten Morseschreiber ansteuerte.

Die ersten Worte, die er anlässlich einer Vorführung am 24.03.1896 an der Universität von St. Petersburg mit diesem Tastfunk übertrug, waren »Heinrich Hertz«.

Ende des 19. Jahrhunderts: Funkübertragung von mehreren Kilometern

Dem Italiener Guglielmo Marconi gelang mit dieser Popowschen Schaltung eine Funkübertragung von etlichen Kilometern. Durch Vermittlung seiner englischen Mutter erhielt er 1897 ein britisches Patent auf diese Schaltung und Unterstützung für weitere erfolgreiche Funkversuche. Mit der steigenden Reichweite wuchs das Interesse



von Reedereien. Bald rüstete er Schiffe und Landstationen aus, gründete 1900 eine eigene Firma und besaß de facto das Monopol für Seefunkverbindungen. Berühmt wurde Marconi 1901 für die erste erfolgreiche Übertragung eines Funktelegramms von England über den Atlantik nach Neufundland in Amerika. Viele erfolglose Versuche waren vorausgegangen.

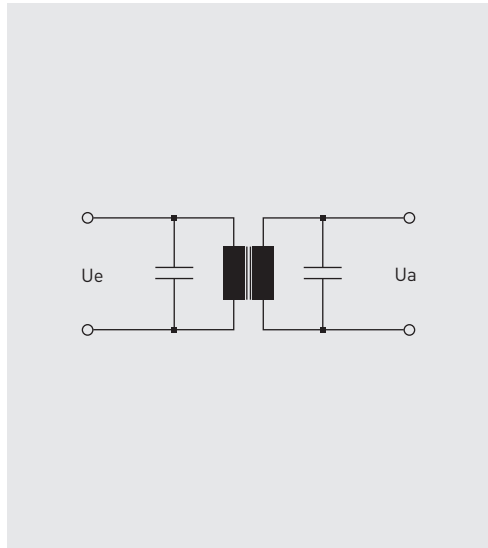
Auf deutscher Seite befassten sich ab 1897 Professor Adolf Slaby mit seinem Assistenten Georg Graf von Arco mit funktechnischen Versuchen. Kaiser Wilhelm II war technisch sehr interessiert und wohnte am 27.8.1897 einer Vorführung von Slaby bei. Der Kaiser wollte von der Monopolgesellschaft Marconis unabhängig bleiben und förderte die Versuche Slabys. So wurde zwei Monate später, am 07.10.1897, von Slaby bereits ein »Weltrekord« von 21 km Entfernung aufgestellt, wobei die zwischen 300 und 500 m langen Antennen von Fesselballonen getragen wurden. Im Frühjahr 1898 wurde auf der Strecke von Berlin nach Jüterbog 60 km Funkstrecke überbrückt.

Industrialisierung der Funktechnik

Im gleichen Jahr wurden dann auch deutsche Firmen gegründet, so die »Funkentelegraphische Abteilung« der AEG unter der Leitung von Graf von Arco sowie die »Funkentelegraphie GmbH« in Köln. Gleichzeitig gründete Professor Ferdinand Braun von der Technischen Hochschule in Straßburg die »Gesellschaft für Telegraphie System Professor Braun und Siemens & Halske m.b.H.« (Telebraun) in Hamburg. Zugleich hielt die Funktechnik Einzug beim Militär – zuerst bei der Marine, wenig später in der »Luftschifferabteilung« und beim Heer.

// Meilensteine der Funkentwicklung

Das Bestreben zur Vergrößerung der Reichweite und der Zuverlässigkeit der Funkverbindung führte zu vielen kleinen Verbesserungen, wobei auch mancher Irrweg beschritten wurde.

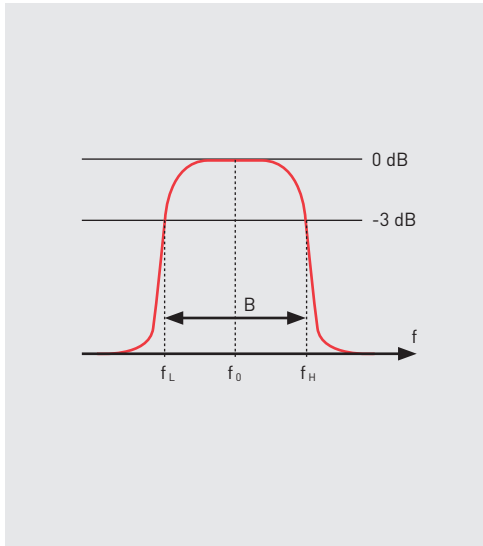


Schaltbild eines Bandpassfilters

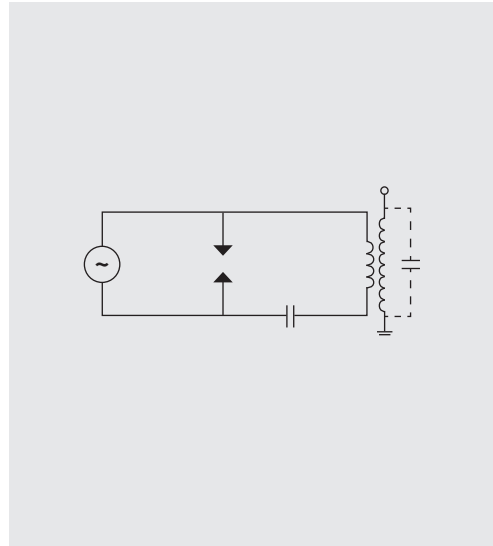
Höhere Empfindlichkeit der Empfänger

Zunächst galt es, die Empfindlichkeit der Empfänger zu steigern. Das erreichte man durch bessere Detektoren. Wilhelm Schloemilch erfand 1903 die »elektrolytische Zelle« mit zwei Platinelektroden in verdünnter Schwefelsäure. Diese Zelle wirkte bei einer kleinen Vorspannung sehr gut als Gleichrichter und löste rasch die Kohärer ab. Ab 1906 verdrängte der Kristalldetektor nach Professor Braun die elektrolytische Zelle als Empfangsgleichrichter. Von den vier Werkstoffen Pyrit, Silizium, Molybdän und Carborund erwiesen sich Pyrit und Carborund als am besten geeignet. Sie waren einerseits empfindlich genug für schwache Empfangssignale, andererseits robust gegenüber den eigenen starken Sendesignalen. Daher setzten sie sich als Kristalldetektor durch. Übrigens war der Empfangsgleichrichter das unverzichtbare Element zum späteren Tonempfang mit einem Kopfhörer.

Mit der Erfindung des Wellenmessers im Jahre 1902 konnte man Wellenlängen/Frequenzen ge-



Frequenzgang eines Bandpassfilters



Prinzipschaltbild eines Löschfunktensenders

zielt messen und abstimmen, um die Funkgeräte zu optimieren. Der Wellenmesser bestand aus einem Schwingkreis mit Drehkondensator und steckbaren Schwingspulen, die bei Resonanz über einen Detektor ein Galvanometer ausschlagen ließen. So funktionieren noch heutige Absorptionfrequenzmessgeräte wie das Grid-Dip-Meter oder die Satelliten-Finder.

Im Jahre 1904 verbesserte man die Trennschärfe, indem ein zweiter Schwingkreis in den Empfänger eingebracht wurde. Der abgestimmte Antennenkreis und die gute Filterung durch den zweikreisigen Bandfilter verminderten Störungen durch Nachbarsender und ermöglichten den parallelen Funkbetrieb auf mehreren Wellenlängen.

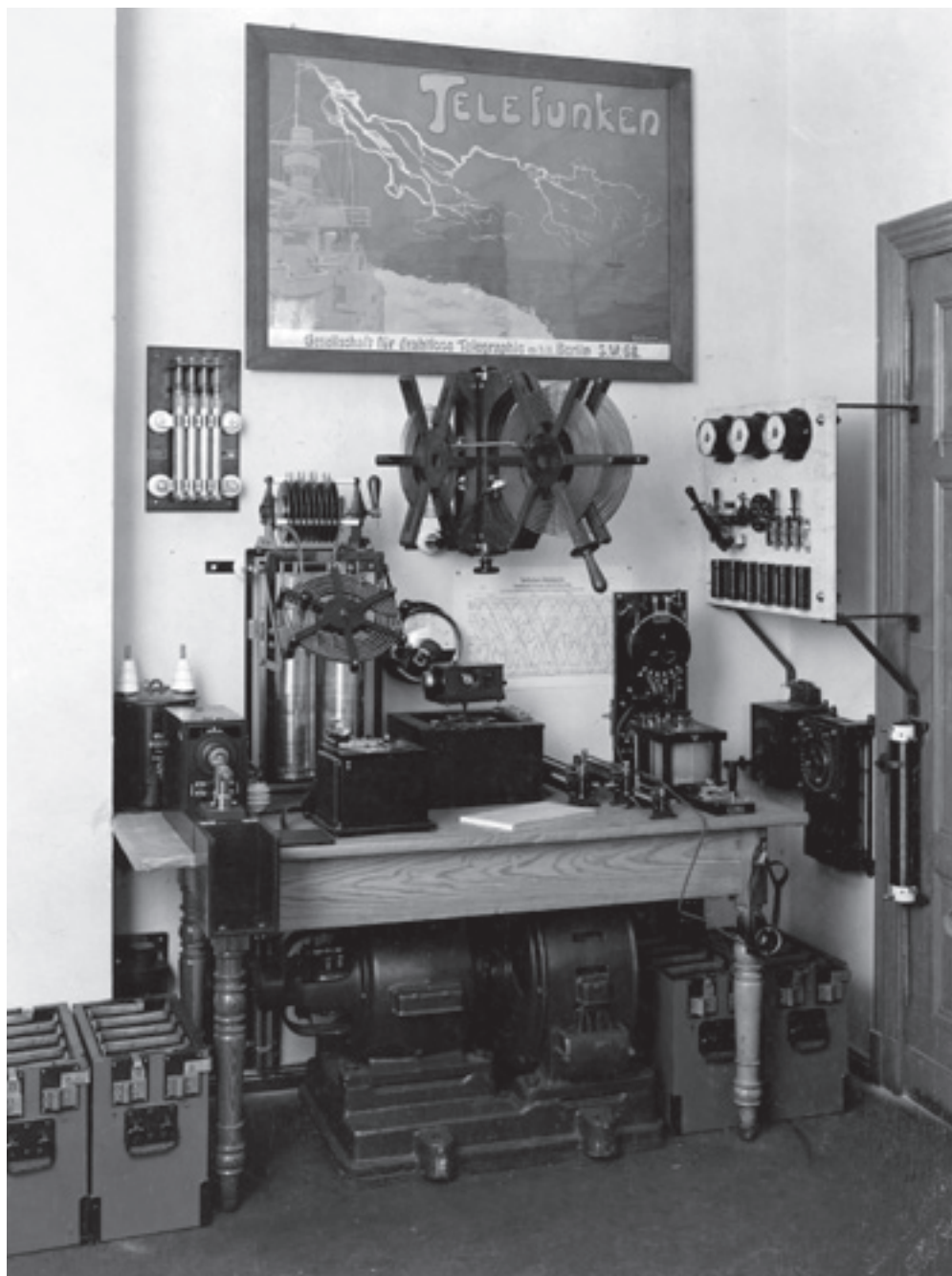
Verbesserung von Wirkungsgrad und Leistung

Auf der Senderseite versuchte man, den Wirkungsgrad und die Leistung zu verbessern. Die vom Funkeninduktor angestoßenen Wellen klangen sehr schnell ab. Erst als die Funkdauer der

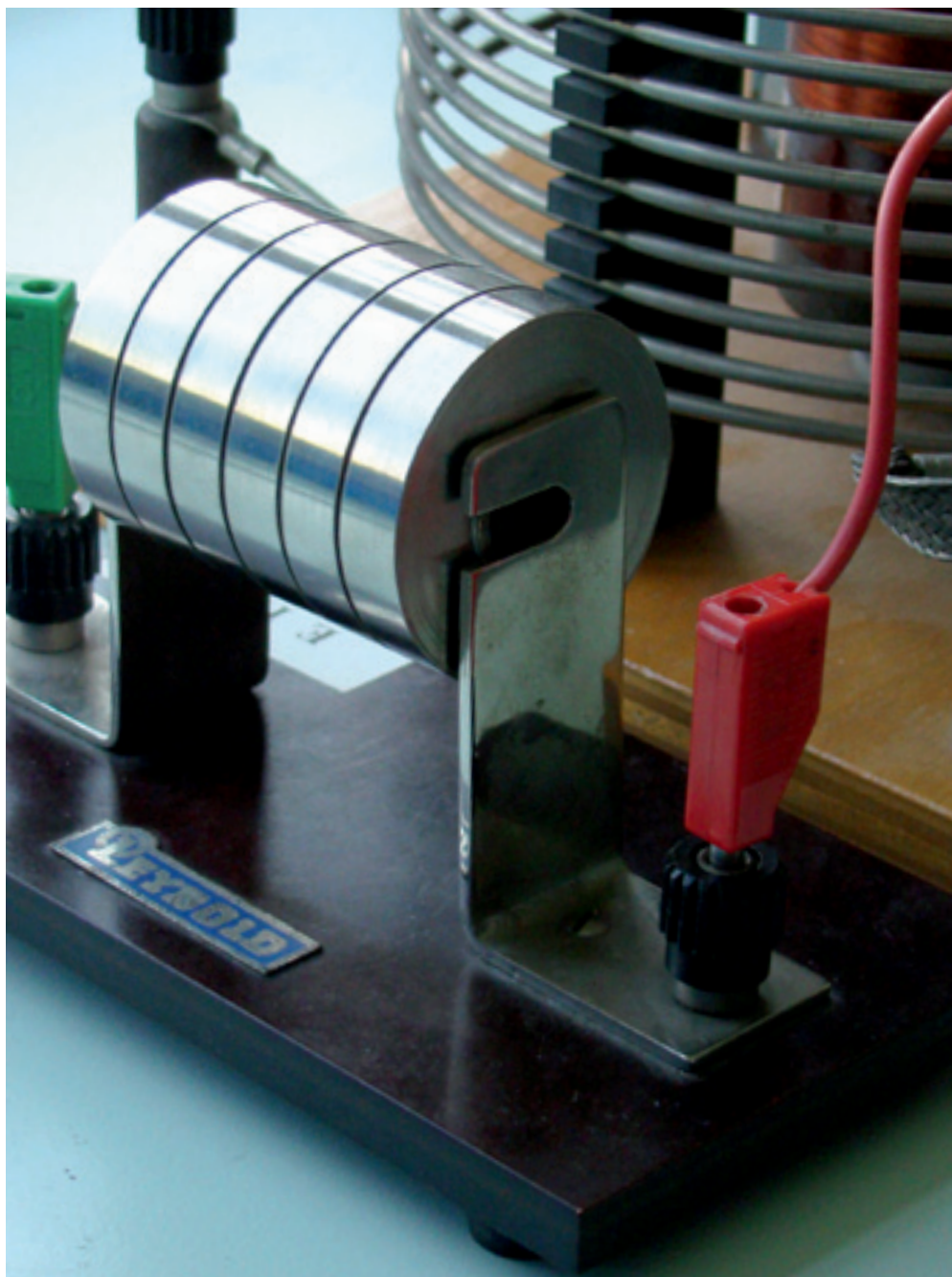
so genannten Knallfunktensender durch Anblasen der Funkenstrecke verkürzt wurde, schlangen sie länger nach bis zum nächsten Funken. Durch Serienschaltung von vielen Funkenstrecken mit kleinen Elektrodenabständen verlöschten die Funken auch ohne Anblasen. So entstand der Löschfunktensender nach Prof. Max Wien mit einer schon fast kontinuierlichen Abstrahlung, die aber immer noch wie mit einer Sägezahnspannung moduliert war. Durch sorgfältige Abstimmung zwischen dem Antennenschwingkreis und dem Senderschwingkreis ergab sich eine Verringerung der belegten Bandbreite und damit ein Wirkungsgrad von 50 bis 70 %. 1909 wurden mit einem Löschfunktensender von 25 kW Leistung eine Reichweite von 4600 km erreicht. Aber alle diese Sender strahlten gedämpfte Wellen ab, die für eine Ton- oder gar Musikübertragung nicht geeignet waren.

Erfindung des Lichtbogensenders

Daher versuchte man nun, ungedämpfte Wellen zu erzeugen. Seit 1900 war bekannt, dass ein von



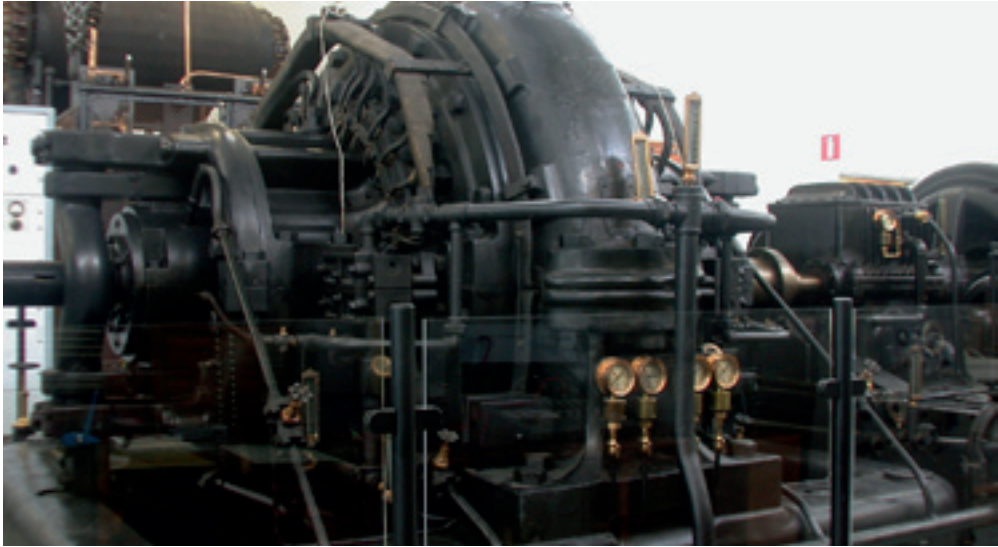
Löschfunktensender von Telefunken



Ansicht einer Löschfunkenstrecke mit Teslatransformator



Ansicht eines Lichtbogensenders nach Poulsen



Maschinensender nach Alexanderson, links Generator, rechts davon der Vervielfacher

Gleichstrom gespeister Lichtbogen ebenfalls Hochfrequenz erzeugte («singing arc», singender Lichtbogen). Der negative Widerstand des Lichtbogens führt zu Schwingungen, die von der umgebenden Schaltung abhängig sind.

Der dänische Physiker Valdemar Poulsen brachte in einen abgestimmten Schwingkreis einen Lichtbogen ein und hatte damit einen leistungsfähigen Hochfrequenzgenerator entwickelt, der an einen Antennenkreis angekoppelt wurde. Damit hatte er 1903 den Lichtbogensender erfunden, der schmalbandiger und ärmer an Neben- und Oberwellen ist. Das kam der Funkreichweite und dem Simultanbetrieb mehrerer Sender im gleichen Frequenzband zugute. Der nun gleichspannungsfreie Antennenkreis konnte über eine Taste für Telegraphie unterbrochen oder über Mikrofone mit Sprache moduliert werden.

1904: Die erste Sprechverbindung

Poulsen gelang zum ersten Mal 1904 eine Sprechverbindung über Funk. 1906 wurde die ausgereif-

te Technik veröffentlicht, die die Grundlage für die heutige Radio- und Funktechnik bildete.

Die typische Sendeleistung für deutsche Heeresgeräte lag bei 1,5 kW in mobilen und 4 kW in ortsfesten Anlagen, bei der kaiserlichen Marine 6 kW auf großen Schiffen. Im zivilen Bereich wurden ab 1910 Funkstationen mit 100 kW für kontinentale Funkverbindungen vor allem in den USA eingesetzt. Der wohl stärkste Lichtbogensender wurde 1922/23 in Malabar/Java (heutiges Indonesien) errichtet. Mit einer primären Leistungsaufnahme von 2400 kW stand der Sender über eine Entfernung von 11.500 km in Verbindung mit der Großstation in Kootwijk/Niederlande.

»Maschinensender« für Überseefunk

Parallel dazu verlief die Entwicklung der Maschinensender, in denen die Hochfrequenzleistung direkt durch schnell rotierende Wechselstromgeneratoren erzeugt wurde. Die obere Grenzfrequenz wird dabei durch die Mechanik bestimmt. Bei 81 kHz und 1 kW Leistung wurde eine Entfer-



Verschiedene Empfangs- und Leistungsröhren



Röhrentyp RE 144 von Telefunken (20er Jahre)

nung von 310 km erreicht. Schalttechnische Maßnahmen zur Frequenzvervielfachung führten bis 1916 zu Frequenzen bis 150 kHz bei Leistungen bis 250 kW und später bis 1000 kW. Diese Sender wurden für Überseefunkverbindungen und in den aufkommenden Pressediensten eingesetzt.

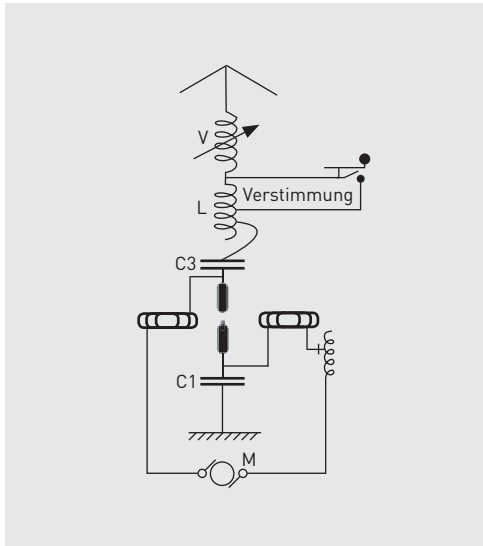
Ungedämpfte Sender strahlen eine sehr saubere Hochfrequenz praktisch ohne Eigengeräusch ab. Sie waren in den damaligen Empfängern nur durch das Fehlen von Geräuschen erkennbar. Tastfunkzeichen waren als leises Knacken hörbar. Daher musste das lautlose Empfangssignal künstlich mittels Summer oder Ticker hörbar gemacht werden. Wenn also »die Nachricht über den Ticker kam«, so standen entweder Pulsenlichtbogensender oder Maschinensender eines Pressefunkdienstes dahinter.

Entwicklungsschub durch elektronische Verstärkerröhren

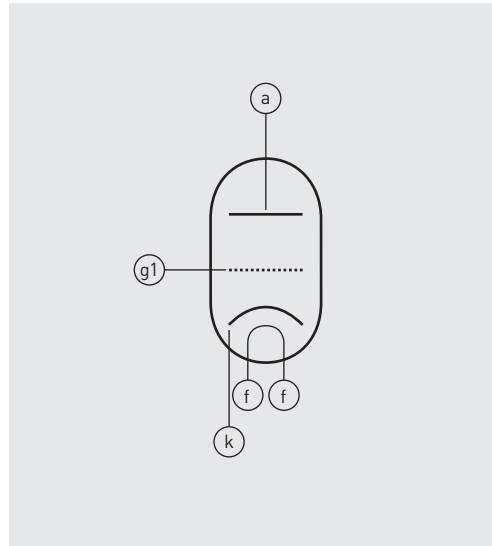
Die nächste deutliche Leistungssteigerung auf der Sender- und Empfängerseite wurde durch die

elektronischen Verstärkerröhren erreicht. 1904 arbeitete Professor Arthur Wehnelt in Erlangen an einer gasgefüllten »Ventilröhre«, in der eine Glühkathode Elektronen emittierte, die von einer Anode aufgefangen wurden und die sich zur Gleichrichtung von Wechselströmen eignete. In den USA meldete Lee de Forest 1907 seine Audion-Röhre zum Patent an, eine gittergesteuerte Dreipolröhre mit Glühkathode in einem evakuierten Glaskolben. Das Patent wurde aber in Europa bis 1912 nicht bekannt. Zudem konnte sein Audion noch keine Verstärkung leisten.

In Deutschland entwickelte Robert von Lieben eine gasgefüllte Dreipolröhre als Verstärker. Erst nach Entwicklung hochleistungsfähiger Molekularluftpumpen durch W. Gaede war es 1911 möglich, Hochvakuum-Dreipolröhren mit brauchbaren Verstärkungsfaktoren zu bauen. 1913 wurden in drei Ländern unabhängig und fast zeitgleich die entscheidenden Patente für das rückgekoppelte Audion und den Röhrensender erteilt.



Prinzipschaltbild eines Poulsen-Lichtbogensenders



Prinzipschaltbild einer Triode

Die Audionröhre verbesserte die Empfindlichkeit der Funkempfänger um Größenordnungen. Damit konnten die Sendeleistungen in gleichem Maße zurückgenommen werden, sofern die Entfernung konstant blieb. Die Senderöhren hatten anfänglich nur geringe Leistungen von einigen Watt. Bis 1918 wurden Senderöhren mit 1,5 kW gefertigt, eine wassergekühlte Senderöhre von 5 kW war in Erprobung, und ein Telefunken-Sender erreichte bereits eine HF-Leistung von 10 kW. Telefunken stellte zu der Zeit schon rund 1000 Empfängeröhren und 100 Senderöhren pro Tag her.

Nach dem Ersten Weltkrieg ging das Zeitalter der »Dinosauriersender« zu Ende, die Zeit der Röhrenfunkgeräte hatte begonnen. Technisch elegante Elektronik löste die Leistungseskalation ab. Der Einzug in immer höhere Frequenzen konnte beginnen. Der öffentliche Rundfunk startete 1923.

// Eigenschaften der Funkwellen

03

Grundlegende Eigenschaften

Ausbreitungseigenschaften

Rauschen

// Grundlegende Eigenschaften

Die Erforschung der Funkwellen und ihre Nutzung zielte von Anfang an in die Richtung größtmöglicher Reichweite. In diesem Merkmal ist der Funk den Schallwellen weit überlegen. Während ein Megaphon von 25 Watt bestenfalls eine Reichweite von 250 m erzielt, reichen Dezimeterwellen von 25 Milliwatt bis zu 2500 m weit. Somit ist ihre Reichweite um den Faktor 1:10.000 höher.

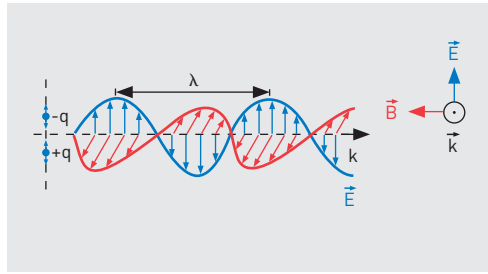
Ein weiteres Merkmal von universeller Bedeutung ist die Ausbreitung der Funkwellen in alle Richtungen und damit ihre große Flächenabdeckung. Davon lebt u. a. der öffentliche Rundfunk. Die Funkabdeckung wird besonders deutlich an der Versorgung von z. B. ganz Europa durch einen einzigen Fernsehsatelliten.

Mit Funk können Verbindungen auch in der Bewegung betrieben werden, also zu Verkehrsmitteln und zu sich damit fortbewegenden Personen. Und: Funk reicht an Orte, die anders nicht zu erreichen sind. Das geht von Messpunkten an unzugänglichen Stellen in technischen Prozessen bei kurzen Entfernungen bis hin zu den entferntesten Objekten im Weltall für die Forschung.

Eine weitere wichtige Eigenschaft von Funk ist seine Unabhängigkeit von Kabeln, die störende Hindernisse darstellen können. Funk kann einen Sicherheitsbeitrag zum Arbeitsschutz leisten und z. B. auch in der Medizin den Arzt bei Operationen wirksam unterstützen.

Frequenz und Wellenlänge

Eine elektromagnetische Welle besteht aus gekoppelten elektrischen und magnetischen Feldern, die sich im Idealfall homogen in alle Richtungen im Raum ausbreiten. Das elektrische Feld E und das magnetische Feld B stehen senkrecht aufeinander und bewegen sich in Richtung des Wellenvektors k . Im Vakuum breitet sich die Welle mit Lichtgeschwindigkeit c_0 aus. Für technische



λ - Wellenlänge

c_0 - Ausbreitungsgeschwindigkeit im Vakuum

$c_0 = 299792,5 \text{ km/s}$; f - Frequenz in Hz (1/s)

$$\lambda = \frac{c_0}{f}$$

Ausbreitung einer elektromagnetischen Welle

Anwendungen ist die Frequenz f oder die Wellenlänge λ von Bedeutung. Im Vakuum ergibt sich der Zusammenhang zwischen Wellenlänge und Frequenz zu:

$$\lambda = c_0 / f$$

// Ausbreitungseigenschaft elektrischer Wellen

Die Ausbreitung elektrischer Wellen wird von unterschiedlichsten Faktoren beeinflusst. Wesentlich ist hierbei die Freifelddämpfung und die sie überlagernden Störungen und Interferenzen.

Geht man bei einem Sender von einem idealen Kugelstrahler aus, wird die abgestrahlte Leistung P_s mit zunehmendem Abstand auf eine immer größer werdende Kugeloberfläche verteilt. Die Strahlungsdichte S_r nimmt damit quadratisch ab.

Strahlungsdichte

Möchte ein Empfänger das Signal aufnehmen, so wird eine Antenne zum »Einfangen« der abgestrahlten Leistung eingesetzt. Logischerweise

$$S_r = \frac{P_s}{4\pi r^2}$$

$$P_E = S_r \cdot A_W$$

Oben: Strahlungsdichte in der Entfernung r
 Unten: Empfangsenergie in der Entfernung r

$$L_{FS} = \frac{P_s}{P_E} = \left(\frac{4\pi r}{\lambda} \right)^2 \cdot \frac{1}{G}$$

Berechnung der Freifelddämpfung L_{FS}

kann nur ein Bruchteil der abgestrahlten Leistung eingefangen werden. Man spricht hier von der fiktiven Antennenwirkfläche A_W .

Die Freifelddämpfung L_{FS} berechnet sich dann aus dem Verhältnis der abgestrahlten zur empfangenen Sendeleistung (siehe Bild rechts oben).

$1/G$ beschreibt hierbei das Produkt der Antennengewinne, auf die an dieser Stelle nicht weiter eingegangen wird.

Entscheidend bei dieser Herleitung sind im Wesentlichen drei Sachverhalte:

1. Die Freifelddämpfung und damit auch die Empfangsleistung hängen quadratisch von der Entfernung ab.
2. Die Freifelddämpfung hängt quadratisch von der Frequenz ab.
3. Die Freifelddämpfung hängt von der effektiven Antennenwirkfläche ab.

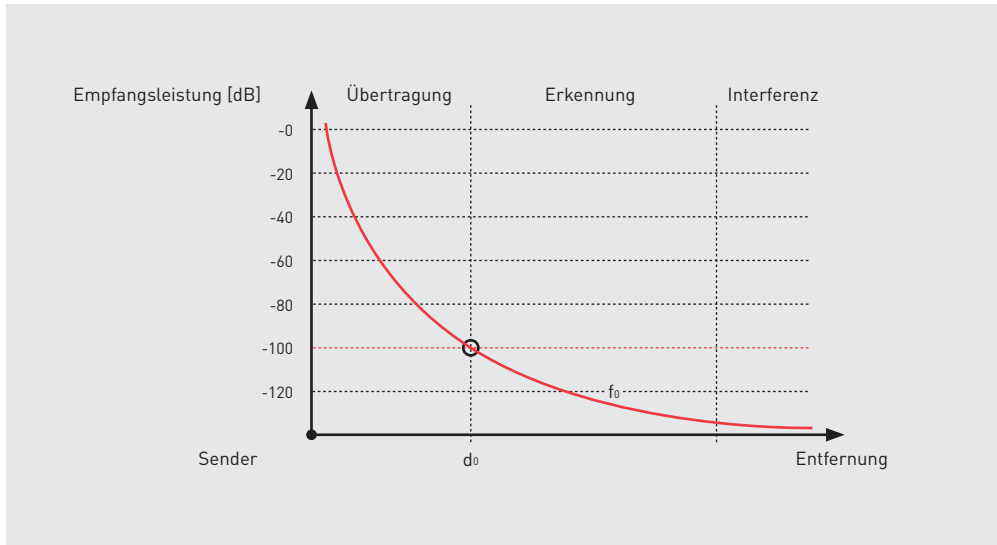
In der Abbildung auf der folgenden Seite ist exemplarisch die Empfangsleistung eines Empfängers bei einem gegebenen Sender so aufgezeigt.

Die Grenzempfindlichkeit des Empfängers beträgt nach Datenblatt typischer Weise ca. 100 dBm.

Ist die Empfangsleistung besser als die Empfindlichkeit, spricht man davon, dass sich der Empfänger im Übertragungsbereich befindet. Nimmt die empfangene Leistung weiter ab, kann nur noch sporadisch ein Datenaustausch erfolgen – das System befindet sich im Erkennungsbereich. Ab einer bestimmten Entfernung ist kein Signal mehr für eine Kommunikation verwendbar. Hier trägt das Sendesignal nur noch zur Interferenz und einem allgemeinen Störteppich bei.

Reichweite von Funksignalen

In der Praxis hängt die Funkreichweite von vielen Faktoren ab, so dass die Hersteller sich zumeist nicht auf eine exakt verlässliche, auf alle denkbaren Einsatzfälle zutreffende Angabe festlegen können. Wenn man aber alle Faktoren kennt, ist die Reichweite genau zu berechnen. Leider sind meist nicht alle Faktoren bekannt, so dass man



Die Empfangsleistung hängt quadratisch von der Entfernung ab.

Abschätzungen oder Grenzwerte einführen muss. Wie man trotzdem zu verlässlichen Aussagen kommen kann, soll an einer Bilderserie erläutert werden. Hierzu wird in einem Diagramm auf der Abszissenachse die Reichweite im logarithmischen Maß in Kilometern aufgetragen und auf der Ordinatenachse der jeweilig zu betrachtende Leistungspegel ebenfalls im logarithmischen Maßstab in dB dargestellt.

- Die Empfangsbandbreite wird mit 1 MHz festgelegt, die Empfängertemperatur mit 290 °K (17 °C).
- Natürliches Rauschen aus der Umwelt bleibt unberücksichtigt, weil es unter dem Rauschpegel des Empfängers liegt.
- Die Rauschmaß Z des Empfängers wird mit 4 dB günstig angenommen.
- Als Mindeststörabstand wird 10 dB gewählt für eine Bitfehlerrate (BER) von unter 10^{-5} .

Die logarithmischen Maßstäbe bieten den Vorteil, dass die quadratische Abnahme des Sendepegels als gerade Linie dargestellt werden kann.

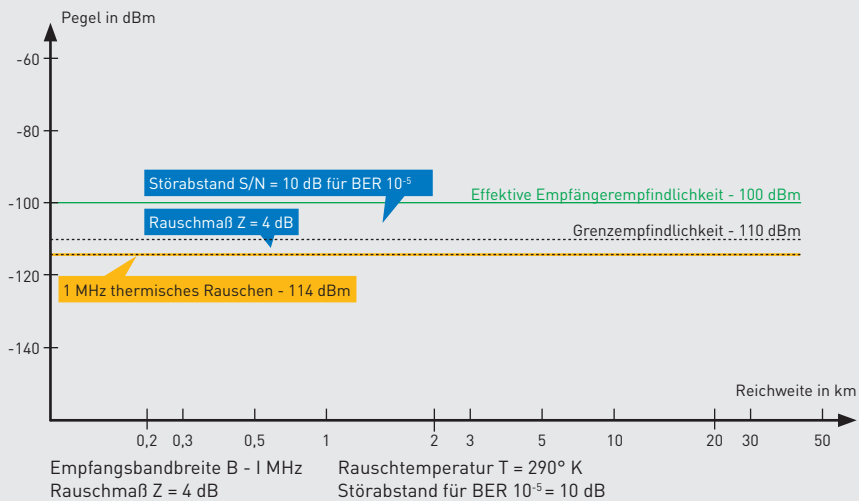
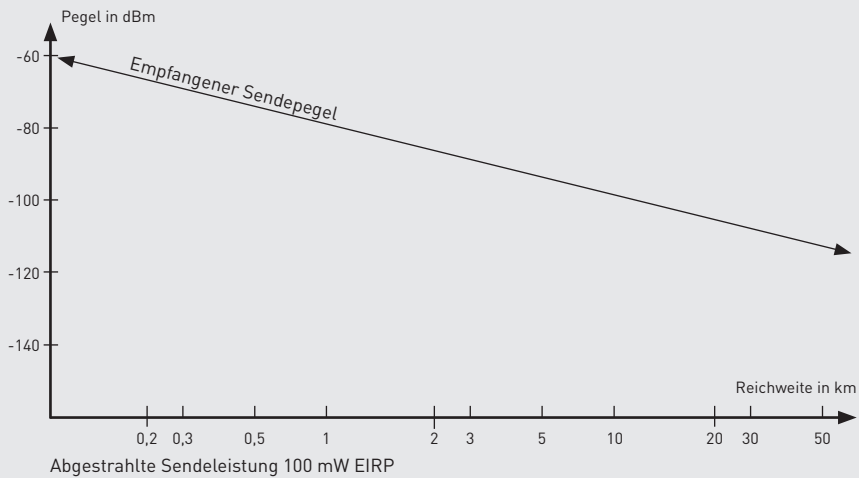
Randbedingungen sind:

- In allen Diagrammen sind keine Antennengewinne berücksichtigt, sondern kugelförmige Abstrahlung. Es wird einheitlich eine Sendeleistung von 100 mW EIRP (Effective Isotropic Radiated Power) zu Grunde gelegt.
- Besondere Ausbreitungsbedingungen wie Überreichweiten sind aus Gründen der Übersichtlichkeit weggelassen worden.

// Rauschen

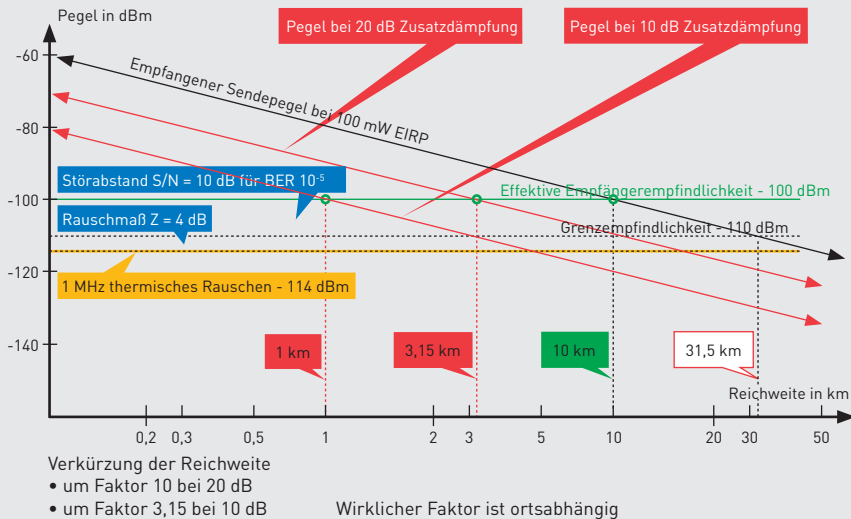
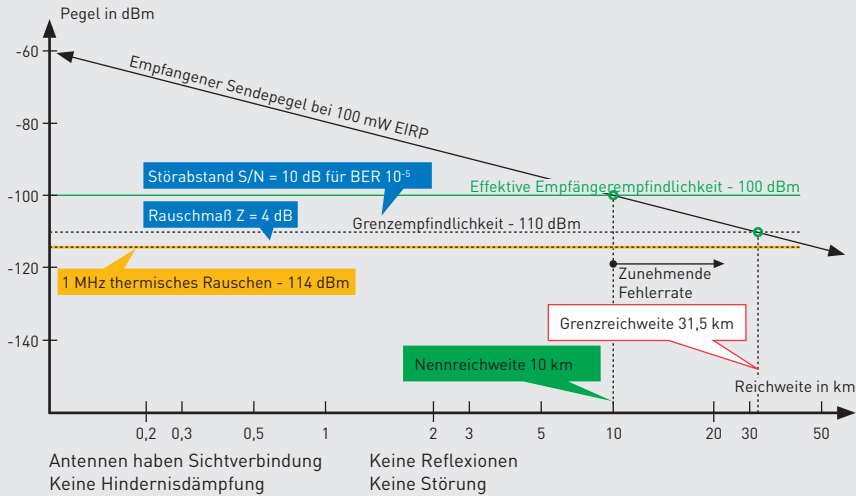
Mit dem Einsatz von empfindlichen Superheterodyn-Empfängern ab 1918 war man unversehens an eine Grenze gestoßen, von der an es keine Steigerung der Empfindlichkeit mehr gab. Es war das Empfängerrauschen. Forscher untersuchten die Zusammenhänge und fanden heraus, dass es sich dabei hauptsächlich um thermisches Rauschen handelt.

Atome und Moleküle führen in jedem Aggregatzustand Schwingungen aus, die man als Brown-



Oben: Diagramm 1 zeigt, wie der empfangene Sendepiegel mit der Entfernung abnimmt.

Unten: Diagramm 2 zeigt die Rauschpegel des Empfängers, die unabhängig von der Entfernung sind.



Oben: Diagramm 3 zeigt die theoretisch erreichbare Reichweite als Schnittpunkt von Sendepiegel und Empfängerempfindlichkeit.

Unten: Diagramm 4 berücksichtigt die Zusatzdämpfungen des Sendepiegels mit 10 dB bzw. 20 dB. Hierbei tritt eine Verkürzung der Reichweite um den Faktor 3,15 bei 10 dB bzw. um den Faktor 10 bei 20 dB ein.



Oben: Diagramm 5 berücksichtigt nun zusätzliche Störpegel, die die Schwelle der Empfindlichkeit des Empfängers übersteigen und daher wirksam werden. Die Folge ist eine weitere Verkürzung der Reichweite.

Unten: Diagramm 6 ist ein konkret durchgerechnetes Beispiel für eine SRD- Anwendung (Short Range Device; Modellbau-Fernsteuerung) im ISM-Frequenzbereich von 2,4 GHz.

Thermische Rauschleistung
am Empfängereingang

$$N = k \cdot T \cdot B$$

Rauschen nach der 1. Stufe

$$N = z \cdot k \cdot T \cdot B$$

Rauschwerte am Empfänger

sche Molekularbewegung bezeichnet. Ihre Schwingungsamplitude verändert sich mit der vierten Potenz der absoluten Temperatur. Die mit den Atomen oder Molekülen mitschwingenden Elektronen stellen einen hochfrequenten Wechselstrom dar, der an dem Eingangswiderstand bzw. der Impedanz der Eingangsstufe des Empfängers zu einer Wechselspannung führt und als Rauschen wahrgenommen wird. Die Rauschleistung hängt vom Frequenzintervall B der Empfängereingangsschaltung ab.

Die so genannte spektrale Rauschleistungsdichte N_0 , also die Rauschleistung pro Frequenzintervall, ist über einen weiten Frequenzbereich unabhängig von der Frequenz; man spricht in diesem Zusammenhang von weißem Rauschen oder Johnson-Nyquist-Rauschen. Das führt zu der Formel für die thermische Rauschleistung: Dabei ist die Boltzmann-Konstante

$$k = 1,38 \cdot 10^{-23} \text{ Js} / ^\circ\text{K}$$

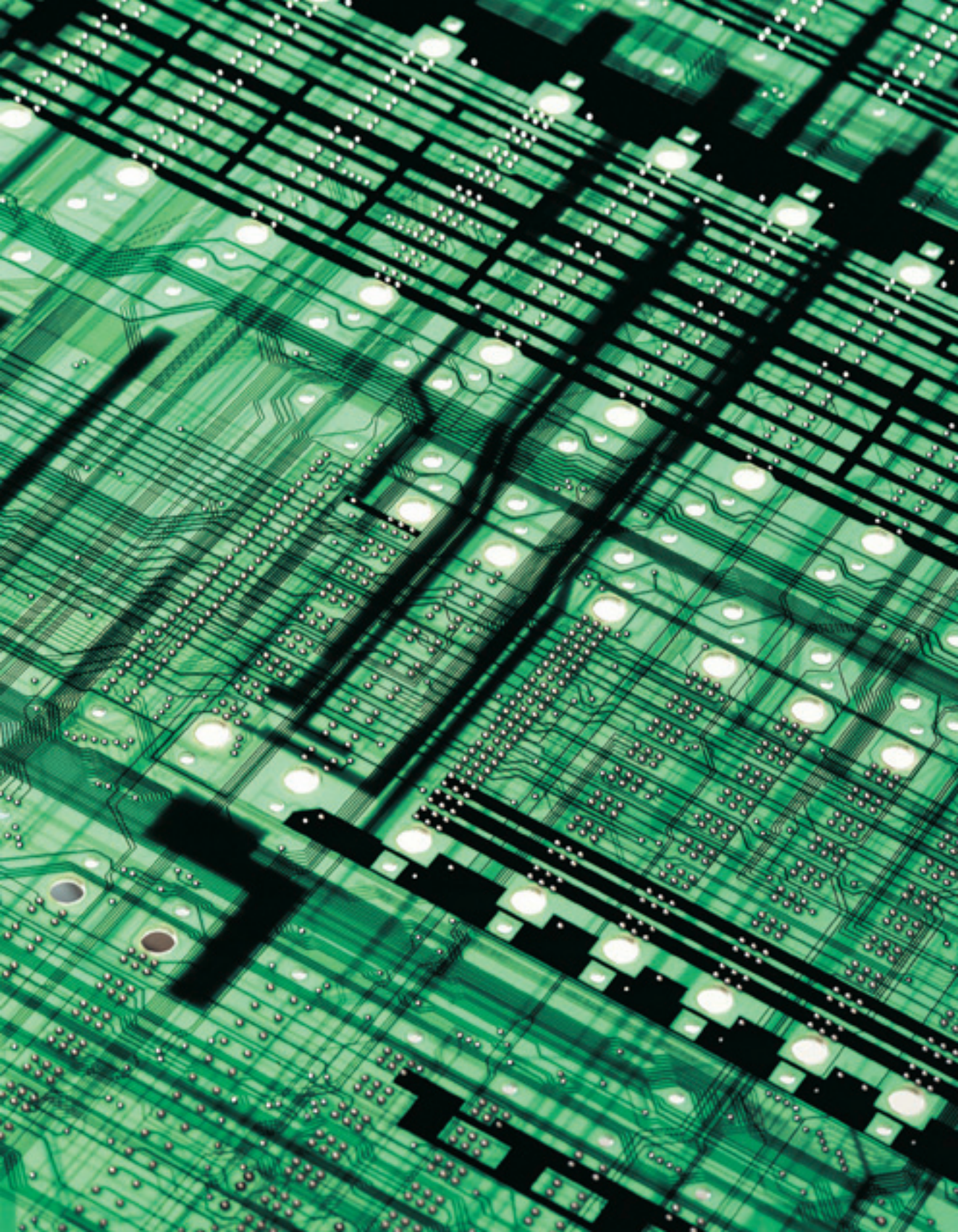
Der zweite Effekt, das so genannte Schrotrauschen, entsteht in der ersten Verstärkerstufe durch die Elektronen des Verstärkerstromes. Diese müssen einzeln über eine Potentialschwelle gehoben werden und fallen dann in eine Potentialsenke, wobei ein winziger Impuls erzeugt wird. Die Summe dieser Impulse hört sich so an als würde man Schrotkugeln auf eine harte Unterlage fallen lassen – daher der Name. Dieser Rauschanteil heißt Empfängerrauschzahl z , die typischerweise im Bereich zwischen 4 und 40 liegt. Daraus resultiert ein so genanntes Rauschmaß z zwischen 6 dB und 16 dB. Das Rauschmaß z ist also ein Maß für die Güte eines Eingangsverstärkers. Rauscharme Verstärker liegen unter 10 dB. Aus beiden Rauschanteilen ergibt sich schließlich die Formel für das Empfängerrauschen wie nebenstehend dargestellt.

Man kann das Rauschen nur begrenzt vermindern:

- Die einfachste Möglichkeit ist die Begrenzung der Bandbreite B im Eingang des Empfängers auf das Mindestmaß.
- Die zweite Möglichkeit liegt in der Kühlung der Eingangsstufe auf eine wesentlich niedrigere Temperatur T .
- Die dritte Möglichkeit sind parametrische Verstärker, bei denen die Energie für die erste Verstärkerstufe nicht als Strom, sondern durch die rauschfreien Quanten einer um den Faktor 10 höheren »Pumpfrequenz« bereit steht ($E = h \cdot \nu$).

Solch aufwändige Verstärker werden nur im Ausnahmefall gebraucht, z. B. in der Weltraumforschung. Ansonsten nutzt man für den jeweiligen Frequenzbereich ausgesuchte rauscharme Vorverstärker mit Halbleitern wie Gallium-Arsenid-Feldeffekt-Transistoren.

Weitere Rauschanteile wie das Funkelrauschen der Elektronenröhren und das $1/f$ -Rauschen (rosa Rauschen) sind in diesem Zusammenhang nicht von Bedeutung.



// Grundlagen der Funktechnik: Frequenzen

04

Historische Entwicklung

Koexistenz von Funkdiensten

// Historische Entwicklung der Frequenznutzung

Mit der Erfindung des Funks wuchs international lawinenartig der Bedarf an Frequenzen für die neuen Dienste. Die anfängliche Begrenzung auf Langwelle und Mittelwelle – die Kurzwelle wurde noch für den Weitverkehr als ungeeignet erachtet – führte rasch zu gegenseitigen Störungen.

Der Berliner Funkentelegraphievertrag von 1906 schuf die erste Ordnung. Mit der Entdeckung der großen Reichweiten von Kurzwellen durch die Funkamateure wurde der Bedarf auch darauf ausgedehnt. Die Funkdienste nahmen schneller zu als die Frequenzen. Der Genfer Wellenplan von 1923 war der erste Versuch einer Regelung.

Zunehmendes »Frequenzgerangel«

Die Schere zwischen Bedarf und Verfügbarkeit ging immer weiter auf. Die Frequenzzuteilungen reichten den meisten Staaten nicht, sie hielten sich nicht mehr an die Wellenpläne. Das allgemeine Frequenzgerangel führte zu einem veritablen Chaos. Kaum eine Rundfunkfrequenz war durch Sender anderer Staaten nicht gestört, besonders abends. Die Einführung von Frequenzrastern, Leistungsbegrenzungen und die weite räumliche Trennung von Sendern gleicher Frequenz brachten in den folgenden Wellenplänen nur vorübergehende partielle Erleichterungen.

Eine deutliche Verbesserung brachte die gesteigerte Empfindlichkeit und Trennschärfe der Empfänger mittels Heterodyn- und Superheterodyn-Technik, wodurch die Sendeleistungen entsprechend verringert werden konnten. Die Erschließung höherer Frequenzen für Rundfunk und Fernsehen im VHF-Bereich (UKW) führte zur Verlagerung von RF/FS und entspannte die alten Wellenbereiche beträchtlich.

Frequenznutzung heute – Die Aufgaben der ITU

Die Nutzung der Frequenzen ist eine hoheitliche Aufgabe und unterliegt der staatlichen Kontrolle.

Das heißt: Nicht jeder darf in einem beliebigen Frequenzspektrum Signale emittieren. Die Nutzung von sämtlichen Frequenzbändern unterliegt damit der Genehmigung nationaler und internationaler Behörden, und eine Nichtbeachtung der jeweils gültigen Gesetze ist als Straftat anzusehen.

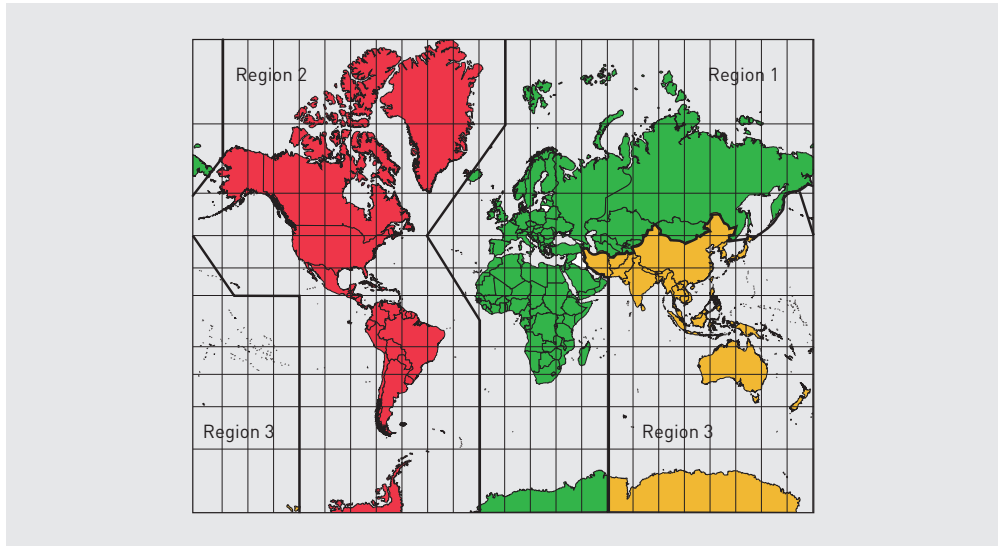
Um der hohen Dynamik der weltweit eingesetzten Funktechnologie Rechnung zu tragen und eine weitgehende Harmonisierung anzustreben, kümmert sich die ITU (Internationale Fernmelde Union) um die internationale Frequenzkoordination. Ziel ist die effiziente Nutzung der Ressourcen und die Vermeidung von Störungen und Interferenzen zwischen den Funkdiensten der verschiedenen Länder. Die Vollzugsordnung für den Funkdienst (Radio Regulations) ist die wichtigste Grundlage der Frequenzverwaltung durch die ITU. Im Rahmen dieser Ordnung werden weltweit drei Frequenzregionen unterschieden:

1. Europa und Afrika
2. Nord-, Mittel- und Südamerika
3. Asien und Australien

Die Funkbereichszuweisung erfolgt nach einem internationalen Frequenzzuweisungsplan, der sowohl die Funkkategorien als auch die Frequenzbereiche zuweist. Darüber hinaus gibt es einzelne internationale Abkommen, bei denen die ITU sich um eine weltweite Harmonisierung einzelner ausgezeichnete Frequenzbereiche für spezielle Dienste bemüht.

Europäische Harmonisierung

Auf europäischer Ebene setzt die CEPT (Conférence Européenne des Administrations des Postes et Télécommunications) die entsprechenden Anforderungen um. Ziel ist auch hier, zumindest auf europäischer Ebene eine vollständige Harmonisierung zu erreichen. Seit 2002 liegt ein europäischer Frequenzzuweisungs- und Frequenznutzungsplan vor, der mit europäischem Recht und den jeweiligen Ausführungsbestimmungen der Länder verbindlich umgesetzt werden soll.



Funkregionen der ITU

Die Länder der europäischen Gemeinschaft sind dazu angehalten, die Richtlinien und Entscheidungen des Europäischen Parlaments und Rates über den Rechtsrahmen für die Frequenzpolitik, die R&TTE Richtlinie sowie die dienstspezifischen Richtlinien und Entscheidungen, wie z. B. die GSM-Richtlinie oder die UMTS-Entscheidung, zu befolgen.

Darüber hinaus wurde mit der EU-Richtlinie über »Funkanlagen und Telekommunikationsendeinrichtungen« (1999/5/EG) eine verbindliche Richtlinie für das Inverkehrbringen von entsprechenden Geräten in Europa getroffen, die mittlerweile in europäisches und nationales Recht überführt wurde. Die Richtlinie ermöglicht einen beschleunigten Marktzugang, indem die Geräte nicht aufwändige nationale Prüfverfahren und eine behördliche Zulassung durchlaufen müssen. Statt dessen werden harmonisierte Konformitätsbewertungsverfahren angewendet, so dass ein Großteil der Produkte mit »Herstellereklärungen« in Verkehr gebracht werden dürfen.

Nationale Frequenzzuweisung

Da Funk eine hoheitliche Aufgabe ist, bemühen sich die einzelnen Staaten nach ihren Möglichkeiten, die Richtlinien umzusetzen. In Deutschland gehen die Richtlinien in den Frequenzbereichszuweisungsplan (FreqBZP) über, der den Funkdiensten und weiteren Anwendungen die entsprechenden Funkbereiche zuweist. Die Festlegung erfolgt durch Rechtsverordnung unter der Aufsicht der Bundesnetzagentur, die nach §46 TKG (Telekommunikationsgesetz) den Frequenznutzungsplan (FreqNP) für die einzelnen Frequenzbereiche spezifiziert. Auf 660 Seiten kann dann die jeweilige Verwendung des Frequenzbereichs von 9 kHz bis hin zu 275 GHz eingesehen werden (Frequenznutzungsteilpläne 1 bis 486). Hier tiefer in die Materie einzusteigen, würde den Rahmen des Buches bei Weitem sprengen.

Zu erwähnen ist noch, dass der FreqNP für medizinische, wissenschaftliche und industrielle Anwendungen (Medical, Scientific, Industrial, MSI) besondere Frequenzen für Geräte vorsieht, die

Frequenzbereich in MHz	maximale Kanalband- breite/ Kanalraster in kHz	Maximale äquivalente Strahlungsleistung [ERP]/Maximale Magnetische Feldstärke	Relative Frequenzbelegungs- dauer/ Listen before Talk (LBT)
a) 6,765–6,795	Keine Einschränkung	42 dB μ A/m in 10m Entfernung	Keine Einschränkung
b) 13,553–13,567	Keine Einschränkung	42 dB μ A/m in 10m Entfernung	Keine Einschränkung
c) 26,957–27,283	Keine Einschränkung	42 dB μ A/m in 10m Entfernung	Keine Einschränkung
d) 40,660–40,700	Keine Einschränkung	10 mW	Keine Einschränkung
e) 433,050–434,790	Keine Einschränkung	10 mW	Keine Einschränkung
f) 868,000–868,600	Keine Einschränkung/ Schmal- und Weitband- modulation	25 mW	$\leq 1,0$ % oder LBT
g) 868,700–869,200	Keine Einschränkung/ Schmal- und Weitband- modulation	25 mW	$\leq 1,0$ % oder LBT
h) 869,300–869,400	25	10 mW	Keine Einschränkung
i) 869,400–869,650	25/Schmal- und Weitbandmodulation	500 mW	≤ 10 % oder LBT
j) 869,700–870,000	Keine Einschränkung/ Schmal- und Weitband- modulation	5 mW	Keine Einschränkung
k) 2,400–2,483,5	Keine Einschränkung	10 mW	Keine Einschränkung
l) 5,725–5,875	Keine Einschränkung	25 mW	Keine Einschränkung
m) 24,000–24,250	Keine Einschränkung	100 mW	Keine Einschränkung
n) 61,000–61,500	Keine Einschränkung	100 mW	Keine Einschränkung
o) 122,000–123,000	Keine Einschränkung	100 mW	Keine Einschränkung
p) 244,000–246,000	Keine Einschränkung	100 mW	Keine Einschränkung

Frequenznutzungsparameter für Short Range Devices (SRD)

Von	Bis	Typ	Anmerkungen
6,765 MHz	6,795 MHz	A	SRD
13,553 MHz	13,567 MHz	B	SRD
26,957 MHz	27,283 MHz	B	SRD
40,66 MHz	40,70 MHz	B	SRD
433,05 MHz	434,79 MHz	A	SRD, nur Region 1 (Europa, Afrika, Nachfolgestaaten der UdSSR und Mongolei)
902 MHz	928 MHz	B	nur Region 2 (Nord- und Südamerika)
2,400 GHz	2,500 GHz	B	Region 1, 2 und 3
5,725 GHz	5,875 GHz	B	/
24 GHz	24,25 GHz	B	/
61 GHz	61,5 GHz	A	/
122 GHz	123 GHz	A	/
244 GHz	246 GHz	A	/

Verschiedene Frequenzbereiche und ihre Verbreitung

wegen ihrer geringen effektiven Sendeleistung vereinfachten Bestimmungen unterliegen.

ISM-Band

Eine besondere Bedeutung haben die so genannten ISM-Bänder, die für industrielle, wissenschaftliche und medizinische sowie häusliche Anwendungen lizenzfrei genutzt werden dürfen und eine geringe effektive Sendeleistung haben. Mit der Allgemeinzulassung müssen lediglich Auflagen bezüglich der Sendeleistung und der Störung benachbarter Frequenzbereiche eingehalten werden. Die entsprechenden Geräte nennt man auch Short Range Devices (SRD).

Es werden zwei verschiedene ISM-Bandtypen unterschieden:

Typ A:

Anwendungen bedürfen einer Genehmigung der jeweiligen nationalen Behörden. Die Genehmigung kann auch pauschal erteilt werden.

Typ B:

Anwendungen benötigen keine Genehmigung und müssen lediglich mit Störungen jeder Art zu recht kommen.

ISM-Bänder in unterschiedlichen Frequenzen sind durch die internationale Fernmeldeunion (ITU) festgelegt. Leider ist die Harmonisierung nicht so weit fortgeschritten, dass alle ISM-Frequenzen überall verfügbar sind. Darüber hinaus dürfen Länder eigene Frequenzbereiche freigeben.

Zusammenfassend führt das zu zwei Effekten.

1. Das 2,4 GHz-Band ist als einziges Band welt-

weit verfügbar, so dass es die Voraussetzung für weltweit einheitliche Funk-Produkte bietet. Das macht auf der einen Seite einen großen Charme aus, auf der anderen Seite kämpfen die verschiedensten Technologien um das schmale Frequenzband. WLAN nach IEEE 802.11b und g, Bluetooth und ZigBee (IEEE 802.15.4) gehören zu den prominentesten Vertretern der 2,4 GHz-Kategorie.

2. Aufgrund der günstigen Ausbreitungseigenschaften ist der Sub-GHz-Bereich besonders attraktiv. Hierzu gehören das ISM-Band um 433 MHz und 900 MHz. Beide Bänder sind jedoch nicht einheitlich verfügbar. In Europa ist darüber hinaus noch der Bereich von 863 ... 870 MHz als SRD-Band für spezielle Anwendungen verfügbar. Dieses führt häufig zu Produkten, die wahlweise im 433 MHz-Band (Region 1), 868 MHz (Europa) und 915 MHz-Band (Region 2) eingesetzt werden.

// Koexistenz von Funkdiensten

Es gibt nur wenige Dienste, die für sich exklusiv Frequenzbänder beanspruchen können. Die meisten Dienste müssen sich mit anderen die Frequenzbänder teilen. Hierbei kann es zu gegenseitigen Störungen kommen. Besonders problematisch ist das bei den ISM-Frequenzen.

Zur Vermeidung von Störungen gibt es Regelungen im FreqNP und in den technischen Vorschriften der Euro-Normen EN, ENELEC und ETSI. Diese Vorschriften zielen darauf ab, durch »Verkehrsregeln« allen im Frequenzband angesiedelten konkurrierenden Diensten eine möglichst hohe Nutzung zu gestatten. Anders ausgedrückt: Das jeweilige Frequenzband soll optimal belastet und ausgenutzt werden

Regelungen des FreqNP

Die bekannteste Maßnahme des FreqNP ist die Deckelung der Sendeleistung, sei es auf einen konstanten Wert oder zeitabhängig auf unter-

schiedliche Leistungen. So dürfen z. B. bestimmte MW-Sender tagsüber mit höherer Leistung senden als nachts, wenn die Reichweite durch die Ausbreitungsverhältnisse zunimmt. Die zweitwichtigste Maßnahme ist die zeitliche Begrenzung des Senderechtes, entweder als Prozent- oder Stundenregelung.

Die nächste Maßnahme ist eine räumliche Begrenzung (Standortkoordination) wie z. B. im UKW-Grenzabkommen vereinbart, damit das Territorium des Nachbarn nicht beeinträchtigt wird. Trotzdem betreibt z. B. Frankreich einen sehr starken Sender in Straßburg, der weit nach Süddeutschland hinein funkt.

Schließlich gibt es die geregelte Mitbenutzung von Frequenzen, vor allem bei sich überschneidenden Aufgaben der Dienste. Ein Beispiel: Für Such- und Rettungszwecke können militärische Luftfunkstellen die Frequenzen 156,3 MHz 156,375 MHz, 156,5 MHz und 156,675 MHz des UKW-See-funkdienstes mitbenutzen. Mit dieser Regelung wird die Zusammenarbeit der SAR-Dienste auf See ermöglicht. Nur die Bundeswehr verfügt über SAR-Luftfunkstellen (Hubschrauber und Suchflugzeuge), die dann im Einsatz mit den Schiffen auf See funken müssen. Ähnliche Bestimmungen gibt es für Organisationen und Behörden mit Sicherheitsaufgaben, die bestimmte Kontaktfrequenzen teilen oder gar Überschneidungen an gemeinsamen Frequenzbandgrenzen verwenden.

Als generelle Regelung gibt es noch die Einteilung in primäre und sekundäre Nutzer. Hierbei dürfen meist die sekundären Dienste nicht die primären Dienste stören und haben auch meist keinen Anspruch auf Schutz durch nachgeordnete Dienste.

Regelungen des europäischen Normenwerks

Das Europäische Institut für Telekommunikationsnormen (Kürzel ETSI; englisch: European Telecommunications Standards Institute) ist eine der



drei großen Normungsorganisationen in Europa. Sie trifft Festlegungen, mit denen eine möglichst hohe Nutzung durch viele Nutzer oder Dienste im gleichen Frequenzband sichergestellt werden sollen. Das sei am Beispiel der ETSI EN 300 328 V1.7.1 (2006-10) für den 2,4 GHz veranschaulicht.

Regelungen zur Frequenzmitbenutzung:

- Spektrale Leistungsdichte (z. B. 100 mW/MHz)
- Maximale Verweildauer auf einer Frequenz (z. B. 0,4 Sek.)
- Minimale und maximale Einzelfrequenzen im zugewiesenen Frequenzband, (z. B. 14 Frequenzen für nicht adaptive und 20 für adaptive Frequenzspringer)
- Adaptive Frequenzagilität (zielt auf eine gleichmäßige Belastung des Spektrums. Es werden jeweils wenig belastete Frequenzen/Kanäle im Band bzw. die unbenutzten Lücken bevorzugt).

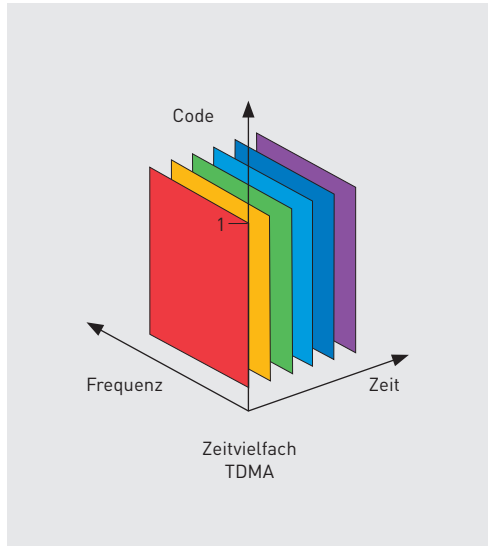
Zugangsregelung, Spectrum Access Techniques:

- Detect And Avoid (DAA)
- Listen Before Talk (LBT)
- Media Access Protokoll.

LAN-Regelungen

Neben den speziellen Funkregelungen gibt es aus den kabelgebunden geschlossenen Netzwerken (LAN) übernommene Senderechtsverwaltungen, entweder mit festen Zeiten (Time Slot) im msec-Bereich oder mit »Staffelübergabe«-Token, die nun auch in funkgestützten Netzwerken (WLAN) angewendet werden. Hierbei werden jedem Teilnehmer im Netz entsprechend seines Datenaufkommens entweder Time Slots zugewiesen, oder es gibt eine feste Reihenfolge der Teilnehmer, in der sie ihre Daten senden können.

Zusammenfassend kann man sagen, dass die betrieblichen Regelungen eine Optimierung des Verkehrsdurchsatzes durch feste oder adaptive »Verkehrsregeln« bei konkurrierenden Teilnehmern ermöglichen und damit einen wichtigen Beitrag zur Optimierung im Funk leisten.



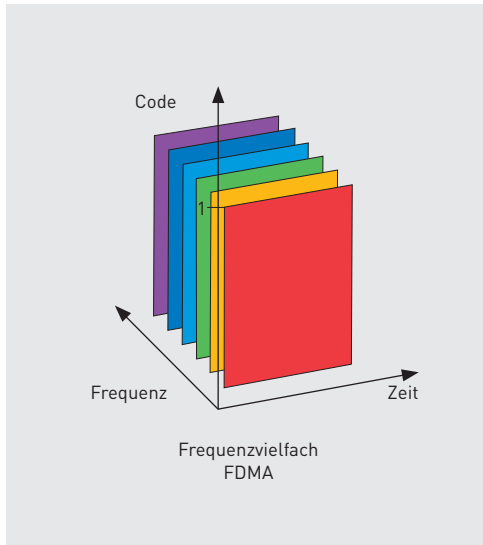
Verschiedene Multiplexverfahren erlauben die optimierte Nutzung von Frequenzen.

Multiplexverfahren zur Mehrfachnutzung von Ressourcen

Im Funk werden Multiplexverfahren zur Mehrfachnutzung der Zeit-Bandbreite-Ressource eingesetzt. Wenn der Zugriff auf diese Ressource über unterschiedliche Frequenzen innerhalb des zugewiesenen Spektrums erfolgt, so spricht man von Frequency Division Multiple Access (FDMA). Erfolgt der Zugriff über die Zeit, handelt es sich um Time Division Multiple Access (TDMA). Breitbandige Digitalverfahren, die nicht nur die ganze Zeit, sondern auch das ganze Spektrum belegen, verwenden unterschiedliche Codierungen und heißen deshalb Code Division Multiple Access (CDMA).

FDMA

Beim FDMA-Verfahren steht ein Teil des Spektrums bzw. ein Kanal die gesamte Zeit dem Nutzer zur Verfügung, die anderen Kanäle den anderen Nutzern. Das bekannteste Beispiel ist die Trägerfrequenztechnik, die viele Fernsprechanäle in einer Richtfunk- oder Kabelstrecke bereitstellt. Es

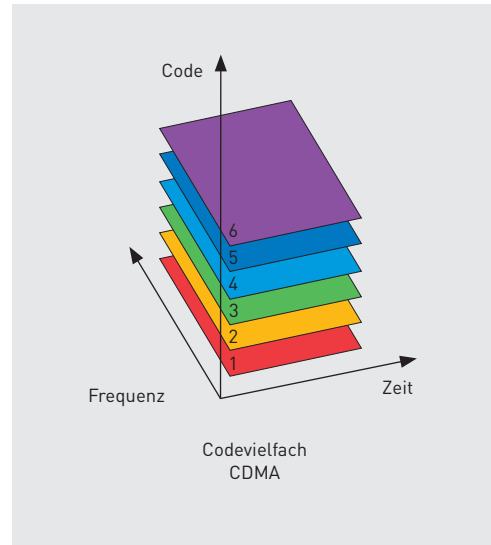


Verschiedene Multiplexverfahren erlauben die optimierte Nutzung von Frequenzen.

können auch zwei Nachrichteninhalte in einem Kanal »gemultiplext« werden, wie z. B. bei der Stereo-Übertragung im UKW-Rundfunk oder die Bild- und Tonübertragung beim Fernsehen.

Bei FDMA handelt es sich (Rundfunkdienste ausgenommen) allgemein nicht um eine feste Zuordnung des Kanals zu einem Nutzer für alle Zeit (synchrone FDMA), sondern nur für die Dauer seiner Informationsübertragung. Daher sind Regelungen erforderlich, so genannte Protokolle, die sicherstellen, dass beim Verbindungsaufbau bereits belegte Kanäle geschützt bleiben und nur frei ausgewählt werden (asynchrone FDMA). Das ergibt eine wirtschaftlichere Nutzung.

Mehrfachnutzung derselben Frequenz zur gleichen Zeit ist bei FDMA nur über eine räumliche Trennung möglich – entweder durch die Entfernung oder aber durch Richtantennen. Die Nutzinformation wird direkt auf die Funkfrequenz moduliert und nicht zuerst auf eine Pulsfolge.



Verschiedene Multiplexverfahren erlauben die optimierte Nutzung von Frequenzen.

TDMA

Beim TDMA-Verfahren steht für einen Teil der Zeit das gesamte Spektrum zu Verfügung, in den anderen Zeitabschnitten nutzen die anderen Teilnehmer das gesamte Spektrum. Die feste Zuordnung eines Time Slots zu einem Teilnehmer (synchrone TDMA) ist ebenfalls nicht erforderlich. Diese Zuordnung benötigt man nur für die Dauer der Informationsübertragung. Ein Teilnehmer mit viel Informationsbedarf kann daher mehrere Time Slots belegen, sofern die anderen entsprechend weniger Bedarf haben. Daher ist auch hier ein Protokoll erforderlich, das die belegten Time Slots schützt und nur freie belegen lässt (asynchrone TDMA).

Mehrfachnutzung desselben Time Slots und des gesamten Spektrums macht wiederum eine räumliche Trennung, entweder durch Entfernung oder durch gerichtete Funkverbindung, erforderlich. Auch hierbei wird die Nutzinformation direkt auf die Funkfrequenzen moduliert und nicht zuerst auf eine Pulsfolge.

CDMA

Beim CDMA-Verfahren wird die Nutzinformation nicht direkt auf die Funkfrequenzen moduliert, sondern zuvor auf einen Code-Pulszug von erheblich höherer Bitrate. Dabei kann der Bandbreitenbedarf und der Zeitbedarf so groß werden, dass die gesamte Zeit-Bandbreite-Ressource benötigt wird.

Eine Mehrfachnutzung ist dennoch möglich, allerdings nur unter Ausnutzung der Eigenschaften der Kodierung. Die anderen Nutzer verwenden einfach einen anderen Code. Da jeder Empfänger seinen Code kennt, kann er ihn aus dem »Stimmengewirr« herausheören, seine Nachricht wieder dekodieren und zur weiteren Bearbeitung bereitstellen.

Die technische Kunst liegt in der optimalen Kodierung, die eine möglichst gute Trennung der verschiedenen Nutzer ermöglichen soll. Man nennt das Kreuzkorrelation. Andererseits soll sich aber der richtige Empfänger schnell und sicher auf seinen Sender synchronisieren können. Das nennt man Autokorrelation.

Mischformen

In moderne Funksystemen werden häufig Kombinationen der zuvor genannten Technologien verwendet. Hierdurch können zusätzliche Vorteile wie z. B. eine erhöhte Abhörsicherheit und der Schutz gegen Störungen erreicht werden.

Prominente Vertreter dieser Mischformen sind die Frequenzsprungverfahren FHSS wie z. B. Bluetooth, die sowohl Zeit- als auch Frequenzvielfachtechnik verwenden.

Um ein Umfeld auf Koexistenz zu untersuchen sind die jeweiligen Kanaldefinitionen genau zu analysieren und ihre Beeinflussung ist entsprechend abzuschätzen.

Fazit und Ausblick:

Bedarf an Frequenzen wächst noch immer

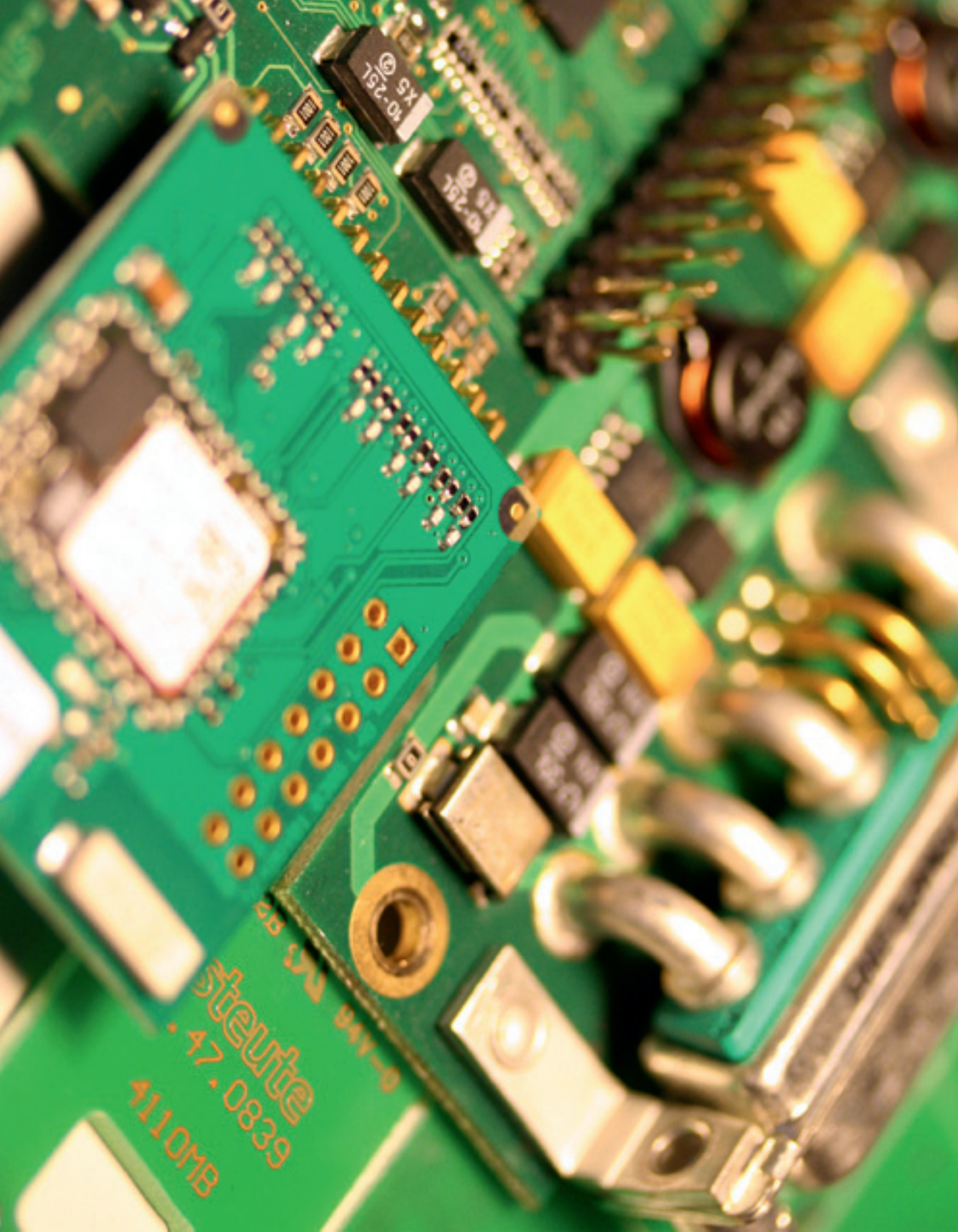
Die hier dargestellten Multiplexverfahren sind letztlich nur nötig, weil die Ressourcen der Funknetze begrenzt sind. Auch heute noch steht der wachsende Bedarf an Frequenzen dem nicht beliebig erweiterbaren Spektrum gegenüber. Rund 40 verschiedene Funksysteme und 2 Millionen Funkdienste sind zu koordinieren. Außerdem greift der Funk nun auch in den Weltraum hinaus. Der Funk hat die allgemeine Globalisierung vorweggenommen, die Teilung der Welt in die drei Funkzonen ist zum Teil überholt, nun müssen gleiche Regeln gelten und eine weltweite Normung wurde nötig. Die ITU hat in der VO Funk das Spektrum von 9 kHz bis 400 GHz vorausschauend mit Reservierungen und Regelungen ausgefüllt, obwohl die heutige Technik den Bereich noch nicht völlig erschließen kann. Aber das ist nur eine Frage der Zeit.

Es bleiben als Fazit folgende Erkenntnisse:

- Auch zukünftig muss mit dem begrenzten Gut des Frequenzspektrums sparsam und sorgfältig umgegangen werden.
- Die Dienste müssen den spezifischen Ausbreitungsbedingungen zugeordnet sein.
- Funk soll nur dann genutzt werden, wenn keine andere Möglichkeit wie z. B. Breitbandkabel vorhanden ist. Hier geht Notwendigkeit vor Komfort.
- Es sind alle Möglichkeiten der Technik auszunutzen, dabei sind die sich bereits entwickelnden Trends zur Optimierung konsequent weiter zu verfolgen.

Die Optimierung verfolgt folgende Ziele:

- Rauschen, Sendeleistung, Reichweite
- Kanalausnutzung, Modulation
- Datenreduktion, Redundanz, Sicherung
- Betriebsverfahren, Zugriff und Vielfachnutzung
- Schutzmaßnahmen



steute
4110MB
47.0839

// Das Funkfeld

05

Störungen und Interferenzen

Kurzbeschreibung der Störschutzverfahren

Ausbreitungsmodelle

Dämpfung

Besondere Ausbreitungsaspekte

Funktopologie

// Störungen und Interferenzen

Neben der reinen Freifelddämpfung gibt es noch weitere Einflussgrößen, die in einem realen Umfeld auftreten, aber schwer beschreibbar sind. Genau wie Licht breitet sich Funk grundsätzlich geradlinig aus. Da Funk eine vergleichbare Wellencharakteristik hat wie Licht, gelten auch vergleichbare Effekte.

Abschattung

Unter Abschattung versteht man einen Effekt, bei dem durch natürliche (Berge, Schluchten) oder künstliche Hindernisse (Bauwerke jeder Art, temporäre Installationen) die freie Ausbreitung des Signals zwischen Sender und Empfänger unterbrochen ist. Geräte im Funkschatten haben nur einen deutlich reduzierten Signalpegel.

Beugung

Als Beugung oder Diffraktion bezeichnet man einen Effekt bei Wellen an einem Hindernis, bei dem sich eine Welle in einem geometrischen Schattenraum des Hindernisses ausbreitet. Durch Beugung entstehen neue Wellen, die sich konstruktiv oder destruktiv überlagern können und damit zu Interferenzen führen.

Fading

Unter Fading versteht man einen Effekt, bei dem ein Signal aufgrund von Brechung oder Reflexion an Objekten den Empfänger auf mehreren Wegen phasenverschoben erreicht. Durch Mehrwegeausbreitung hervorgerufene Fadingverluste sind gerade bei bewegten Objekten von großer Bedeutung.

Reflexion

Treffen Wellen auf im Bezug zur Wellenlänge glatte Oberflächen, werden diese reflektiert. In der Regel wird nur ein Teil der Welle reflektiert, der weitere Wellenanteil breitet sich im Reflexionsmedium aus. An glatten Oberflächen gilt das Reflexionsgesetz, an rauen Oberflächen erfolgt

eine diffuse Streuung. Die reflektierten Wellen überlagern sich konstruktiv oder destruktiv.

Streuung

Treffen elektromagnetische Wellen auf Objekte, die das Wellenfeld beugen oder reflektieren, wird das Wellenfeld gestreut. An den Objekten tritt eine Vor- und Rückwärtsstreuung auf, die von der Oberfläche des Streuobjektes abhängt.

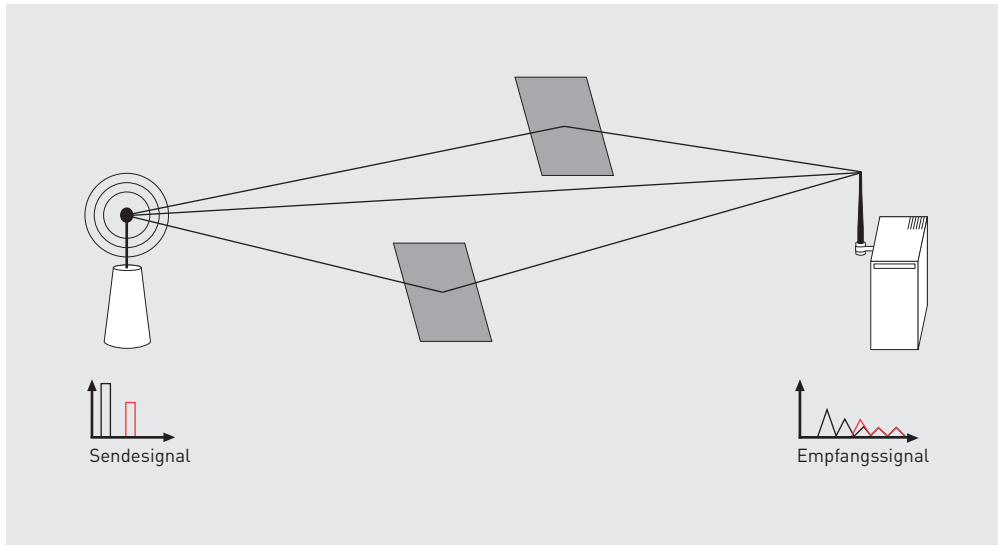
Alle diese störenden Faktoren, die je nach Frequenz und Modulation sowie Störobjekt und Umfeld unterschiedlich stark zu Tage treten, können zur Verschlechterung des Empfangs führen. Das kann vermieden werden, wenn die Antennen Sichtverbindung haben. Deshalb sollte man Antennen so hoch aufstellen, dass sie sich gegenseitig »sehen« können, aber nicht so hoch, dass auch andere Antennen in Sichtweite geraten und gestört werden.

Zudem steht die eigene Sendeleistung in Konkurrenz zu:

- gleichberechtigten oder bevorrechtigten Sendern anderer Dienste
- technischen Geräten wie Elektromotoren mit ihren Kollektorfunkeln
- elektronischen Geräten kleiner Reichweite, wie elektronische Schlüsselsender und Schalter
- natürlichen Störquellen wie Kosmos, Sonne, Mond und Atmosphäre.

Sie alle bringen eine Energie in das Funkfeld und müssen vom eigenen Sender übertönt werden.

Damit derartige Störungen nicht zu einem Abbruch der Informationsübertragung bzw. zu einer Übertragung verfälschter Informationen führen, wurden verschiedene Störschutzverfahren entwickelt, die das folgende Kapitel kurz beschreibt.



Mehrwegeausbreitung schafft erschwerte Empfangsbedingungen

// Kurzbeschreibung der Störschutzverfahren

1. Kurzzeitverfahren (Burst Communications)

Die Daten werden mit hoher Bitrate und möglichst kurzer Dauer durch das Funkfeld gesendet, um dem Störer eine Entdeckung zu verwehren oder aber um seine Reaktionszeit bis zum Störeinsetz auszunutzen.

2. Verschleierte Funkübertragung

Das Sendesignal wird in seiner Bandbreite derart weit gespreizt, dass die spektrale Leistungsdichte unter das natürliche Rauschen fällt und daher der Funkbetrieb vom Störer nicht entdeckt werden kann. Nur der autorisierte Empfänger entspreizt das Signal wieder richtig und hebt es über den Rausch- und Störpegel hervor.

3. Frequenzsprungverfahren (Frequency Hopping)

Das »Frequency Hopping Spread Spectrum« (FHSS) sendet kurze Datenbursts auf ständig wechselnden Frequenzkanälen. Der Störer kann

wegen seiner Reaktionszeit nicht folgen. Stört er aber präventiv breitbandig, so muss er seine Leistung so breit verteilen, dass die spektrale Leistungsdichte dann nicht mehr ausreicht, um den hohen Leistungspuls des Springers wirksam zu stören. FHSS ist zugleich eine Möglichkeit zur simultanen Nutzung desselben Frequenzbandes durch mehrer Nutzer, sofern deren Kollisionsrate unter 40 % bleibt.

4. Direktsequenz-Spreizverfahren

Das »Direct Sequence Spread Spectrum« (DSSS) moduliert eine um Größenordnungen höhere Pulsrate einer binären Zufallsfolge (Direktsequenz) mit dem Nutzsignal und gibt sie auf das Funksignal. Dadurch wird wie bei der verschleierten Funkübertragung die spektrale Leistungsdichte minimiert, muss aber nicht unter das natürliche Rauschen sinken. Dieses Verfahren ist sehr robust gegen alle möglichen Störverfahren, da die Störsignale beim autorisierten Empfänger durch den Entspreizungsprozess um dasselbe Maß abgeschwächt werden wie das Spreizver-

hältnis von Direktsequenzbitrate (Chirate) zu Nutzbitrate beträgt. Hier wird der Störer also in den Aufwand einer Leistungseskalation getrieben.

5. Chirp

Als ein Chirp (von engl. chirp = Zwitschern) bezeichnet man in der Signalverarbeitung ein Signal, dessen Frequenz sich zeitlich ändert. Bandspreizende Modulationsverfahren wie Chirp Spread Spectrum (CSS) eignen sich dazu, Nutzsignale aus dem Rausch- oder Störpegel durch Pulskompression auf der Empfangsseite mit SAW-Filtern (Surface Acoustic Wave, akustische Oberflächenwellen) wieder herauszuholen. Technische Anwendungen liegen vor allem bei SAR (Synthetic Aperture Radar)-Systemen in Flugzeugen und Satelliten vor.

6. OFDM

Bei OFDM (Orthogonal Frequency Division Multiplex) handelt es sich um ein Modulationsverfahren, das mehrere orthogonale Trägersignale innerhalb des Funkkanals zur digitalen Datenübertragung verwendet. Kommt es innerhalb der Kanalbandbreite des OFDM-Signalspektrums zu einer schmalbandigen Störung, können diejenigen Trägersignale, die von der Störung betroffen sind, von der Datenübertragung ausgenommen werden. Die gesamte Datenübertragungsrate sinkt damit nur um einen kleinen Teil. OFDM eignet sich daher eher gegen Zufallsstörungen und Wobbelstörer (Chirp) als gegen Breitbandstörungen.

// Ausbreitungsmodelle

Aufgrund der zuvor beschriebenen Eigenschaften ist eine exakte Beschreibung von Funkausbreitung bei realen Gegebenheiten nur schwer möglich. Um eine Vergleichbarkeit von Reichweiten unterschiedlicher Geräte zu ermöglichen, werden unterschiedliche Kanalmodelle zum Vergleich herangezogen.

- LOS (Line of Sight) – beschreibt die reine Sichtverbindung zwischen Sender und Empfänger. In der Regel wird hier eine störungsfreie Sichtverbindung vorausgesetzt.

- NLOS (Non Line of Sight) – beschreibt eine Kommunikationsbeziehung, bei der sich Sender und Empfänger nicht sehen. Hier ist eine Vergleichbarkeit von Systemen kaum gegeben, da die Randbedingungen nicht standardisiert sind.

- AWGN (Additive White Gaussian Noise). Ein AWGN-Kanal ist ein idealisierter Kanal mit reiner LOS-Verbindung, bei der die reale Störung durch ein additives weißes Rauschen nachgebildet ist. AWGN-Kanäle werden häufig in mathematischen Modellen eingesetzt, spiegeln aber nicht die Realität wider.

In einer realen Umgebung kommen immer Überlagerungseffekte von Funksignalen vor. Hierdurch erreichen die ausgesendeten Funkwellen einen Empfänger auf unterschiedliche Wege, was man auch als Mehrwegeausbreitung bezeichnet. Ein unausweichlicher Vorgang in realen Umgebungen. Unterschiedliche Modulationsverfahren sind in unterschiedlicher Weise empfindlich für Reflexions- und Mehrwegeszenarien.

// Dämpfung

Um zuverlässige Ausbreitungssituationen zu erzielen, reicht es nicht aus, die typischerweise angegebenen LOS-Reichweiten von Funksystemen als Maßstab zu nehmen. Die idealisierten Bedingungen werden im realen Umfeld durch Wände und Decken korrumpiert, so dass in der Regel deutlich geringere Reichweiten erreicht werden.

Betrachtet man die gängigen Baustoffe, so kann man ein sehr unterschiedliches und zudem frequenzabhängiges Dämpfungsverhalten feststellen. In den folgenden Abbildungen sind einige Grafiken aus der BSI-Richtlinie »Elektromagneti-

sche Schirmung von Gebäuden« entnommen, die sehr qualifiziert das Dämpfungsverhalten verschiedener Baustoffe und Bauausführungen beschreibt.

Aus den vorangestellten Grafiken wird deutlich, dass man intuitiv keine qualifizierte Aussagen über das Dämpfungsverhalten von Baustoffen machen kann. Generell gilt: Niedrige Frequenzen werden wesentlich besser durch Wände hindurch übertragen als hohe Frequenzen. Für eine erste Abschätzung reicht auch die Tabelle rechts.

// Besondere Ausbreitungsaspekte

Sind mehrere Funkteilnehmer in einem Umfeld aktiv, kann es weitere Effekte geben, die zu negativen Begleiterscheinungen beitragen. Dazu gehört das Hidden-Station-Problem. Man bezeichnet damit eine Kommunikationsbeziehung, bei der ein Teilnehmer eine aktive Kommunikation nicht erkennen kann, weil er sich außerhalb des Übertragungs- und Erkennungsbereiches befindet.

Ein Beispiel:

Station A kommuniziert mit Station B. Station C möchte auch mit Station B Verbindung aufnehmen, befindet sich aber außerhalb des Erkennungsbereichs von A. C kann nicht erkennen, dass A mit B redet. Nimmt C jetzt die Kommunikation mit B auf, kann es zu einem Konflikt in der Station B kommen, da C unkoordiniert mit A auf B einredet. In der Regel führt dies zu einem Kommunikationsabbruch auf beiden Seiten.

Ein anderes Kommunikationsszenario ist das Exposed-Station-Problem. Es tritt auf, wenn eine Station durch die Kommunikation anderer Geräte beeinflusst wird. In dem abgebildeten Fall kommuniziert Station B aktiv mit Station A. Station C möchte eine Verbindung mit D eingehen. C bemerkt, dass der Kanal durch B belegt ist, obwohl eine Kommunikation prinzipiell zu D aufgebaut

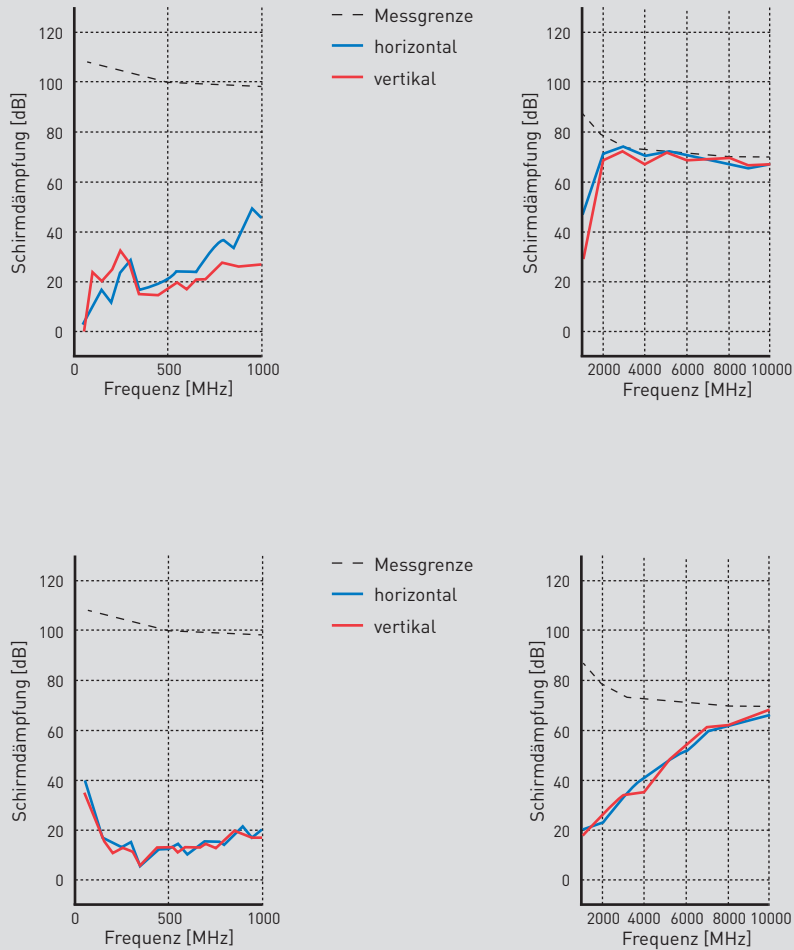
Material	Dicke	Dämpfung
Holz	< 30 cm	1 ... 10 %
Gips (-karton)	< 10 cm	1 ... 10 %
Glas (unbeschichtet)	< 5 cm	1 ... 10 %
Pressspan	< 30 cm	30 %
Bimsstein	< 30 cm	10 %
Gasbetonstein	< 30 cm	20 %
Ziegelstein	< 30 cm	35 %
Armierter Beton	< 30 cm	30 ... 90 %
Metallgitter	< 1 cm	90 ... 100 %
Metall, Alukaschierung	< 1 cm	100 %
Regen, Nebel, Schnee	/	60 ... 90 %

Dämpfungsverhalten einzelner Werkstoffe

werden könnte. Ein Verbindungsaufbau kommt nicht zustande.

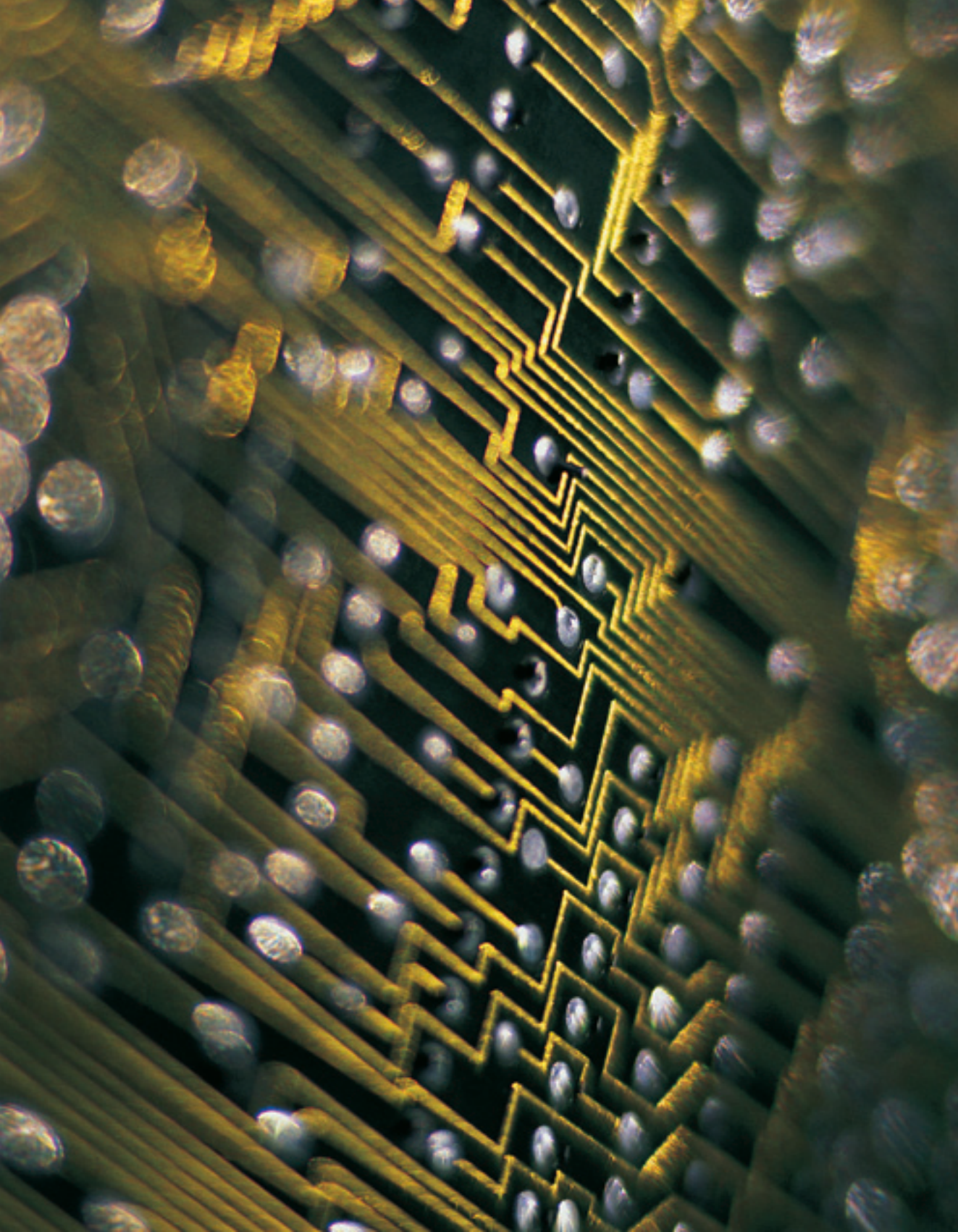
// Funktopologie

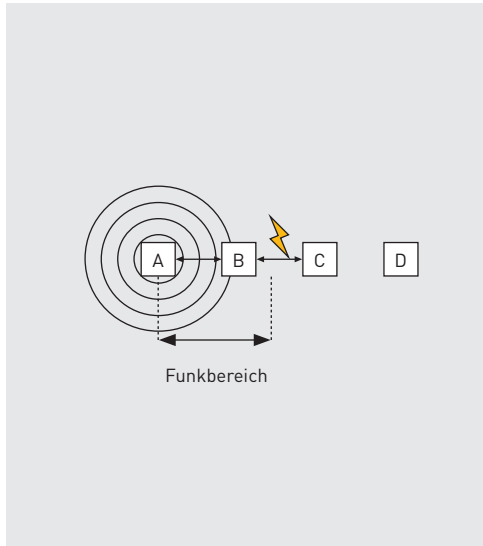
Ein zentraler Aspekt beim Einsatz von Funktechnologien ist die Konfiguration der möglichen Netzwerktopologien. Man wünscht sich ein infrastrukturfreies Netz, bei dem mobile Einheiten einfach und unkompliziert miteinander kommunizieren können. Aber sind strukturfreie Netze wirklich optimal? Ein gutes Beispiel gibt die Mobiltelefonie. Die Illusion, von Handy zu Handy zu telefonieren, wird in der Realität durch ein komplex gemanagtes Netzwerk realisiert. Eine Funkverbindung besteht nur zwischen den Basisstationen und den mobilen Geräten, der Rest der Kommunikation wird über klassische Infrastrukturnetze abgewickelt. Eine optimale Struktur liegt folglich in der richtigen Kombination von direkter und infrastrukturfreier Verkabelung.



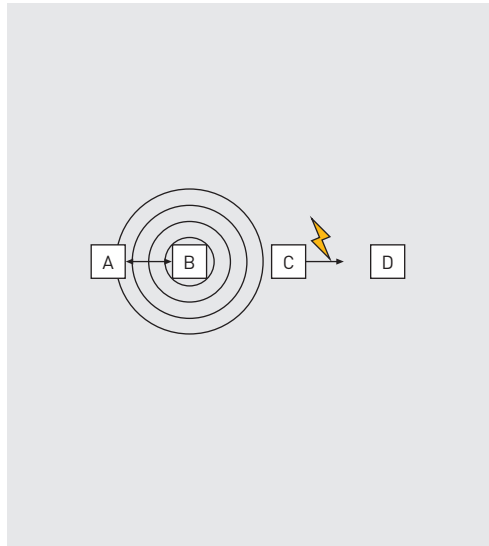
Oben: Frequenzabhängiges Dämpfungsverhalten einer Kalksandsteinmauer (Quelle: BSI)

Unten: Frequenzabhängiges Dämpfungsverhalten einer 20 cm stahlarmierten Betondecke (Quelle: BSI)





Das Hidden-Station-Problem betrifft Stationen außerhalb der Funkreichweite



Das Exposed-Station-Problem begrenzt die Anzahl möglicher Verbindungen

Stationäre Infrastruktur

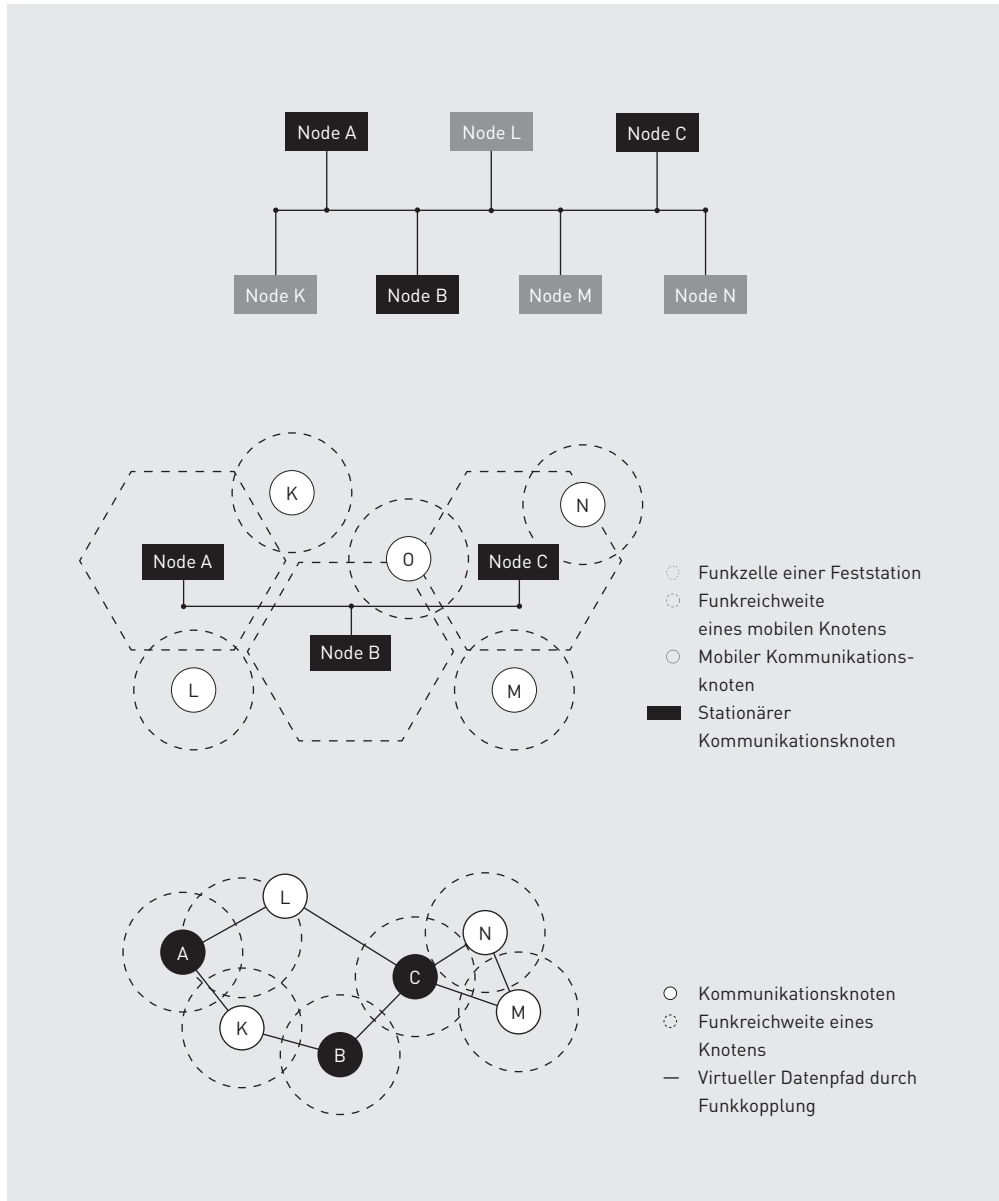
Klassische stationäre, kabelgebundene Netzwerke weisen gegenüber funkbasierten Systemen entscheidende Vorteile auf. Die Struktur ist fest und nur noch von den angeschlossenen Systemen abhängig. Hierdurch ist das Verhalten bei bekannter Topologie und Technologie vorhersagbar. Feldbussysteme und Ethernet-Netzwerke zeigen, dass eine stationäre Infrastruktur relativ problemlos beherrschbar ist.

Mobile Infrastrukturnetzwerke

Eine Flexibilisierung der starren Struktur ermöglicht Infrastrukturnetzwerke für mobile Anwendungen. Das Netz wird zu einem Infrastrukturnetzwerk. Die unterschiedlichen Accesspunkte sind durch das Infrastrukturnetzwerk verbunden. Je nach Auslegung können die Zugriffspunkte zentral oder dezentral verwaltet werden. Ebenfalls kann die Abdeckung der Fläche entweder vollständig oder punktuell sein. Bei den zellularen GSM-Netzen ist die vollständige Abdeckung der Umgebung mit aneinandergrenzenden Funkzel-

len unabdingbar. Für individuelle Anwendungen sind aber auch lückenhafte zellulare Strukturen denkbar, da die Funkzellen untereinander ohnehin statisch verbunden sind. Entscheidender Vorteil einer derartigen Struktur ist das relativ sicher vorhersagbare Verhalten der Systeme. Durch den Single-Hop der mobilen Teile zur Feststation ist mit der Streckenkenntnis der stationären Infrastruktur das Kommunikationsverhalten vorhersagbar. Auch sind die Datensicherheit (Security) und Abrechnungsverfahren in einem Infrastrukturnetzwerk verhältnismäßig einfach zu handhaben.

Besondere Anforderungen gelten für mobile Geräte. Das Binden von mobilen Geräten an einer einzelnen stationären Station ist dabei kein Problem. Bewegt sich das mobile Gerät aber durch das gesamte Netz über Funkzellengrenzen hinweg, sind neue Herausforderungen zu meistern. Einerseits muss das mobile Gerät an jeder beliebigen Stelle des Netzwerks gefunden und mit dem Netzwerk verbunden werden. Man spricht



Oben: Stationäre Linienverkabelung ist problemlos beherrschbar.

Mitte: Infrastrukturnetze sind gut beherrschbar und finden in verschiedenen Funktechnologien Anwendung.

Unten: Ad-hoc-Netzwerke ermöglichen in Zukunft die infrastrukturfreie Kommunikation über picozellulare Strukturen hinweg.

hier auch von Roaming. Andererseits sollte die Kommunikation eines bewegten Geräts auch beim Verlassen von Netzzellengrenzen nicht abgebrochen werden. Das Gerät sollte also von einer stationären Zelle zur anderen vollkommen transparent weitergereicht werden. In diesem Fall spricht man von Handover. Beide Verhaltensmuster sind in der Regel für mobile Geräte gewünscht. In der technischen Praxis ist dieses Verhalten sowohl in GSM-Netzen als auch bei WLAN 802.11 nach der WIFI-Spezifikation vorgesehen und umgesetzt.

Peer-to-Peer und Ad-hoc-Netzwerke

Verzichtet man auf die Infrastrukturkomponenten, spricht man von so genannten Peer-to-Peer-Netzwerken. Hierbei kommunizieren die mobilen Geräte unmittelbar miteinander, ohne auf Infrastrukturkomponenten zurückgreifen zu müssen. Dieses Verhalten wird heute typischerweise bei Bluetooth und WLAN 802.11-Netzwerken angewendet. Der Verzicht auf Infrastruktur hat schon aus Kostengründen besonderen Charme. Problematisch ist jedoch die Sicherheit des Netzzugangs, da man in der Regel nicht weiß, welcher Sender bzw. Rechner sich gerade in das Netz integriert.

Eine besondere Form dieser sogenannten Peer-to-Peer-Netze ist das Ad-hoc-Netzwerk, bei dem sich die Stationen selbst untereinander organisieren und gegebenenfalls Nachrichten zu anderen Stationen innerhalb des Netzverbundes weiterreichen, ohne selbst die volle Reichweite zu besitzen. Diese besondere Form der selbst organisierenden Netze ist Gegenstand der Forschung und lässt spannende Anwendungsszenarien zu. Besonders bei Packet Switching können die Laufwege der Datenpakete je nach Netztopologie weltweit reichen und durch Überflutung fremder Datenpakete im eigenen Netz zum Verlust der Netzkontrolle führen.

Der besondere Unterschied zu Peer-to-Peer-Netzen ist die Tatsache, dass bei Ad-hoc-Netzwerken die mobilen Geräte selber Teilfunktionen wie Router und Gateway besitzen und Nachrichten vollkommen transparent weiterreichen. Die Nachrichtenverteilung wird damit vollständig in die Endgeräte delegiert, die nicht nur den eigenen Datenverkehr abwickeln, sondern in einer Tandemfunktion auch den Verkehr anderer Stationen vermitteln. Im Weiteren bilden sich Ad-hoc-Netzwerke dynamisch. Das bedeutet, dass ein Netzwerk nur für inkrementelle Zeiten als statisch angesehen werden kann.

Bisher sind noch nicht alle Probleme im Bereich der Ad-hoc-Netzwerke gelöst. Im wissenschaftlichen Bereich findet man Ansätze unter den Stichworten Autonome Mobile Plattform und Multi-Hop-Netzwerke. Unter der RFC 2501 ist bereits ein Standard für derartige Netzwerke unter MANET (Mobile Ad Hoc Networking) definiert.

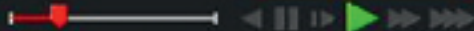
3 Min 6 Sec



14:42:52

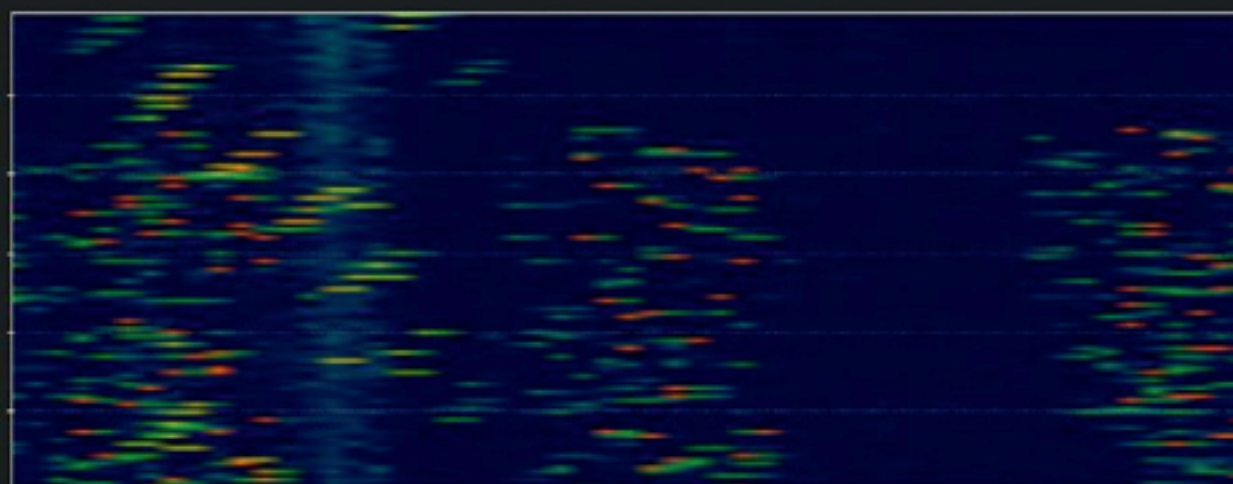


Timeframe: 1 min



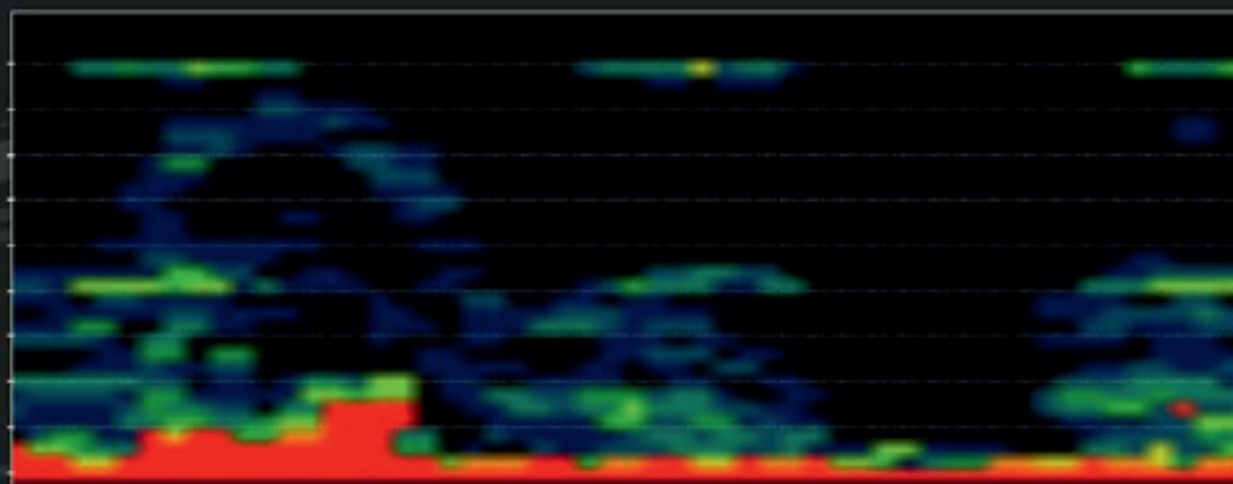
Time [sec]

50
40
30
20
10



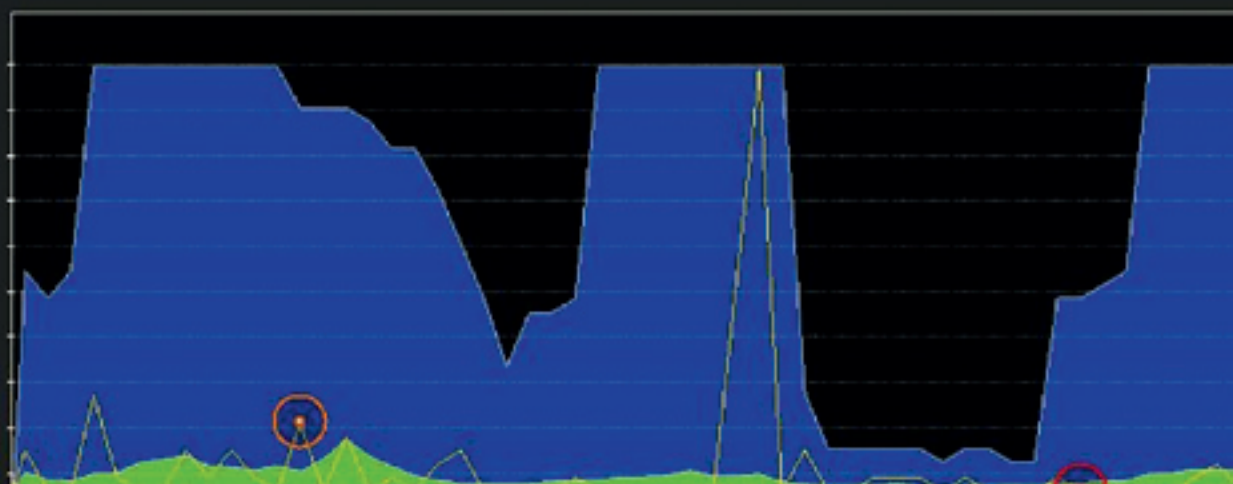
Amplitude [dBm]

-50
-55
-60
-65
-70
-75
-80
-85
-90
-95



Amplitude [dBm]

-50
-55
-60
-65
-70
-75
-80
-85
-90
-95



// Der Funk-Kanal

06

Kanalausnutzung durch Modulation

Digitalisierung, Datenreduktion, Redundanz und Fehlersicherung

// Kanalausnutzung durch Modulation

Wurde bisher die äußere Optimierung von Funksystemen mit Frequenz-, Leistungs- und Standortkoordination betrachtet, so geht es jetzt um die innere Optimierung, also um die bestmögliche Ausnutzung der zugewiesenen Bandbreite. Dazu wählt man das geeignete Modulationsverfahren aus.

Amplituden- und Einseitenbandmodulation (AM/SSB)

In Zeiten der analogen Übertragung wurde zunächst eine Sender- oder Trägerfrequenz in ihrer Amplitude moduliert. Man nennt dies Amplitudenmodulation (AM). Dabei bilden sich zwei Seitenbänder aus, die gleichen Nachrichteninhalte haben, nämlich HF-Träger plus NF und HF-Träger minus NF. Eines der Seitenbänder kann man weglassen, ohne Information zu verlieren. Man nennt das Einseitenbandmodulation, (englisch Single Side Band/SSB). Dazu gibt es Varianten mit Trägerfrequenz, mit verminderter Trägerfrequenz und mit unterdrückter Trägerfrequenz.

Im Ergebnis kommt man mit der halben Bandbreite aus und kann die andere Hälfte anderweitig nutzen, z. B. indem man entweder den Niederfrequenzbereich verdoppelt, etwa von 3,4 kHz (Sprachkanal) auf 7 kHz (Musikkanal) oder indem man zwei verschiedene Tonkanäle in einem Funkkanal überträgt.

Im modernen Kurzwellenfunk ist Einseitenbandübertragung üblich. In Mittel- und Langwelle kommt diese Modulation in Einzelfällen vor. Datenübertragung über Kurzwelle geschieht meist durch Umtastung von 2^n Tonfrequenzen mit so genannten Parallen Modems (Modulator-Demodulator, für n = ganze Zahlen).

Dabei ist es von Vorteil, dass das selektive Fading (Schwund) im Übertragungskanal nicht alle Tonkanäle gleichzeitig betrifft und somit bei an-

gepassten Fehlersicherungsverfahren eine gute Übertragungssicherheit erreicht wird. Das andere Verfahren nutzt eine schnelle serielle Bitübertragung mit Laufzeitentzerrung (serielles Modem). Beide Verfahren haben spezifische Vor- und Nachteile.

Breitbandige Vielkanalsysteme zur Telefonübertragung über Richtfunk und Kabel nutzen die Einseitenbandtechnik heute noch mit der Trägerfrequenztechnik. Dabei werden gleichzeitig 12, 24, 48, 60, 120, 240, 480 oder 960 Telefonkanäle übertragen. Auch das analoge Fernsehen nutzt Einseitenbandtechniken. Für qualitativ hochwertige Bild- und Tonübertragungen ist diese Technik aber nur eingeschränkt geeignet.

Frequenzmodulation (FM)

Mit der Einführung von UKW gab es sehr viel mehr Bandbreite – anstelle von 1 MHz wie bei der Mittelwelle zuerst 12 MHz, später 20 MHz. Die Chance wurde genutzt zur Einführung der Frequenzmodulation FM. Dabei schwingt die Sendefrequenz bei gleich bleibender Amplitude im Takt der NF um die Mittenfrequenz. An Stelle der Amplitude tritt die maximale Abweichung von der Mittenfrequenz, der Frequenzhub.

FM ist immun gegen viele Störungen, vor allem gegen Blitze, weil die Störungen der Amplituden abgeschnitten werden (englisch: clipping). Außerdem wird durch die Verbreiterung der Kanalbandbreite auf 300 kHz gegenüber der NF-Bandbreite von 20 kHz für Musik ein Gewinn erzielt von 1:15 oder 12 dB. Diese Frequenzspreizung führt zur erheblichen Steigerung der Übertragungsqualität. Damit ist HiFi möglich. Aber eine Frequenzökonomie ist das nicht, eher das Gegenteil. Bonuseffekt dieser großen Bandbreite war die spätere Erweiterung auf Stereoübertragung. Wegen der quasi-optischen Ausbreitung können die UKW-Kanäle häufig zugeteilt werden. UKW hat sich weltweit als das Band für die Radioübertragung etabliert und entlastet daher andere Frequenzbänder.

Digitale Modulationsverfahren

Bei den digitalen Modulationsverfahren liegt die Information in Bits vor, hierbei werden Bits als »Ein« Zustand, No-Bits als »Aus« Zustand übertragen. Die einfachste Form ist Morsen, bei dem die Senderfrequenz ein- oder ausgeschaltet wird oder richtiger gesagt, indem die Amplitude umgetastet wird – daher der englische Ausdruck Amplitude Shift Keying (ASK). Die Umtastung der Sendefrequenz zwischen zwei diskreten Werten bei durchlaufender Amplitude heißt Frequenzumtastung (Frequency Shift Keying/FSK).

Eine häufige Form ist die »weiche« Frequenzumtastung, bei der die Bits vorher durch ein Gaussfilter geformt werden, (Gaussian Frequency Shift Keying, GFSK). Das GFSK-Verfahren wird z. B. bei Bluetooth, DECT und W-LAN verwendet. Die Umtastung der Phase der Sendefrequenz um 180° bei gleich bleibender Amplitude und Frequenz ist das dritte und wichtigste digitale Modulationsverfahren. Sie heißt Phasenmodulation (Phase Shift Keying, PSK; siehe weiter unten).

Mischformen der digitalen Modulation

Neben den Grundformen der digitalen Modulation gibt es noch Mischformen mit analogen Verfahren. Discrete Multitone Transmission (DMT) ist ein Multiträgerverfahren, bei dem im Übertragungskanal viele diskrete analoge Tonfrequenzen parallel getastet und übertragen werden. Dieses Verfahren wird bei der ADSL-Technik zur Datenübertragung im ISDN-Kanal genutzt.

Die Quadraturamplitudenmodulation (QAM) ist eine Modulationsart, die Amplitudenmodulation und Phasenmodulation miteinander kombiniert. Dabei werden derselben Trägerschwingung zwei voneinander unabhängige Signale aufgeprägt. Im Prinzip werden die Signale jeweils per Amplitudenmodulation auf einen Träger gleicher Frequenz, jedoch mit um 90° verschobener Phase, moduliert. Anschließend werden die beiden derart modulierten Trägerschwingungen addiert.

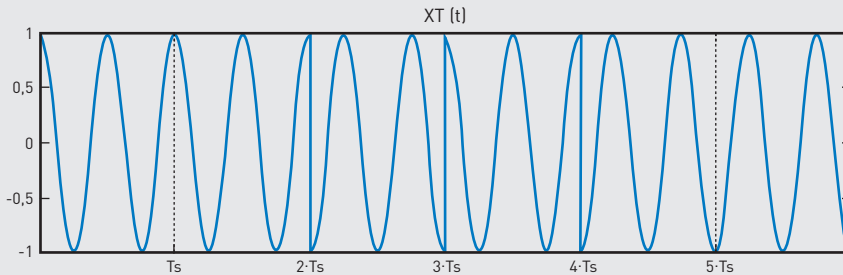
OFDM (Orthogonal Frequency Division Multiplex) ist eine spezielle Implementierung des Multiträger-Verfahrens. Die zu übertragende Nutzinformation mit hoher Datenrate wird zunächst auf mehrere Teildatenströme mit niedriger Datenrate aufgeteilt. Diese Teildatenströme werden jeder für sich mit einem herkömmlichen Modulationsverfahren wie der Quadraturamplitudenmodulation mit geringer Bandbreite moduliert. Anschließend werden die einzelnen Trägersignale addiert. Das bewirkt, dass sich die Sub-Trägersignale möglichst wenig gegenseitig beeinflussen.

Phasenmodulation PM

Die Phasenmodulation ist eng verwandt mit der Frequenz- und Winkelmodulation. Phasen- und Frequenzmodulation sind Formen der Winkelmodulation. Hierbei handelt es sich um Phasenumtastung (engl. Phase Shift Keying PSK). Dabei wird die Phase einer Sinusschwingung (Träger) durch Phasenverschiebung moduliert. Man spricht von binärer Phasenmodulation, BPSK, wenn zwischen zwei Phasenlagen umgeschaltet (umgetastet) wird. Typischerweise entsprechen die Phasenlagen 0° und 180° den binären Zuständen »0« und »1«.

Bei einer mehrstufigen Phasenmodulation repräsentiert eine Umtastung eine Folge mehrerer Bits. Bei 4-PSK (QPSK) wird zwischen 4 Phasenzuständen umgeschaltet, z. B. 45° , 135° , 225° und 315° . Jede Phasenlage entspricht 2 Bit. Bei 8-PSK sind es 3 Bit, etc. Bei der Übertragung von Faksimiles über das Telefonnetz wird zum Beispiel 4-PSK verwendet. Bei der GSM-Erweiterung EDGE (Enhanced Data Rates for GSM Evolution) wird beispielsweise 8-PSK eingesetzt und damit die Bruttoübertragungsrate gegenüber einer binären Modulation im sonst gleichen Kanal verdreifacht.

QPSK wird bei der Signalübertragung in digitalen Satellitenkanälen, bei der terrestrischen Ausstrahlung digitaler Signale und auch bei drahtgebundenen Übertragungsverfahren verwendet.



Im Bild wird das binäre Signal ooLoLL durch Phasensprünge dargestellt

Mittlerweile findet diese Art der Modulation auch Anwendung bei der HSDPA-Technik in UMTS-Netzen (High Speed Downlink Packet Access). Hier wird die Datenrate von 384 kBit/s auf ca. 2 Mbit/s angehoben und ermöglicht im Mobilfunk vergleichbare Datenraten zu DSL im Festnetz. Die QPSK liefert physikalisch die gleichen Ergebnisse wie eine 4-QAM, die allerdings eine Amplituden- anstatt einer Phasenmodulation nutzt und sollte deshalb nicht mit dieser verwechselt werden.

Die Phasenmodulation lässt sich hervorragend an die Übertragungseigenschaften eines vorgegebenen Kanals anpassen und hat sich für die digitalisierte Übertragung von Sprache, Rundfunk, Fernsehen und Daten weltweit durchgesetzt. Der Empfänger muss nicht mehr den genauen Wert einer analogen Amplitude oder Frequenz detektieren, sondern es genügt zu entscheiden, ob ein Bit vorliegt oder nicht. Das macht die Phasenmodulation so robust gegen natürliche Schmutzeffekte im Übertragungskanal.

Der Signal-/Störabstand kann verringert werden, und das führt bei gleicher Sendeleistung zu größeren Reichweiten oder bei vorgegebener Reichweite zur Reduzierung der Sendeleistung.

Entscheidender Vorteil aller digitalen Modulationsverfahren ist die Übertragung einer möglichst großen Datenrate durch eine optimale Anpassung an die physikalischen Eigenschaften des Übertragungskanals.

Pulsformung

Die steilen Pulsflanken der digital vorliegenden Information führen bei jedem Modulationsverfahren zur Bildung von Oberwellen, die über die zugewiesene Bandbreite hinausreichen können und Nachbarkanäle stören.

Ein Impuls ist eine Amplitudenänderung in der Zeitdimension. Setzt man dies in die Frequenzdimension um, so entstehen eine Grundfrequenz und ein Spektrum von harmonischen Frequenzen. Rechnerisch ist das mit der Fourier-Transformati-

on beweisbar. Je steiler nun die Flanken des Impulses und je schmaler der Impuls ist, um so höher wird der Leistungsanteil der Oberwellen.

Der Empfänger einer digital modulierten Nachricht benötigt aber keine supersteilen Flanken. Ihm genügt es zu wissen, ob in dem Zeitfenster für einen Impuls eine Spannung vorliegt, die einen bestimmten Schwellwert übersteigt oder nicht. Die steilen Flanken kann er sich dann selbst wiederherstellen.

Das Problem hat zwei Lösungen. Die erste besteht darin, dass man die Datenrate so weit absenkt, dass die Oberwellen in der erlaubten Bandbreite bleiben. Die andere und bessere Lösung besteht darin, die Impulse »weicher« zu machen, indem man die Flanken sanft ansteigen und abfallen lässt. Dazu schickt man die »harten« Impulse durch ein pulsformendes Filter.

In der Praxis haben sich drei Pulsformen durchgesetzt. Beim Cosinus-Impuls handelt es sich um die positive Halbwelle einer Cosinus-Schwingung. Beim Cosinus-Quadrat-Impuls handelt es sich um eine Glockenform, wie sie zwischen den beiden Minimalwerten einer Cosinus-Schwingung dargestellt wird, allerdings mit doppelter Grundfrequenz. Und beim Gauß-Impuls handelt es sich um eine breitere Glockenform wie bei der Gaußschen Normalverteilung, allerdings wird der Puls an den Flanken beschnitten. Dieser Puls gilt als der mit dem geringsten Oberwellenanteil.

Nimmt man einem rechteckigen Signal, das abwechselnd aus gleich langen Bit besteht, immer mehr Oberwellen weg, so bleibt am Ende nur die sinusförmige Grundschwingung übrig. Dabei trägt eine vollständige Schwingung 2 Bit Information. Kurz gesagt: 1 Hertz = 2 Bit. Folgen aber die Bits nicht abwechselnd, braucht man doch mehr Bandbreite. Die Grenze, bei der man gerade noch möglichst viel Bits durch den engen Kanal übertragen kann, liegt je nach Randbedingungen

zwischen 1,3 und 1,6 Bit pro Hertz. Die dabei entstehenden Oberwellen reichen zwar in den Nachbarkanal, sind aber in ihrer Störleistung schwach genug, um dessen robuste Datenübertragung nicht unbrauchbar zu machen. Davon machen viele digitale Dienste Gebrauch, u. a. auch das digitale Fernsehen über Satelliten. Im digitalen Flugfunk werden beispielsweise 16 kBit/sec im 25 kHz-Raster übertragen, das sind 1,5 Bit pro Hertz.

Polarisation

Eine viel genutzte Möglichkeit zur Optimierung besteht darin, einen Funkkanal doppelt zu belegen, indem die beiden Übertragungskanäle nur durch die horizontale oder vertikale Polarisierung der Funkwellen im gleichen Frequenzband getrennt sind. Das ist Standard in der Satellitentechnik.

// Digitalisierung, Datenreduktion, Redundanz und Fehlersicherung

Analoge Signale

Zur Übertragung einer akustischen oder optischen Information über einen Funkkanal muss das jeweilige Signal zunächst in eine elektrische Form gebracht werden. Das erledigt ein Mikrofon, welches Schallschwingungen in elektrische Schwingungen umsetzt oder eine ältere noch analoge Videokamera. Aber auch viele Messwerte entstehen noch in analoger Form, selbst wenn sie direkt als elektrische Werte vorliegen.

Diese Signale können unmittelbar zur analogen Modulation von Funkkanälen herangezogen werden und belegen dann eine typische Bandbreite, wie im vorigen Kapitel dargestellt. Die analoge Übertragung ist zwar angenehm schmalbandig, aber leider sehr empfindlich gegen Störungen im Übertragungskanal, die später nicht mehr eliminiert werden können.

Kaskadiert man mehrere Funkfelder hintereinander, um große Entfernungen zu überbrücken, so

addieren sich die Störanteile, und die Verbindung degeneriert bis zur Unbrauchbarkeit. Daher hat die CCIR (heute ITU-R) für Richtfunk und Kabel den hypothetischen Bezugskreis von 2500 km definiert und Störanteile so festgelegt, dass mit 3 Picowatt pro km (3 pW/km) einerseits noch eine verständliche Fernübertragung möglich ist, andererseits aber die Anforderungen an die Technik noch zu bezahlbaren Geräten führen. Aber die Übertragungsgrenze von 2500 km Reichweite bleibt bestehen.

Digitale Signale

Bei der Übertragung mit digitaler Modulation können Störungen im Funkkanal auf der Empfangsseite ausgeblendet werden, so dass das empfangene Signal ziemlich fehlerfrei zurückgewonnen wird. Somit findet eine Reichweitenbegrenzung nicht mehr statt. Das ist einer der wichtigen Gründe, weshalb man zunehmend zur digitalen Übertragung greift. Doch dazu müssen die analog entstehenden Informationen erst »digitalisiert« werden. Hierfür haben sich mehrere Verfahren bewährt, von denen hier die Delta-Modulation und die Puls-Code-Modulation wegen ihrer Bedeutung kurz dargestellt werden.

Bei der Delta-Modulation werden analoge elektrische Tonsignale, z. B. 16.000 mal in der Sekunde abgetastet und verglichen. Wenn die Amplitude steigt, wird eine binäre 1 gesendet, wenn sie fällt eine binäre 0, bei gleich bleibenden Wert wird eine 101010-Folge gesendet. Die Bitrate ist also 16 kbps. Das ist für Sprachübertragung ausreichend, für Musikübertragung aber nicht. Dazu bräuchte man höherer Abtastraten und eine Signal-Vor- und -Nachbereitung mit beispielsweise Pre-Emphase und De-Emphase.

Bei der Puls-Code-Modulation PCM wird ebenfalls in konstanten Zeitabständen der analoge Wert abgetastet. Der Wert wird aber mit einem Maßstab gemessen und als digitale Zahl ausgegeben. Im ISDN-Telefonkanal wird die Sprache 8000 mal

in der Sekunde abgetastet und als ein Byte von 8 Bit Länge ausgegeben. Der Maßstab hat demnach $2^8 = 256$ Unterteilungen. Die Bitrate im Telefonkanal ergibt sich damit zu $8 \text{ Bit} \times 8000/\text{sec} = 64 \text{ kbps}$. Auch hier werden Pre- und De-Emphase angewandt, so dass die Sprache sehr natürlich und »wie aus dem Nebenzimmer« klingt, obwohl der Teilnehmer vom anderen Ende des Globus spricht.

Die PCM wurde bereits im Jahre 1939 von Reeves erfunden und patentiert. Damals fehlten die technischen Möglichkeiten zur Verwirklichung. Heute, im Zeitalter der Integrierten Digitalen Bausteine ist sie wirtschaftlich und sinnvoll nutzbar. Digitaltechnik ist nun billiger als Analogtechnik geworden. Das ist ein weiterer wichtiger Grund für den Siegeszug der digitalen Informationsübertragung.

Mathematisch ist beweisbar, dass beide digitalen Modulationen das ursprüngliche Analogsignal eindeutig und fehlerfrei abbilden können, abgesehen von dem durch die Quantisierungsstufen der Amplitude entstehenden Quantisierungsgeräusch.

Bezogen auf eine Bandbreite von 3,4 kHz pro analogem Sprachkanal sind die Ansprüche der digitalen Sprachkanäle an die Bandbreite sehr viel größer. Rechnet man mit 1,5 Bit pro Hertz, so kommt die Delta-Modulation auf rund 25 kHz und die PCM auf rund 100 kHz Bandbreite. Somit wird eine Datenreduktion nötig.

Datenreduktion

Mit der Datenreduktion meint man die Anwendung von Verfahren, die zweckangepasst die Datenmenge verringern, ohne den Informationsinhalt merkbar zu verschlechtern.

Dazu ein Beispiel: Eine DIN-A4-Seite von 210 mm x 297 mm wird mit 600 Bildpunkten pro Zoll (Pixel) abgetastet. Das sind dann 35.925.120 Bild-

```
ans=x;
if (x > y) {
    temp=y/x;
    ans=x*sqrt(1.0+temp*temp);
} else {
    temp=x/y;
    ans=y*sqrt(1.0+temp*temp);
}
return ans;
}

fcomplex Csqrt(fcomplex z)
{
    float w;
    if ((z.r == 0.0) && (z.i == 0.0)) {
        c.r=0.0;
        c.i=0.0;
    } else {
        w = sqrt((sqrt(z.r*z.r + z.i*z.i) + z.r)/2.0);
        if (z.r >= 0.0) {
            c.r=w;
            c.i=z.i/(2.0*w);
        } else {
            c.i=(z.i >= 0) ?
            c.r=z.i/(2.0*c.i);
        }
    }
}
```

punkte. Jeder Punkt hat 24 Bit Farbtiefe. Das ergibt 862,2 MBit Informationsmenge (im Bitmap-Format .bmp). Ist die Seite unbedruckt und leer, so könnte man doch stattdessen nur »Seite leer« oder »alle Punkte weiß« senden. Das wäre weniger als 1 kBit, und der Datenreduktionsfaktor läge ungefähr bei 1 : 1 Mio.

In der Realität fällt der Faktor kleiner aus, aber dennoch lohnt sich die Reduktion. Sie kann entweder zu Verringerung der Bandbreite oder zur Verkürzung der Sendezeit verwendet werden. Mit dieser Aufgabe sind internationale Forschungsinstitute und übernationale Expertengruppen wie z. B. die »Joint Picture Expert Group JPEG« betraut und haben bereits gute Kompressionsverfahren entwickelt wie JPEG-2 oder JPEG-4.

An der Datenreduktion von (auch bewegten) Bildern arbeitet die »Moving Picture Expert Group MPEG«. Ihre Standards erfassen nicht nur Video-Informationen, sondern auch die zugehörigen Audio-Informationen. Ihre Standards sind Grundlage für das digitale Fernsehen (Digital Video Broadcast DVB) und für DVD.

Selbst auf dem PC und im Internet sind die komprimierten Datenformate weit verbreitet. Solche Verfahren ermöglichen z. B. Videokonferenzen über ISDN-Telefonleitung oder das Internetsurfen mit dem Handy. Übrigens war der historische Vorläufer dieser Datenreduktion die »Faksimile-Übertragung« (Telefax) über Telefonleitung.

Datenreduktion ist also eine ganz entscheidende Maßnahme zur Optimierung der Funkübertragung. Ohne Datenreduktion hätte sich die digitale Informationsübertragung nicht so erfolgreich durchgesetzt, und es gäbe sehr viel mehr Streitigkeiten um die Frequenznutzung.

Redundanz und Fehlersicherung

Redundanz heißt wörtlich Überfluss. Nahezu jede Information enthält Redundanz. Das erkennt

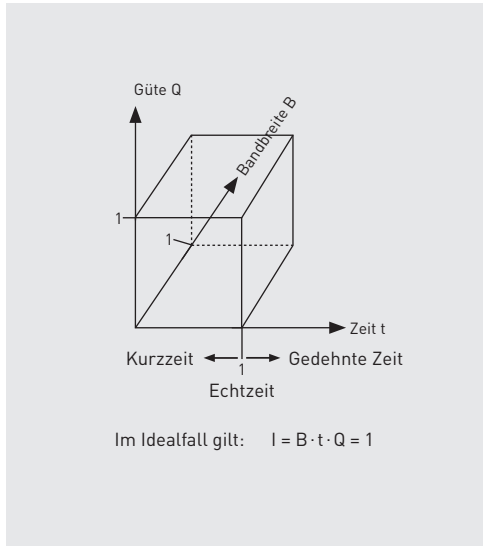
man z. B. daran, wenn man bei einem gedruckten Wort das obere oder untere Drittel abdeckt: Wenn man das Wort dann noch lesen kann, ist der abgedeckte Teil redundant.

In einem weiteren Sinn bezeichnet man mit Redundanz diejenigen Maßnahmen, die von einer Informationsmenge die überflüssigen Anteile entfernen, bis nur noch die unverzichtbare Datenmenge für die Übertragung zur Verfügung steht. Der frei gewordene Datenraum kann dann mit klug gewählten Kontrolldaten so ausgefüllt werden, dass beim Empfänger eintreffende Bitfehler erkannt bzw. korrigiert werden können.

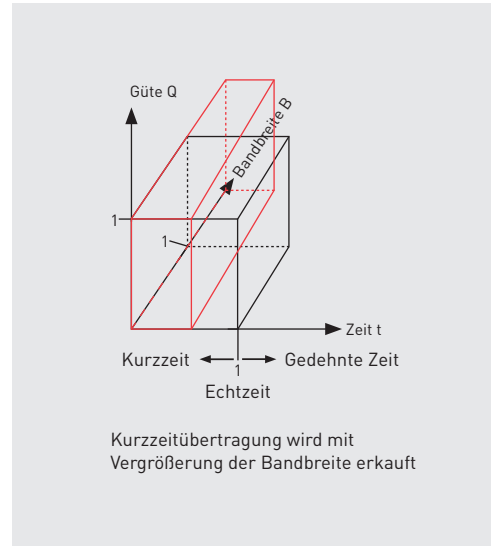
Dazu gibt es prinzipiell zwei Verfahren. Beim ersten und älteren Verfahren werden aufgrund der mitgesendeten Prüfbits (Parity Bit) vom Empfänger Fehler erkannt und automatisch eine Wiederholung des fehlerhaften Datenwortes angefordert, das dann sofort nachgereicht wird. Dieses Verfahren heißt »Automated Request« ARQ und ist in zweiseitig gerichteten Verbindungen (Duplex) das am häufigsten verwendete Verfahren.

Das zweite Fehlersicherungsverfahren ist die Vorwärtskorrektur (englisch »Forward Error Correction« FEC). Bei diesem Verfahren werden der Nutzinformation so viel Zusatzbits mitgegeben, dass eine Korrektur der häufigsten Fehler beim Empfänger vorgenommen werden kann. Es bleibt eine Restfehlermenge. Dieses Verfahren wird in einseitig gerichteten Funkverbindungen (Simplex) häufig eingesetzt, wenn die Gegenstelle nicht antworten kann oder darf.

Es gibt für beide Verfahren eine große Anzahl von Varianten, die an die jeweils typischen Übertragungseigenschaften und Fehlerhäufigkeiten des Funkkanals angepasst sind und zum Teil erhebliche Zusatzdatenmengen erzeugen können. Für Fehlersicherung »bezahlt« man somit entweder mit zusätzlicher Bandbreite oder mit zusätzlicher Übertragungszeit.



Das Übertragungstheorem, Bild 1



Das Übertragungstheorem, Bild 2

Das Übertragungstheorem

Bei der Echtzeit- oder Online-Übertragung werden die Daten verzugslos gesendet, so dass die Datenrate der Informationsquelle zugleich die Übertragungsbandbreite bestimmt.

Steht der Funkkanal aber immer nur kurzzeitig zur Verfügung (nur wenige ms bei Meteorscatter), dann müssen die Daten zwischengespeichert werden, um mit höherer Datenrate bzw. Bandbreite in kürzerer Zeit gesendet zu werden (Offline-Übertragung, siehe Bild 2).

Neben dieser Kurzzeit-Übertragung gibt es auch eine zeitgedehnte Übertragung, bei der die Zeit größer, aber dafür die benötigte Bandbreite kleiner ist (ebenfalls Offline-Übertragung). Das kommt vor, z. B. bei Funkverbindungen von Forschungssatelliten zur Erde, die wegen der riesigen Entfernung und der geringen Sendeleistung mit niedrigen Bandbreiten arbeiten müssen, damit auf der Erde die spektrale Leistungsdichte gerade noch zum Empfang der Daten ausreicht.

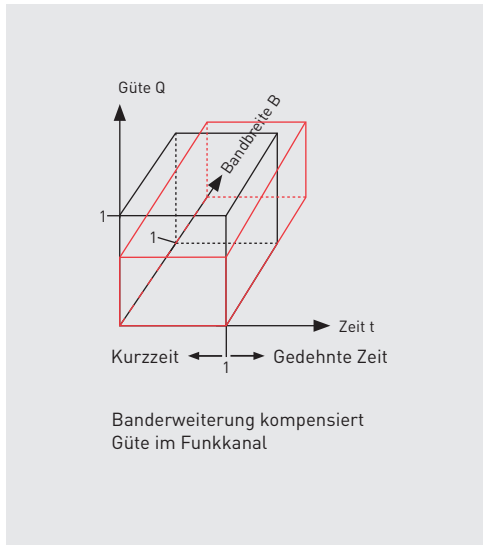
Die Übertragungszeit und die Übertragungsbandbreite sind die beiden Freiheitsgrade, die zur Lösung eines Übertragungsproblems gestaltet werden können.

Eine vorgegebene Datenmenge I soll über einen Funkkanal mit der Bandbreite B in der Zeit t fehlerfrei, also mit der Güte $Q = 1$, übertragen werden.

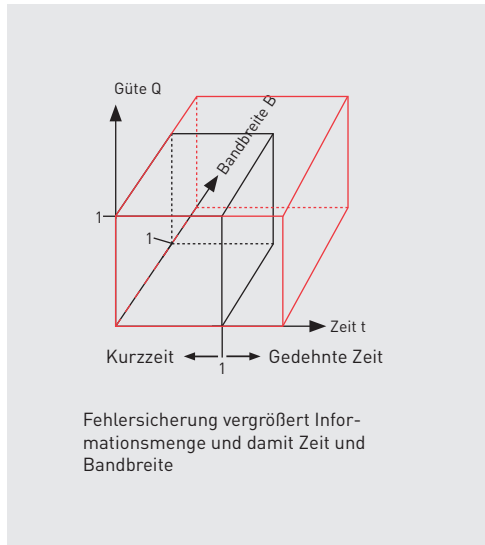
Die Zeit-Bandbreiten-Beziehung ist das Zeitgesetz der elektrischen Nachrichtentechnik nach K. Küpfmüller. Es besagt, dass das Produkt aus der Übertragungszeit t einer Nachricht und der benötigten Bandbreite B für jeden Übertragungskanal eine Konstante K ist.

$$K = B \cdot t$$

Daraus folgt, dass beide gegenseitig austauschbar sind, solange K konstant bleibt. Im idealisierten Fall ist die Konstante gleich der Informationsmenge I , also $K = B \cdot t = I$.



Das Übertragungstheorem, Bild 3



Das Übertragungstheorem, Bild 4

Wenn die vorgegebene Datenmenge I zum Schutz vor natürlichen (Fehlerrate im Funkkanal) oder vor willkürlichen Störungen (ECM) vergrößert werden muss, ergibt sich ein zweites Gesetz. Danach sind die Bandbreite und der Störabstand des vorgegebenen Übertragungskanals gegeneinander austauschbar. Das Produkt aus Bandbreite (bzw. Zeit) und Störabstand (Gütefaktor Q) ist somit eine Konstante, die zudem vom Ausmaß der Störung abhängt. Mit anderen Worten: Störschutz kostet Zeit oder Bandbreite.

Daraus ergibt sich ein zusammenfassendes Gesetz, wonach das Produkt aus Bandbreite B , Zeit t und Güte Q eine Konstante K_q ergibt, und alle drei Dimensionen dieses Würfels gegeneinander austauschbar sind.

$$K_q = Q \cdot B \cdot t$$

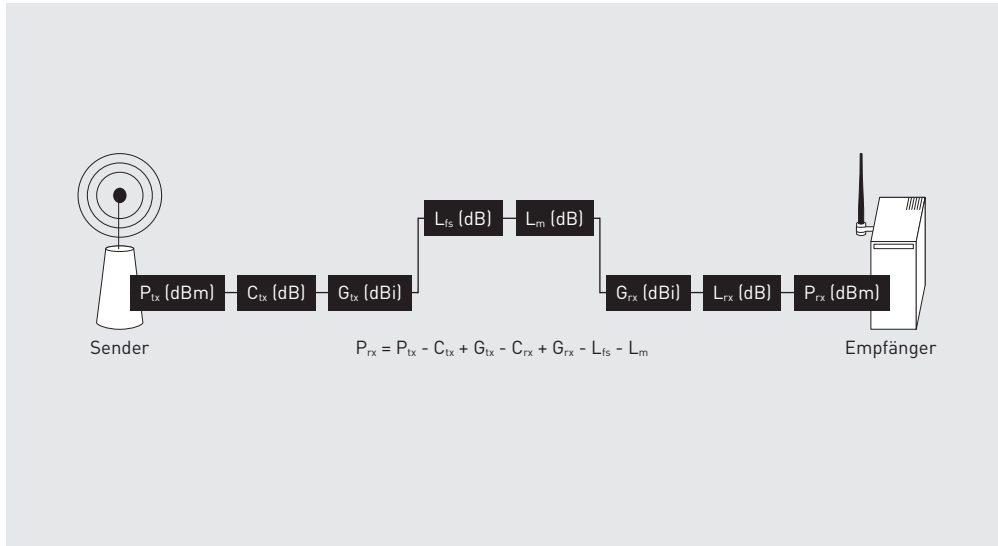
Dieses Gesetz ist das Übertragungstheorem. Es lässt sich anschaulich darstellen als Quader mit den Dimensionen Q , B und t .

Im optimalen und ungestörten Fall hat der Quader mit der Güte Dimension $Q = 1$ den Informationsinhalt I , also $K_q = Q \cdot B \cdot t = I$ (Bild 1). Im gestörten Fall vergrößert sich das Volumen I , z. B. durch zusätzliche Bits mit der Folge, dass nun zur Übertragung entweder mehr Zeit oder mehr Bandbreite benötigt wird. Über die Schutzmaßnahmen gegen ECM durch Bandbreitenspreizung wird weiter unten eingegangen.

Kanalgewinn (Linkbudget)

Schon aus den vorhergehenden Abschnitten wurde deutlich, dass die abgestrahlte Sendeleistung, Gewinn und Richtwirkung der Sendeanenne, die Freifeldämpfung, der Gewinn der Empfangsantenne und die Empfängerempfindlichkeit einen maßgeblichen Einfluss auf die Übertragungsleistung haben.

Hilfreich ist die Betrachtung der gesamten Wirkkette inklusive der vorangestellten Eigenschaften sowie der Beschaltung der Antennentechnik. Die Berücksichtigung aller Komponenten und Ein-



Der Kanalgewinn (Link-Budget) beinhaltet die gesamte Wirkkette.

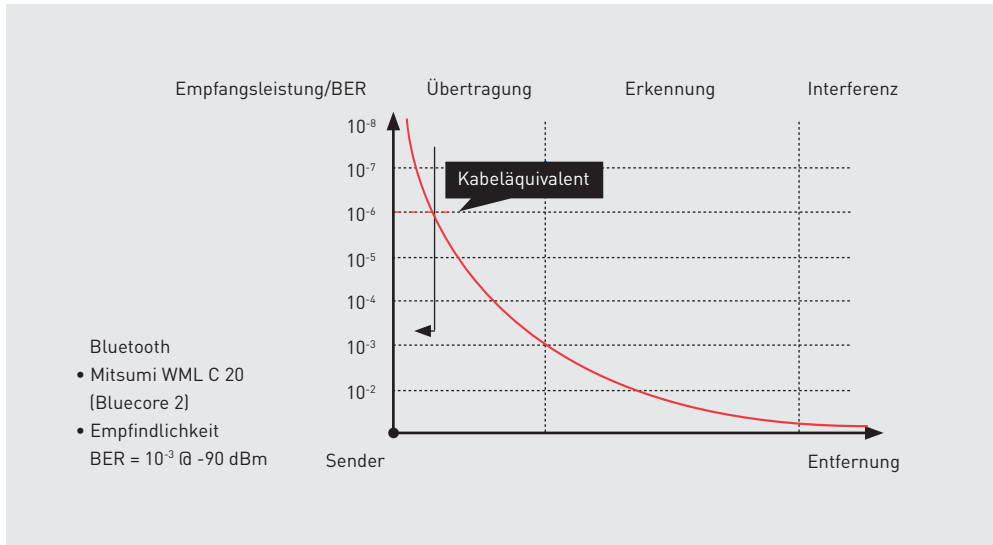
flussgrößen macht den so genannten Kanalgewinn (Linkbudget) aus.

Die Freifelddämpfung ist hierzu bereits beschrieben worden. Doch diese alleine zu betrachten ist prinzipiell zu kurz gegriffen. Betrachtet man den Sender, so spricht man häufig von ERP (Emitted Radio Power) als der abgestrahlten Sendeleistung. Sie setzt sich zusammen aus der Sendeleistung P_{Tx} , der Kabel- bzw. Kopplungsdämpfung C_{Tx} und dem Antennengewinn G_{Tx} . Die Sendeleistung ist damit nur eine von mehreren Einflussgrößen. Weitere wichtige Parameter, die zusammen C_{Tx} ausmachen, sind das Hardwaredesign und die Antennenanbindung. Auch die Antenne hat einen nicht zu unterschätzenden Einfluss auf das Übertragungsverhalten.

Vergleichbares gilt für den Empfänger. Seine Hardware hat mit Antenne, deren Anbindung und natürlich der Empfängerempfindlichkeit maßgeblichen Einfluss auf die Empfangsleistung.

Ein Blick auf kommerziell verfügbare Consumer-Geräte wie z. B. WLAN- oder Bluetooth-USB-Sticks zeigt eine Streuung von fast 20 dB trotz identischer Funk-Chipsätze. Diese Unterschiede erklären sich allein aus einem mehr oder weniger guten Hardwaredesign und der Auswahl einer mehr oder weniger hochwertigen Antenne. Geht man von einer Halbierung der Reichweite bei einer Dämpfung von 6 dB aus, bedeutet das eine Reichweitenreduktion auf gerade einmal 10 %. Die Reichweite beträgt also beispielsweise nur noch 10 statt der gewünschten 100 Meter. In der Praxis sind solche Streuungen und Einschränkungen durchaus zu finden.

Zusammenfassend kann man feststellen, dass es bei Funksystemen auf das Linkbudget ankommt – und hierzu zählt die gesamte beschriebene Wirkkette. In industriellen Funksystemen wird daher besonders viel Wert darauf gelegt, eine optimale Anpassung des Hardwaredesigns vorzunehmen, um alle Möglichkeiten zu nutzen, die in einem technischen System verborgen ist. Dies ist ein



Zusammenhang zwischen Empfangsleistung und Abstand

Grund dafür, dass industrielle Funkssysteme häufig Consumer-Markt-Produkten deutlich überlegen sind, obwohl identische Receiver-Bausteine zum Einsatz kommen.

Bitfehlerrate und Empfindlichkeit

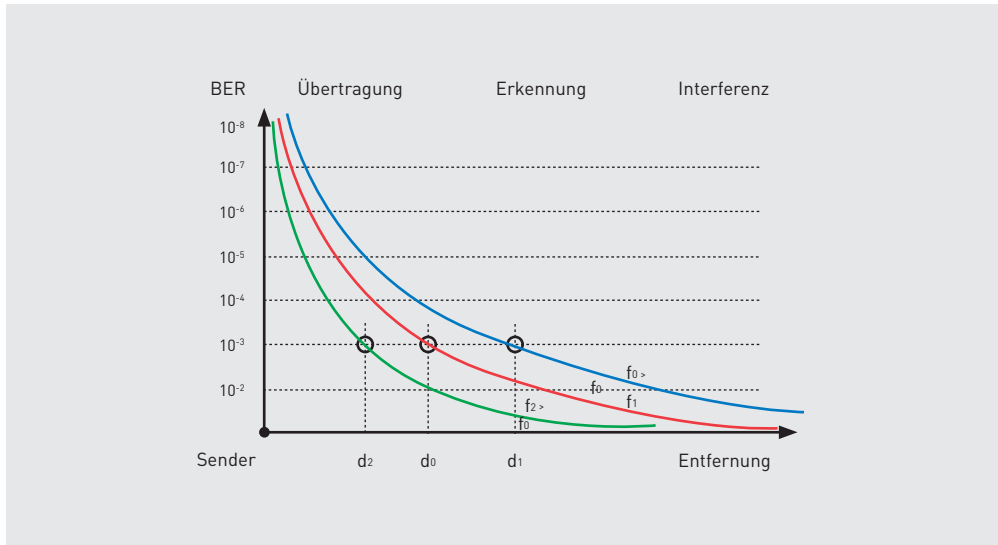
In der Regel wird das Signal/Rausch-Verhältnis nach dem Nyquist-Kriterium als Grenzparameter für die Übertragung von Systemen angegeben. Viel griffiger ist jedoch die Betrachtung der Bitfehlerrate (BER - Bit Error Rate) bei Funksystemen.

Man kann nachweisen, dass die BER unter gleichen Kodierungsbedingungen umgekehrt proportional zu der Empfangsleistung ist. Dabei werden auch die Empfindlichkeiten von Funkempfängern bei einer BER bzw. PLR (Packet Loss Rate) angegeben. In dem unten aufgeführten Beispiel für ein Bluetooth-Modul (Mitsumi WML C20) ergibt sich beispielsweise eine Empfindlichkeit von -90 dBm bei einer Bitfehlerrate von 10⁻³.

Eine Bitfehlerrate von 10⁻³ bedeutet, dass jedes 1000-ste Bit nicht in der gewünschten Form ankommt. Die Grenze BER 10⁻³ beschreibt aber auch den Grenzbereich vom Übertragungs- zum Erkennungsbereich. Bei einer nicht mehr messbaren Kommunikation trägt ein Funksystem nur noch zum Störteppich und damit zur Interferenz bei.

Vergleicht man diese Werte mit einem »normalen« Kabel, dann hat dieses eine BER von ca. 10⁻⁵, ist also zwei Größenordnungen besser als ein Funksystem im Grenzbereich. Sind Sender und Empfänger nur nah genug zusammen, ist damit auch bei Funk eine zum Kabel vergleichbare Zuverlässigkeit zu erreichen.

Betrachtet man die Herleitung der Freifelddämpfung noch einmal ganz genau, dann stellt man neben der quadratischen Abhängigkeit der Entfernung noch eine quadratische Abhängigkeit der Frequenz fest. Das bedeutet, dass die Freifelddämpfung bei niedrigen Frequenzen viel kleiner ist als bei hohen Frequenzen.



Zusammenhang zwischen Empfangsleistung und Abstand bei verschiedenen Frequenzen

Bei identischer Sendeleistung und Empfängerempfindlichkeit kann man also davon ausgehen, dass Systeme mit einer kleineren Frequenz eine deutlich höhere Reichweite haben. Oder man kann bei niedrigen Frequenzen mit viel geringeren Sendeleistungen identische Reichweiten erhalten – was aus der Low-Power-Sicht entscheidende Vorteile hat.

Andererseits ermöglichen hohe Frequenzen den Bau von Antennen mit hohem Antennengewinn bei noch vernünftigen Abmessungen. Das ist die Voraussetzung für Radarsysteme und für Richtfunksysteme mit großen Reichweiten bis hin zur Satellitenkommunikation.

// Funk in der industriellen Automation

07

Funktechnologien für die industrielle Automation

Motive für den Einsatz von Funk in der Automation

Entscheidungsparameter für die Auswahl von Wireless-Technologien

Reichweite und Mobilität

// Funktechnologien für die industrielle Automation

Neben den allgemeinen funktechnischen Herausforderungen stellt sich die Frage, welche Funktechnologie für die industrielle Automation geeignet ist. Diese ist nicht so einfach und keineswegs pauschal zu beantworten. Viele unterschiedliche Funktechnologien haben ihren speziellen Vorteil. Was letztendlich für die Lösung des individuellen Problems relevant ist, kann nur eine differenzierte Betrachtung der Anforderungen zeigen.

Zweifelsfrei ist der Einsatz von Funktechnologie immer dann interessant, wenn durch Mobilität Kosten reduziert werden können – beispielsweise durch verkürzte Inbetriebnahmezeiten, schnellere Servicefähigkeit, kürzere Installationszeiten oder einen verbesserten Bedienkomfort. Ein Einsatz in sicherheitsrelevanten Anwendungen mit alleiniger Funkanbindung, also der kabellose, energieautarke, batterie-lose »Not-Aus-Schalter«, ist jedoch nur mit hohem Aufwand zu erreichen.

Eine häufig geführte Diskussion in diesem Zusammenhang ist die einfache Erweiterung der bisherigen Ethernetnetzwerke durch WLAN nach 802.11 a, b, g oder zukünftige Technologien. Dies ist eine mögliche Erweiterung der klassischen Ethernet-Technik, deckt aber nur einen Aspekt der kabellosen Freiheit ab, der die Bereiche MES (Manufacturing Execution Systems) und ERP (Enterprise Resource Planning) betrifft.

Eine wichtige Rolle für die Automatisierungstechnik spielt die Sensor-Aktor-Ebene, die im Wesentlichen für die Echtzeitbearbeitung zuständig ist. Hier muss der Einsatz von kabelloser Technik sehr behutsam und verantwortungsvoll geplant und umgesetzt werden. Es wird sofort ersichtlich, ohne detailliert auf die Technologie einzugehen, dass der Einsatz von Funktechnik vielschichtig ist. Fasst man die groben Anforderungen zusammen,

so kann man unterschiedliche Anwendungsbereiche für kabellose Geräte identifizieren.

Motive für den Einsatz von Funk in der Automation

Schnellere Installation

Installation betrifft den Anschluss von Sensoren und Aktoren bzw. feldnahe Bediengeräte. Bewegliche oder mobile Geräte müssen in der Regel über schleppkettentaugliche Kabel und Steckverbindungen installiert werden. Bei schnellen oder örtlich flexiblen Geräten ist dies häufig problematisch. Darüber hinaus haben Displays oder Bedienterminals einen häufig wechselnden Arbeitsplatz, so dass hier die »Kabelfreiheit« eine wichtige Rolle spielt.

Einfache Inbetriebnahme

Technische Geräte sind vielfach mit Service-schnittstellen versehen, die eine komfortable Inbetriebnahme ermöglichen. Leider sind die elektrischen und logischen Spezifikationen so vielfältig wie die am Markt anzutreffenden Geräte. Durch den Einsatz mobiler Kommunikation mit einer einheitlichen Schnittstelle lassen sich Inbetriebnahmezeiten deutlich verkürzen. Darüber hinaus können Diagnose- und Überwachungsgeräte abgesetzt von den Maschinen betrieben werden.

Prompter Service

Im Fehlerfall können Geräte über kabellose Verbindungen sofort Interventionskräfte oder sonstiges Servicepersonal alarmieren. Über eine kabelfreie Serviceschnittstelle ist das Servicepersonal in der Lage, an Ort und Stelle das Problem zu analysieren und ggf. eine Verbindung zu einem Service-Desktop oder zur Ersatzteilversorgung herzustellen.

Mobile Datenerfassung

Ein wichtiger Punkt für den Einsatz kabelloser Endgeräte ist die mobile Datenerfassung. In allen

Bereichen der Logistik, aber auch in der Produktion und bei Servicedienstleistern ist der mobile kabellose Datenaustausch von besonderer Bedeutung. Nur so ist eine integrierte umfassende und papierlose Datenverarbeitung möglich, bei der das aufwändige und fehlerträchtige Übertragen von Papier in den zentralen Datenbestand entfällt. Hier sei nur auf die Ortsbestimmung von Waren in der logistischen Kette mittels RFID (Radio Frequency Identification) verwiesen.

Durchgängige Fertigungs- und Produktionssteuerung

Heute werden auch flexible Produktions- und Fertigungsanlagen hart verdrahtet. Eine Umrüstung auf neue Anforderungen zieht in der Regel teure Umrüstarbeiten nach sich. Die Aufweichung der starren Strukturen durch eine starke Modularisierung und ein Datenaustausch über kabellose Verbindungen ermöglicht eine deutliche Vereinfachung der Kommunikationsstruktur und eine flexible Anlagengestaltung.

// Entscheidungsparameter für die Auswahl von Wireless-Technologien

In der Regel wünscht man sich eine universelle, immer einsetzbare Funktechnik. Dieser Wunsch ist jedoch nicht erfüllbar, denn zu unterschiedlich sind die Anforderungen an die Technologie und die Übertragungsleistung. Wer große Reichweiten mit hohen Datenraten wünscht, erfordert systembedingt große Sendeleistungen. Bei niedrigen Frequenzen fehlt die Bandbreite, bei hohen Frequenzen hat man mehr Bandbreite zur Verfügung, aber durch die Freifeldämpfung wird auch mehr Sendeleistung erforderlich. Low-Power scheidet dann aus.

Eine Low-Power-Funktechnik mit einer hohen Batteriestandzeit wird in der Regel nur in einem Sub-GHz-Bereich angesiedelt sein, da hier die Ausbreitungsbedingungen günstiger sind. Ebenfalls darf die Kommunikation nur sporadisch er-

folgen, da sonst die Batterie zu schnell ausgetauscht werden müsste. Ergo ist in diesem Fall ein hohes Datenvolumen nicht möglich.

Die Entscheidung für oder gegen eine Technologie muss also wohl überlegt sein. Es hat sich gezeigt, dass eine differenzierte Betrachtung einiger Randbedingungen eine Priorisierung der Anforderungen deutlich vereinfacht:

Frequenzband

Die Frage nach dem Frequenzband weist schon in eine wichtige Richtung. Gibt es Anforderungen an eine weltweite Verfügbarkeit? Sind in dem Anwendungsgebiet gewisse Frequenzen vorgeschrieben oder verboten? Oder gibt es aufgrund der Ausbreitungseigenschaften die Notwendigkeit, ein bestimmtes Frequenzband zu nutzen?

Modulation

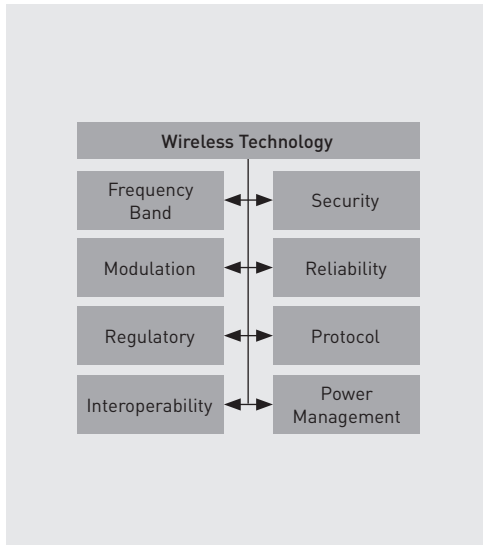
Die verschiedenen Modulationsverfahren sind unterschiedlich robust gegenüber Störungen und Interferenzen. In der Regel ergibt sich aus den technologischen Anforderungen die Auswahl einer Modulation, sofern die gewählte Technologie diesen Freiheitsgrad zulässt.

Regulatorische Bedingungen

Die regulatorischen Bedingungen sind ein sehr wichtiges Entscheidungskriterium. Wie erläutert, ist Funk nationales Recht. Hier geht es um eine differenzierte Betrachtung, welche Randbedingung für welches Einsatzfeld in welchem Bereich eingehalten werden muss. Darüber hinaus ist zu klären, welcher Aufwand bei einer ggfs. notwendigen Zulassung betrieben werden muss.

Interoperabilität

Ist eine Kopplung zu beispielsweise Konsumgeräten notwendig oder gewünscht, sollte man sich Gedanken dazu machen, wie die Interoperabilität sichergestellt werden kann. Häufig sind umfangreiche Interoperabilitätstests notwendig, um eine hinreichende Qualität zu erhalten.



Entscheidungsfelder zur Auswahl einer Funktechnologie

Security (Datensicherheit)

Security ist ein immer wichtiger werdendes Thema in der Funktechnik. Die Verschlüsselung oder Authentifizierung von Kommunikationsbeziehungen ist eine große Herausforderung. Teilweise wird eine leistungsfähige Kryptographie schon auf Chipebene angeboten, in anderen Fällen ist eine entsprechende Software notwendig. Hier muss man sich über die notwendigen Sicherheitsmechanismen im Klaren sein.

Reliability (Zuverlässigkeit)

Unter Zuverlässigkeit versteht man, dass eine Datenkommunikation unter allen Umständen erfolgreich abgewickelt wird. Häufig kommen noch zeitliche Anforderungen hinzu, d. h. eine Kommunikation muss innerhalb einer Zeit erfolgreich abgeschlossen sein. Je kürzer diese Zeitspanne ist, desto komplizierter und aufwändiger wird es.

Protokolle

Wird eine Funktechnologie in ein bestehendes Systemumfeld integriert, ist es häufig notwendig,

standardisierte Protokolle zu bearbeiten. Hier müssen die Randbedingungen und die Kommunikationsbeziehungen bekannt sein, nicht zuletzt weil viele Standardprotokolle wie z. B. TCP eine nicht zu unterschätzende Rechenleistung vom Prozessor verlangen.

Power Management

Low Power wird immer wichtiger. Es ist außerordentlich wichtig, sich zu fragen, welche Teilnehmer in einem Funknetzwerk energiesparend betrieben werden können.

Überblick über relevante Leistungsparameter

Bei der Auswahl sollte auf jeden Fall auch das Anwendungsfeld sehr genau unter dem Aspekt betrachtet werden, welche Leistungsparameter erreicht werden müssen. Gerade in der industriellen Kommunikation haben sich hierzu fünf Parameter als besonders geeignet herausgestellt:

Realtime Cycle, Echtzeitzyklus

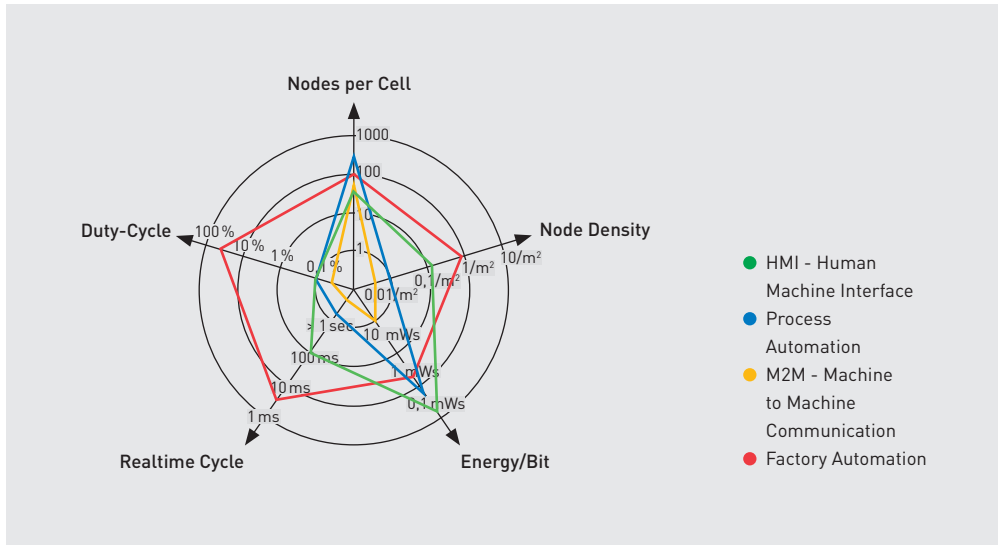
definiert die Zykluszeit, in der ein System abgetastet werden muss. Die Zeiten variieren von wenigen Millisekunden für die Fertigungsautomation bis hin zu etlichen Sekunden in der Prozessindustrie.

Duty-Cycle, Tastgrad

bezeichnet die Nutzungsdauer einer Periode für z. B. eine Kommunikation. Der Tastgrad ist dimensionslos und wird von 0 ... 100 % angegeben. Ein Duty-Cycle von 20 % bedeutet, dass 20 % der Intervallzeit genutzt wird. Bei einem Duty-Cycle von 100 % wird das gesamte Intervall genutzt. Gerade bei schmalbandigen Systemen wie z. B. im 868 MHz-SRD-Band gibt es eine Restriktion von beispielsweise 0,1 % Tastgrad.

Nodes per Cell, Knoten pro Zelle

beschreibt die Anzahl der Kommunikationsteilnehmer innerhalb einer Kommunikationszelle. In der Fertigungsautomation sind einige 10 Knoten typisch für ein Netzsegment. Manchmal begrenzt



Jedes Funk-Anwendungsgebiet hat seine spezifischen Anforderungen.

aber auch die Technologie die Anzahl der Teilnehmer. Bluetooth beispielsweise hat eine Obergrenze von 7 aktiven Teilnehmern pro Piconet.

Node Density, Knotendichte

definiert die Anzahl von Knoten pro Fläche. In einer Kläranlage sind nur wenig Knoten erforderlich, die sind jedoch auf einer großen räumlichen Fläche verteilt. Demgegenüber können beispielsweise in einer Fertigungs- oder Roboterzelle auf kleinstem Raum sehr viele Kommunikationsteilnehmer notwendig sein.

Energy/Bit, Energie pro Bit

ist ein Maß für die Energieeffizienz einer Technologie mit einer Datenrate, kombiniert kann der Gesamtenergiebedarf pro Zeiteinheit berechnet werden, was einen Schluss auf die Energiebereitstellung schließen lässt. Funksysteme können bis hinunter zu energieautarken Systemen skaliert werden. Energieautarke Systeme beziehen ihre Energie aus der Umwelt (Energy Harvesting).

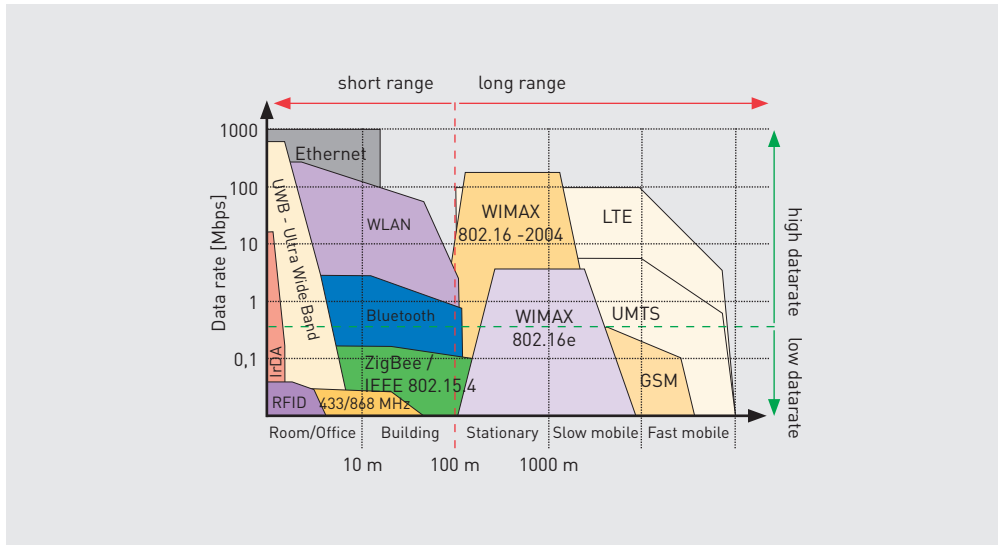
// Reichweite und Mobilität

Funk ist eng verbunden mit der Freiheit, sich frei bewegen zu können. Doch diese Freiheit ist relativ. Daher müssen die Anforderungen klar definiert werden. Wie lang soll die kabellose Leine sein, bis die Kommunikation zusammenbricht? Und wie schnell bewegt sich ein Objekt, zu dem die Funkkommunikation aufrechterhalten werden soll? Das sind entscheidende Fragen, um eine qualifizierte Technologieauswahl treffen zu können.

In der Praxis haben sich hier ganz pragmatische technologische Cluster mit zwei Parametern entwickelt. Zuerst unterscheidet man zwischen kleiner und hoher Datenrate (High/Low Datarate). Die Grenze wurde mehr oder weniger willkürlich zwischen 100 kbps und 1 Mbps gesetzt. Die Unterscheidung zwischen Long Range und Short Range wurde ebenfalls pragmatisch an der 100-Meter-Grenze gezogen.



Eine der ersten Anwendungen der EnOcean-Technologie in der Industrie: Funk-Türgriffschalter an einer Werkzeugmaschine.



Je nach Anwendungsfall sind unterschiedliche Technologien notwendig

Mit dieser Einteilung kann man die folgenden vier Bereiche differenzieren:

1. Short Range/Low Datarate
2. Short Range/High Datarate
3. Long Range/Low Datarate
4. Long Range/High Datarate

Hinzu kommen die Mobilitätsaspekte. Gerade für die Long-Range-Lösungen sollte man zumindest drei Kategorien berücksichtigen:

1. Stationary – Feste Stationen ohne Beweglichkeit, wie sie beispielsweise in Infrastrukturnetzen verwendet werden.
2. Slow Mobile / Pedestrian Mobility – Langsam bewegliche Sender/Empfänger mit typisch bis 6 km/h.
3. Fast Mobile – Übertragung auf Empfänger mit höheren Geschwindigkeiten, wobei dies Definitionssache ist: In Europa ist »fast« nahe der 300 km/h, während in den USA schon 80 mph (miles per hour) als »fast« gelten.

// Grundlagen der Funktechnik: Technologien und Standards

08

IEEE 802.15.4

ZigBee

Wireless HART

Bluetooth

ISM Band	1	2	3	4	5
Frequenzbereich	26.957 ... 27.283 MHz	40.660 ... 40.700 MHz	433.050 ... 434.790 MHz	868 ... 870 MHz	2.400 ... 2.483 GHz
Bandbreite	326 kHz	40 kHz	1.74 MHz	2 MHz	83 MHz
Vorteile	Niedriger Stromverbrauch	Kein dauerhafter Störträger, geringer Stromverbrauch	Relativ breites Band, gute Ausbreitung, moderate Preise	Relativ breites Band, geringe Belegung, Tastzeit auf max. 10% begrenzt	Große Bandbreite, weltweite Zulassung
Nachteile	Hoher Störpegel durch CB-Funk	Zu geringe Bandbreite, Antenne zu groß	Stark belegt, Amateur-Betriebsfunk, 70 cm	Teurer als 434 MHz	Problematisch in der Ausbreitung

Frequenzbereiche und Eigenschaften im ISM-Band

Grundsätzlicher Unterschied zu nicht-industriellen Funk-Anwendungen

Seit der Entdeckung der Funktechnik wurde Funk vor allem zur Überwindung großer Entfernungen genutzt. Funk war und ist also in erster Linie »Weitverkehr«. Deshalb werden die Funkdienste mit ihren koordinierten Frequenzen vor Störern gesetzlich geschützt. In Deutschland geschieht dies durch den Funkkontroll- und Messdienst der Bundesnetzagentur.

Ganz im Gegensatz dazu stehen die industriellen Anwendungen mit ihren »Short range devices« (SRD), deren Nutzung in den vergangenen Jahren ganz erheblich zugenommen hat. Sie funkten im Kurzstreckenverkehr und verwenden dabei öffentlich zugängliche Frequenzen, die nicht gesetzlich geschützt werden. Vielmehr müssen sich die Nutzer hier dezentral selbst abstimmen und koordinieren.

Aus diesem Umstand ergibt sich eine Reihe von Maßnahmen und Spezifikationen, damit diese

SRD verträglich koexistieren (Kompatibilität) oder in lokalen Netzwerken harmonisch zusammenarbeiten können (Interoperabilität). Mit diesen Maßnahmen befasst sich das Kapitel »Koexistenz« ab Seite 139.

Aus den vorhergehenden Ausführungen wird es deutlich, dass es nicht eine einzelne Technologie geben kann, die alle Anforderungen erfüllt. Das folgende Kapitel gibt deshalb einen Überblick über relevante Technologien, um die prinzipielle Funktion, aber auch die Grenzen aufzuzeigen.

Sub-GHz-Bereich

Ist eine Funk-Kommunikation innerhalb von Gebäuden notwendig, sind Frequenzen unterhalb von 1 GHz zu empfehlen. Durch die geringere Dämpfung als beispielsweise bei 2,4 GHz ist in der Regel mit einem um 15 bis 25 dB besseren Linkbudget zu rechnen. Bei gleicher Sendeleistung sind somit wesentlich höhere Reichweiten möglich. Darüber hinaus ist mit sehr kleinen Sendeleistungen in diesem Frequenzbereich auch der

Region	Standard	Transmit Power
USA, Canada	FCC 15.231 (e) RSS-210 FCC 15.240	Field strength: 4400 $\mu\text{V/m}$ @ 3m 10 sec blink rate Field Strength: 55,000 $\mu\text{V/m}$ @ 3m (deployment restrictions apply)
Europe, Africa	ISM Band EN 300 220	Max ERP: <10 mW @ 10% or <1mW @ 100% duty cycle
China	SRR Regulation	Max ERP: 10 mW, occupied bandwidth < 400 kHz
Australia, New Zealand	AS/NZS 4268:2003	Max ERP: 15 mW

Regulatorische Bedingungen im 433 MHz-Band

Einsatz von Geräten möglich, die mit Batterie- oder Umweltenergie (Energy Harvesting) betrieben werden.

Funkanwendungen im Sub-GHz-Bereich sind populär und ungeheuer vielfältig. Eine Klassifizierung nach einem bestimmten Anwendungsgebiet ist nicht möglich. Die Geräte dienen als Funkmodem, Alarmanlage, Wetterstation oder werden für allgemeine Telemetrie-Aufgaben sowie für das Smart-Metering genutzt. Ist nur eine sporadische Datenkommunikation notwendig, können diese Geräte bei kluger Sende- und Empfangssteuerung sehr stromsparend arbeiten und eine Batterielebensdauer bis zu 5 Jahren erreichen. Dies ist ein wesentlicher Vorteil, der den Einsatz in den beschriebenen Anwendungsbereichen überhaupt erst möglich macht.

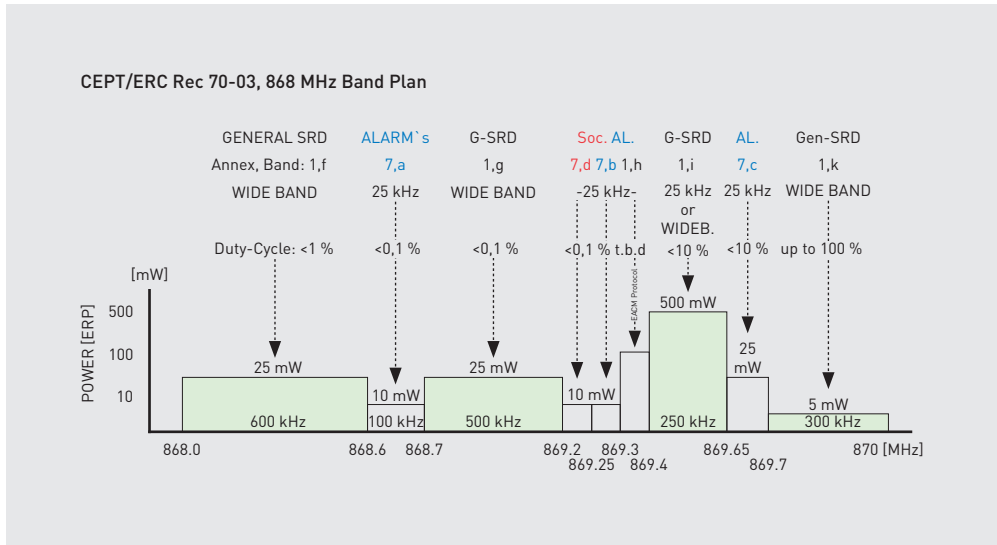
433 MHz

Das 433 MHz ISM-Band nutzt den Frequenzbereich von 433,05 ... 434,79 MHz. Es wird vorwiegend für kundenspezifische, individuelle System-

lösungen mit kurzen bis mittleren Reichweiten eingesetzt. Bei einer maximalen Sendeleistung von bis zu 10 mW ist ein Duty-Cycle von bis zu 10 % zulässig. Bei einer Sendeleistung < 1mW unterliegt der Duty-Cycle keinen Einschränkungen.

Das Frequenzband ist besonders attraktiv, da die zur Verfügung stehende Bandbreite in spektraler und zeitlicher Sicht nicht beschränkt ist. Auch die Art der Modulation ist nicht vorgeschrieben, so dass unterschiedlichste Verfahren implementiert werden dürfen. Dieser Vorteil bringt den Nachteil mit sich, dass besondere Maßnahmen zur Stör- bzw. Interferenzvermeidung getroffen werden müssen. Um eine zuverlässige Übertragung zu erreichen, muss das Störpotential genau analysiert werden, um daraufhin die Kanalkodierung anzupassen. Ist diese Herausforderung gelöst, lassen sich kostenoptimierte, energiesparende Funklösungen realisieren.

Auch in Hinblick auf Zukunftsfähigkeit erscheint das 433 MHz-Band attraktiv. Durch die stetige



Regulatorische Bedingungen für das 868 MHz-SRD-Band

weltweite Harmonisierung wird durch die IEEE angeregt, das Band auch als alternatives MAC-Layer für Wireless Personal Area Networks nach IEEE 802.15.4f zuzulassen. Entscheidende Vorteile sind der geringe Path-Lost sowie die einfache Realisierung der Funkchips.

In Europa wird das 433 MHz-Band bei technischen Anwendungen überwiegend bei schnurlosen Mikrofonen und Kopfhörern, Babyrufanlagen, Zutrittskontrollsystemen, Türöffnern, Bewegungsmeldern sowie medizinischen Systemen eingesetzt.

868 MHz

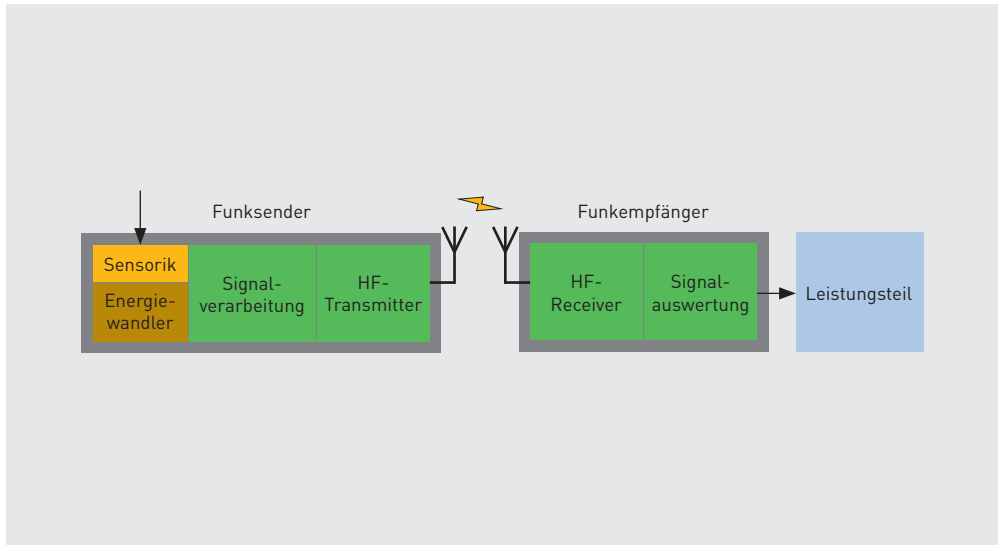
Eines der attraktivsten Frequenzbänder ist in Europa das 868 MHz-SRD-Band. Short-Range-Devices (SRD) bestimmen unseren Alltag. Eine schier unvorstellbare Anzahl von Anwendungen, angefangen beim Funkschlüssel vom Auto über den Brustgurt beim Sport bis hin zum Kopfhörer und kabellosen Alarmsensoren, zeugen von den vielfältigen Einsatzmöglichkeiten.

Im Gegensatz zum 433 MHz-Band hat man sich beim 868 MHz-Band frühzeitig über die möglichen Nutzungsszenarien Gedanken gemacht und den zur Verfügung stehenden Frequenzbereich in Subbänder unterteilt, die für spezifische Nutzungsszenarien genutzt werden dürfen. In den Bandbereichen sind die Nutzung, die Duty-Cycle und die maximale Sendeleistung genau vorge-schrieben, so dass eine weitgehend konfliktfreie Koexistenz der Geräte sicher gestellt ist.

Sendeleistungen sind zwischen 5 und 500 mW bei einem Duty-Cycle von typisch 0.1 % bis hin zu 100 % zulässig. In Verbindung mit den günstigen Ausbreitungseigenschaften lassen sich Reichweiten bis in den Kilometer-Bereich erreichen und auch innerhalb von Gebäuden ist eine gute Reichweite garantiert.

Uneinheitliche weltweite Nutzung

Als nachteilig erweist sich die nicht einheitliche weltweite Nutzung der Frequenzbänder. Das 868 MHz-Band ist für Länder der Gruppe 1 zuge-



Die EnOcean-Technologie ermöglicht batteriefreie Sensorknoten.

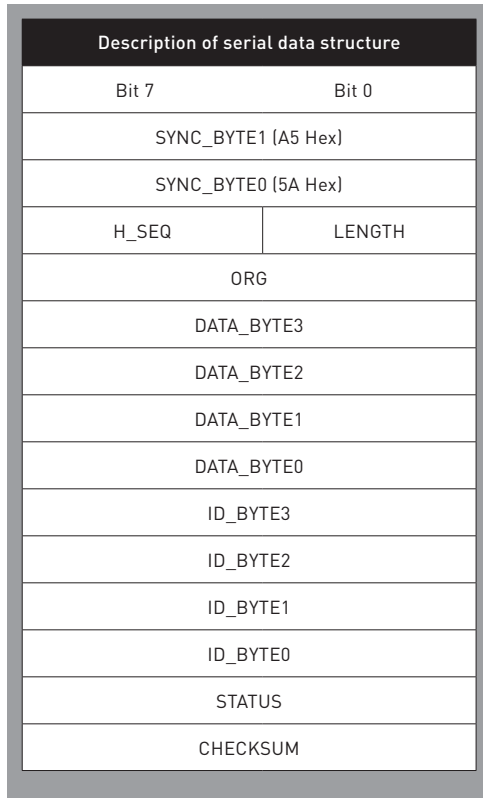
lassen. In den USA wird dieser Frequenzbereich jedoch für die Mobilfunktechnik CDMA genutzt. Als SRD-Band steht hier der Frequenzbereich von 902 ... 928 MHz zur Verfügung, der wiederum in Europa für GSM-Mobilfunk verwendet wird. Glücklicherweise sind die Frequenzbereiche jedoch so dicht beieinander, dass Dual-Mode-Geräte entwickelt werden können. Nahezu jeder 868 MHz-Funkchip-Hersteller lässt auch das 915 MHz-Band zu.

Auch im 868 MHz-Band kann die Modulation und Übertragung frei gewählt werden. Eine Vielzahl von Systemlösungen ist am Markt kostengünstig zu erhalten. Eine Sicherung der Daten gegenüber Fremdzugriff ist nicht vorgeschrieben, so dass eine Verschlüsselung oder Anwendungssicherung innerhalb der jeweiligen Protokollimplementierung realisiert werden muss. Die Datenrate von Modulen in typischen industriellen Anwendungen liegt bei 38.400 Baud. Es sind aber auch Varianten mit bis zu 115.200 Baud möglich.

Da nur das physikalische Layer und die Sicherungsschicht definiert sind, bieten die 868 MHz-ISM-Module keine standardisierte Anwendungsschnittstelle bzw. kein standardisiertes Protokoll. Auch Adhoc-Netzwerke können nicht ohne erheblichen Aufwand umgesetzt werden. In der Regel wird ein eigener Microcontroller benötigt, der für die Protokolle, Verschlüsselung und sonstigen Sicherheitsmechanismen verantwortlich ist. Die 868 MHz-SRD-Technik ist damit eine typische Technologie für die Low-Cost- und Low-End-Sensor-/Aktor-Vernetzung auf firmenspezifischem Niveau.

»Energy Harvesting«: Der EnOcean-Standard

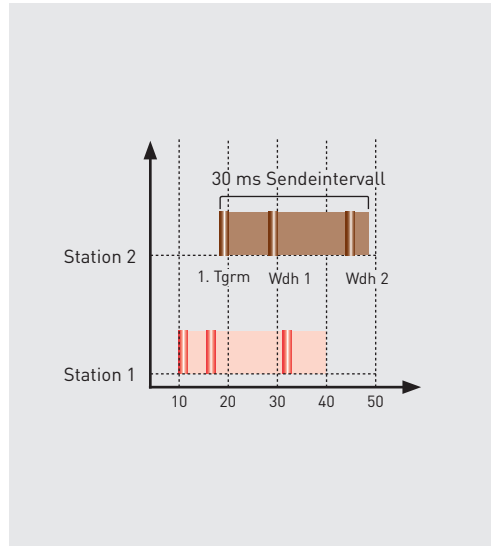
Eine besondere Bedeutung innerhalb der Sub-GHz-Funktechnik hat die Firma EnOcean mit ihrer gleichnamigen Technologie erreicht. EnOcean ist ein Spin-off-Unternehmen von Siemens, das sich 2001 mit der Idee selbstständig gemacht hat, echte Zero-Power-Funktechnologie am Markt zu etablieren.



Bei einer Datenrate von 120 kbps dauert ein Telegramm weniger als 1 Millisekunde

Diese Idee fand rasch einen Markt. Gerade in der Gebäudetechnik ist bei einer hohen Anzahl von Schaltern auch eine Batteriebensdauer von mehreren Jahren nicht mehr akzeptabel, denn der Aufwand für den Batteriewechsel wird einfach zu hoch. EnOcean verfolgt das Grundkonzept, Prozessenergie aus dem Schaltvorgang oder der Umgebung zu gewinnen (Energy Harvesting) und mit einer sehr effizienten Funktechnik die gewonnene Energie für die Übertragung zu nutzen.

Mit der Idee und ersten Implementierungen wurden in den letzten Jahren viele Technologiepreise gewonnen. Heute ist EnOcean eine etablierte Größe in der Ultra-low-Power-Funktechnologie.

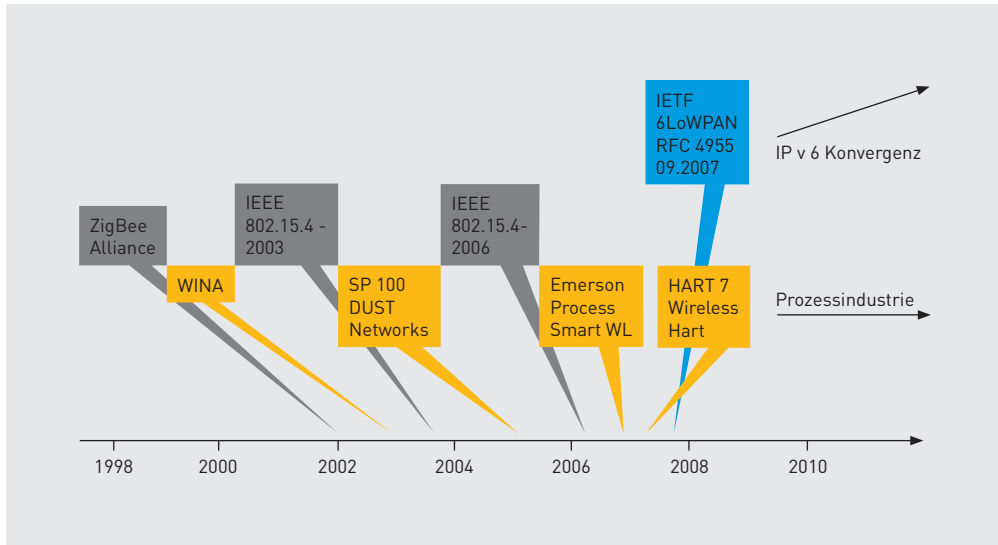


Sendeschema unidirektionaler EnOcean-Verbindungen

EnOcean nutzt für die Übertragung das 868 MHz-SRD-Band oder das 315 MHz-ISM-Band für Anwendungen außerhalb der Gruppe 1-Länder. Durch die hohe Empfängerempfindlichkeit von besser als -95 dBm, eine Sendeleistung von bis zu 10 mW (10 dBm) und eine energiesparende ASK (Amplituden Shift Keying)-Modulation wird für das Versenden eines vollständigen Funkbefehls nur etwa 50 mWs Energie benötigt. Damit sind Reichweiten von typisch 30 Meter im Gebäude und 300 Meter im Freifeld zu erreichen. Durch eine 32 Bit-ID, die Funkempfänger von ihrem Sender lernen können, ist eine eindeutige Gerätezuordnung möglich. Typischerweise werden 4 Byte-Nutzdaten übertragen. Im seriellen Modus ist eine permanente Datenverbindung mit bis zu 9,6 kbps möglich.

Man muss zwischen zwei Betriebsmodellen unterscheiden.

1. Im reinen Sensorbetrieb erfolgt eine unidirektionale Kommunikation. In der Regel wird aus einem Schaltvorgang durch ein Piezoelement



Der IEEE 802.15.4 Standard ist Basistechnologie für unterschiedliche Funknetze.

oder einen miniaturisierten Energiegenerator so viel Energie gewonnen, dass der gesamte Sendevorgang realisiert werden kann. Hierzu wird der Steuerbefehl in einem zufälligen Muster innerhalb von 30 Millisekunden dreimal versendet. Rein statistisch sollte das Signal sicher ankommen. Durch die hohe Datenrate und die kleine Datenmenge wird die Luftschnittstelle nur sehr kurz belegt, so dass die Wahrscheinlichkeit einer Kollision erfreulich gering ist. Eine Rückmeldung zum Sensor ist nicht möglich.

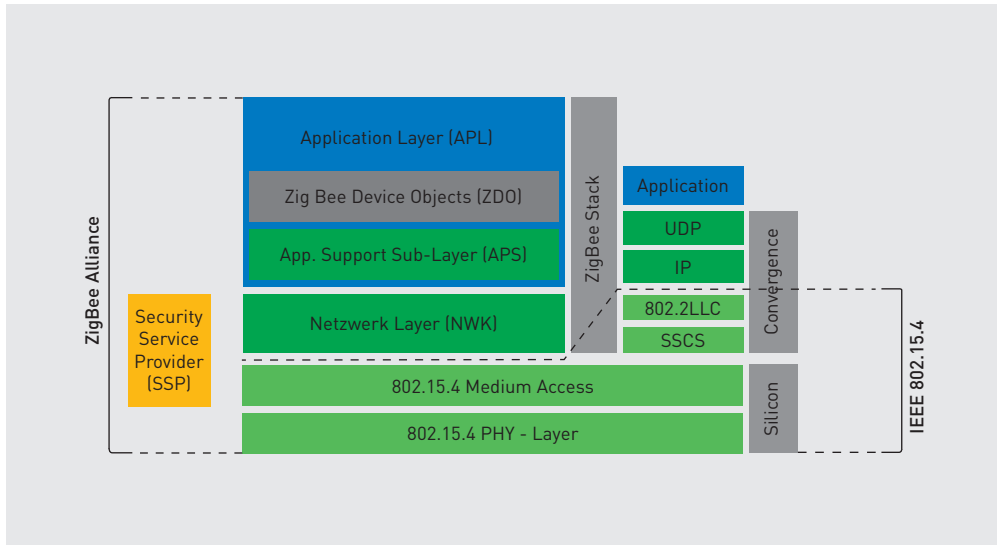
2. Im bidirektionalen Betrieb können Sender und Empfänger permanent Daten austauschen. Um hier wartungsfreie autarke Sensoren herzustellen, sind Energiewandler einzusetzen, die permanent der Umwelt Energie entziehen und in einem Zwischenspeicher puffern. Kleine Solarzellen, Schwingungswandler oder Thermo-wandler eignen sich hierzu hervorragend. Mit der Dolphin-Plattform bietet EnOcean seit Anfang 2010 auch die bidirektionale Kommunikation an.

EnOcean-Funktechnik ist aktuell die führende Technologie im Bereich Zero-Power. Mehr als sechzig Unternehmen bieten mehrere hundert zum größten Teil zueinander kompatible Sensoren an. Durch die Erweiterung auf bidirektionale Kommunikation sind nun auch neue Anwendungsfälle möglich, bei denen ein Feedback zwischen Sensor und Aktor notwendig ist, wie z. B. bei sicherheitsgerichteten Anwendungen.

// IEEE 802.15.4

Die Begriffe IEEE 802.15.4 und ZigBee werden oft synonym verwendet, was jedoch nicht richtig ist. Die IEEE-Norm beschreibt lediglich die unteren beiden Layer (PHY und MAC) im ISO-OSI-Modell für WPANs (Wireless Personal Area Networks). Die höheren Protokollschichten werden durch andere Organisationen geregelt, wie z. B. die ZigBee Alliance oder die HART-Foundation.

Die Normung der Physik und des Mac-Layers erfolgte in der WPAN Arbeitsgruppe IEEE 802.15 in



ZigBee und IEEE 802.15.4 sind nicht identisch.

der Untergruppe 4. Mit Stand Februar 2003 wurde die erste Spezifikation IEEE 802.15.4-2003 veröffentlicht. Mit der Version von 2006 wurden zusätzliche Datenraten im Sub-GHz-Band hinzugefügt.

Weitere Erweiterungen in den Arbeitsgruppen a (Zusätzliche Physical Layer wie UWB Ultra Wide Band und CSS (Chirp Spread Spectrum), c (314-316 MHz, 430-434 MHz und 779-787 MHz für China), d (950-956 MHz für Japan), e (Zusätzliche Funktionen für industrielle Anwendungen), f (Aktive RFIDs) zeugen von einer aktiven Normungstätigkeit. Die Entwicklungen sind wegweisend gerade in Hinblick auf Sensornetze (WSN – Wireless Sensor Networks).

Eine interessante Entwicklung zeigt sich durch die sehr universelle Einsetzbarkeit des IEEE 802.15.4 Basislayers. Eine Vielzahl unterschiedlicher Technologien nutzt dieses Basislayer und erweitert den Protokollstack nur auf den höheren Layern. Aktuell lassen sich zwei Trends ablesen:

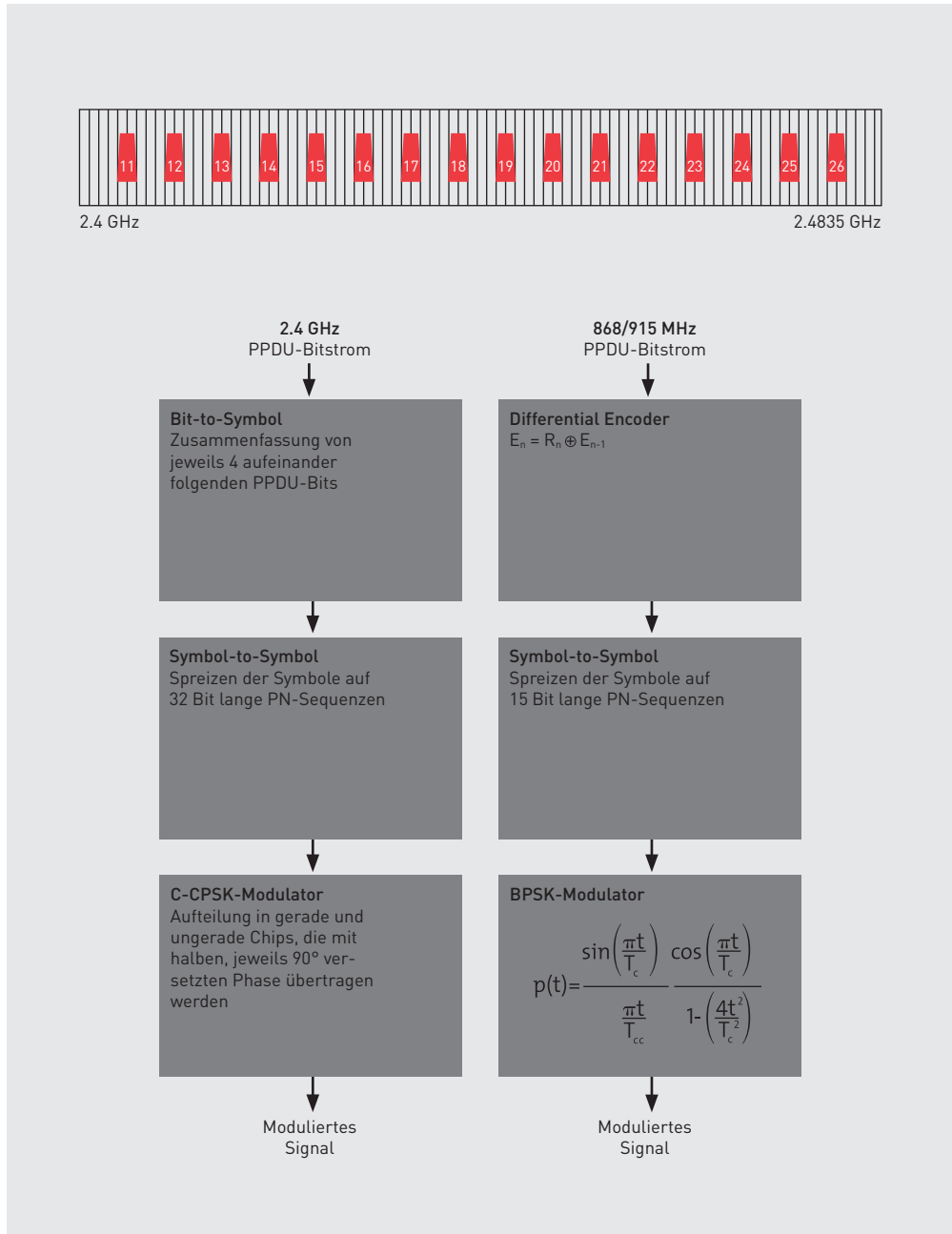
1. Für den Bereich der Prozessautomation hat sich mit Wireless HART im HART7- Standard der Einsatz eines IEEE 802.15.4 Layers auf breiter Basis etabliert.
2. Mit dem Trend zu IP-basierten Netzwerken hat der IETF-Standard 6LoWPAN eine gute Basis geschaffen für IP-basierte Sensornetzwerke.

Neben diesen beiden Trends werden in Zukunft auf dieser Basis sicherlich weitere Lösungen für unterschiedlichste Anwendungsfälle geschaffen.

Grundlagen

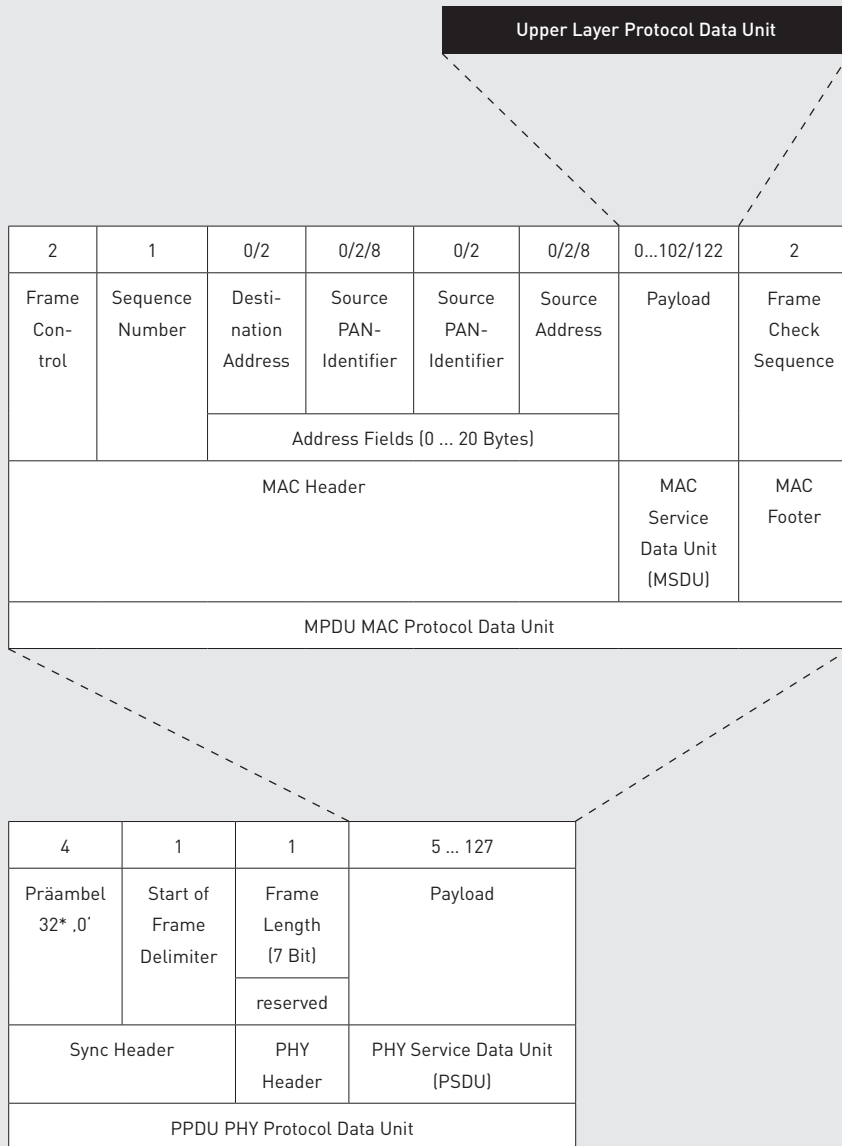
Die IEEE 802.15.4-2003 definiert eine Funkübertragung für das 2,4 GHz-ISM-Band, das europäische 868 MHz-SRD-Band und das amerikanische 915 MHz-Band.

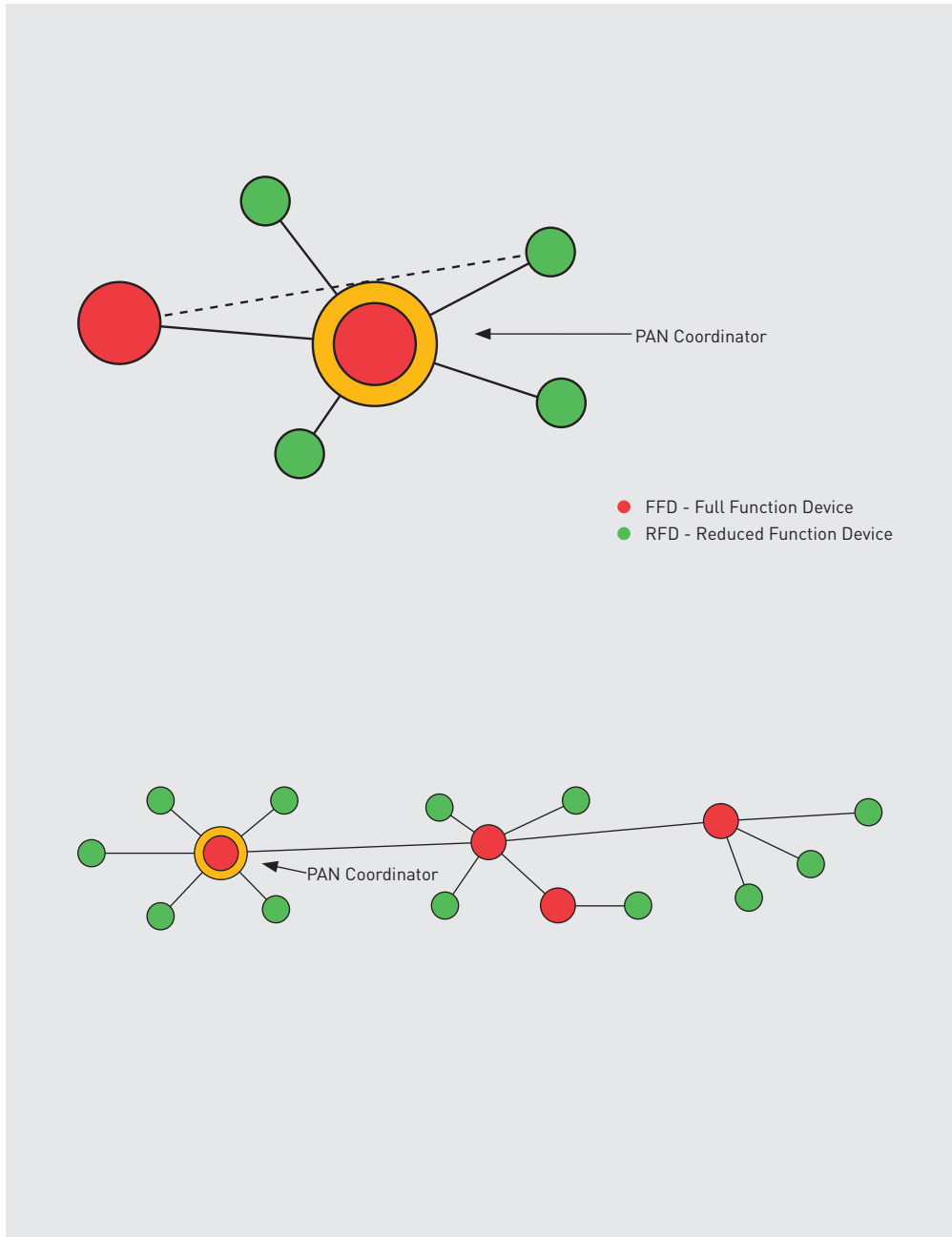
Im 2,4 GHz-Bereich stehen weltweit 16 Kanäle mit einer maximalen Bandbreite von 250 kbps zur Verfügung. Aufgrund der Beschränkungen des SRD-Bandes ist in Europa nur ein Kanal bei 868,3 MHz mit 20 kbps freigegeben, auf dem amerika-



Oben: Nutzung des 2.4 GHz-Band von IEEE 802.15

Unten: Modulationsverfahren für IEEE 802.15.4





Oben: RFDs und FFDs können ein komplexes Netzwerk aufspannen.

Unten: FFDs können in noch komplexeren Netzwerken betrieben werden.

nischen Kontinent können immerhin 10 Kanäle mit einer Datenrate von 40 kbps benutzt werden. Aktuell kristallisieren sich drei Trends heraus:

1. Der Sub-GHz-Bereich wird nach den jeweiligen nationalen Möglichkeiten in den Standard überführt, um die günstigen Ausbreitungseigenschaften zu nutzen (802.15.4 c,d)
2. Der 2,4 GHz-Bereich wird für technische Anwendungen besonders berücksichtigt und auch mit Anwendungsschnittstellen versehen.
3. Es werden alternative Physical Layer angeboten.

Innerhalb der Frequenzbänder werden unterschiedliche Modulationsverfahren verwendet, wobei immer ein DSSS (Direct Sequence Spread Spectrum) -Verfahren mit 15 bzw. 32 Bit-Spreizung zur Anwendung kommt.

Für den Kanalzugriff verwendet 802.15.4 einen CSMA-CA-Algorithmus, vergleichbar zu dem von WLAN nach IEEE 802.11. Für einen optimierten Kanalzugriff können auch so genannte Superframes verwendet werden, bei denen für zeitkritische Anwendungen Time Slots reserviert werden. Um diese Slots bekannt zu machen, setzt ein Netzwerkkoordinator (PAN-Coordinator; siehe Bild Seite 105) Beacons in bestimmten Intervallen ab, auf die sich die registrierten Stationen registrieren können. Ein Kanalwechselmodus, vergleichbar zu Bluetooth, ist nicht implementiert, kann jedoch bei Bedarf durch die Netzwerkschicht realisiert werden.

Eine Besonderheit des IEEE 802.15.4-Standards ist die Netzwerktopologie selber (siehe Bild Seite 105). Es wird eine komplexe Meshed-Star-Topologie unterstützt, die entweder Low Power oder Hochverfügbarkeit ermöglicht. Um kostengünstige Sensoren und Aktoren realisieren zu können, wird zwischen Full-Function-Devices (FFD) und Reduced-Function-Devices (RFD) unterschieden. RFDs können nur als Slave eines FFDs betrieben werden und sind nicht in der Lage, untereinander

zu kommunizieren. Hierdurch lässt sich die Komplexität deutlich reduzieren, so dass RFDs schon auf einem kleinen 8-Bit-Prozessor mit wenig Speicher lauffähig sind.

Die FFDs sind zentrale Netzknoten, die selbstständig agieren können und einen deutlich größeren Funktionsumfang beherrschen müssen.

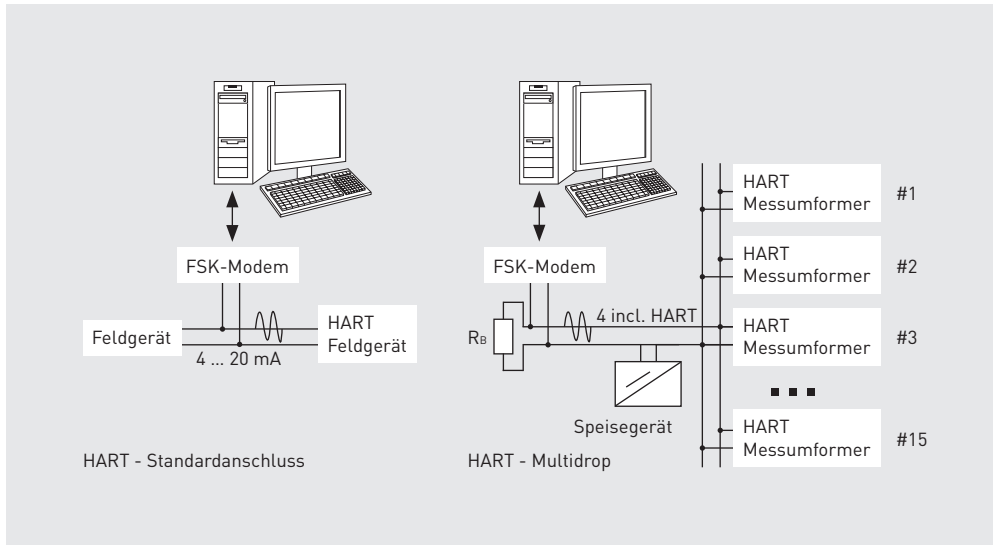
FFDs können untereinander in Verbindung treten oder zu RFDs. In einem Netzsegment muss ein FFD die Rolle des PAN-Koordinators übernehmen. Dieser Knoten ist für das Verbindungsmanagement in einer PAN-Zelle verantwortlich. Alle zur Zelle gehörigen Knoten, sowohl FFDs als auch RFDs, müssen sich bei ihm anmelden. Ein PAN-Koordinator ist auch in der Lage, den Nachrichtenverkehr zwischen zwei RFDs zu managen. Durch die Möglichkeit, FFDs untereinander zu vernetzen, kann man nahezu beliebig komplexe Netzwerkstrukturen aufbauen, wobei ein Routing von Nachrichten über Segmentgrenzen hinweg möglich ist. Man spricht hierbei auch von so genannten Mesh-Netzwerken.

Zur Adressierung der einzelnen Knoten sieht der MAC-Frame sowohl Ziel- und Quelladressen für das Teilnetzwerk (PAN-Identifizier-2-Byte) als auch für den Knoten selber vor (Address 2/8 Byte). Hierdurch können theoretisch in einer Netzwerkstruktur maximal 216 mal 264 Netzknoten erreicht werden.

// ZigBee

ZigBee setzt auf den IEEE802.15.4-Standard eine Dienstleistungsschicht auf. Schwerpunkt sind die Konfiguration und Administration von Kommunikationsknoten sowie das Routing von Nachrichten zwischen den Teilnehmern. Die Realisierung einer Anwendungsschicht wird nicht unmittelbar im ZigBee-Standard beschrieben, vielmehr erfolgt die Definition von Applikationsszenarien und Use-Cases in Profilen. Schwerpunkt ist hier-

Mandatory (Direct & Indirect Addressing Clusters)									
Cluster Name	Clusters ¹	SB ²	Attrib Name	Attribid		TransDataType		Units	Note
				b15 b6	b7 b0				
Input: OnOff DRC	0xXX	X	OnOff	0000 0000	0000 0000	Unsigned Integer 8-Bit	0x1	Data	
Data Definitions							Value	Units	
On							0xFF	Data	
Off							0x00	Data	
Toggle Output (Used for 3 Way Switches)							0xF0	Data	
Input: DimBright-DRC	0xXX	X	DimBright	0000 0000	RRRR RRRR	Unsigned Integer 8-Bit	0x1	Data	5
Data Definitions							Value	Units	
Dim							0x00	Data	
Bright							0xFF	Data	
Input: Preset DRC	0xXX	X	Store Preset	0000 0000	0000 0000	No Data	0x0	N/A	6
			Preset	0000 0001	RRRR RRRR	Unsigned Integer 8-Bit	0x1	%	5,6
Optional (Direct Addressing Clusters)									
Cluster Name	Clusterid ¹	SB ²	Attrib Name	Attribid		Trans Data Typ		Units	Note
				b15 b6	b7 b0				
Input: Adj DRC	0xXX		Current Level	0000 0000	RRRR RRRR	Unsigned integer 8-Bit	0x1	%	5
			Previous Level	0000 0001	RRRR RRRR	No Data	0x0	N/A	5
			Stop	0000 0101	0000 0000	No Data	0x0	N/A	
			Min Dim Level	0000 0110	0000 0000	Unsigned Integer 8-Bit	0x1	%	
			Max Bright Level	0000 0111	0000 0000	Unsigned Integer 8-Bit	0x1	%	
Input: Light Level LSM	0xXX		Current Level	0000 0000	0000 0000	Semi-Precision	0x08	Lux	
Input: Occupancy OS	0xXX		Current State	0000 0000	0000 0000	Unsigned Integer 8-Bit	0x01	N/A	7
Data Definitions							Value	Units	
Occupied							0xFF	N/A	
Unoccupied							0x00	N/A	
Wait: occupancy sensor is stabilizing (power up cycle)							0xF0	N/A	



Wireless HART kann in bestehende Peer-to-Peer-Verbindungen eingesetzt werden oder sogar komplexe Netzwerke aufbauen

bei der Fokussierung auf ein bestimmtes Anwendungsumfeld.

Definitionen für die Gebäudeautomation, Haustechnik und Industriesteuerungen sowie für die Fernsteuerung von Konsumergeräten sind verfügbar. Durch die einheitlichen Gerätebeschreibungen können unterschiedliche Anbieter kompatible Geräte erstellen.

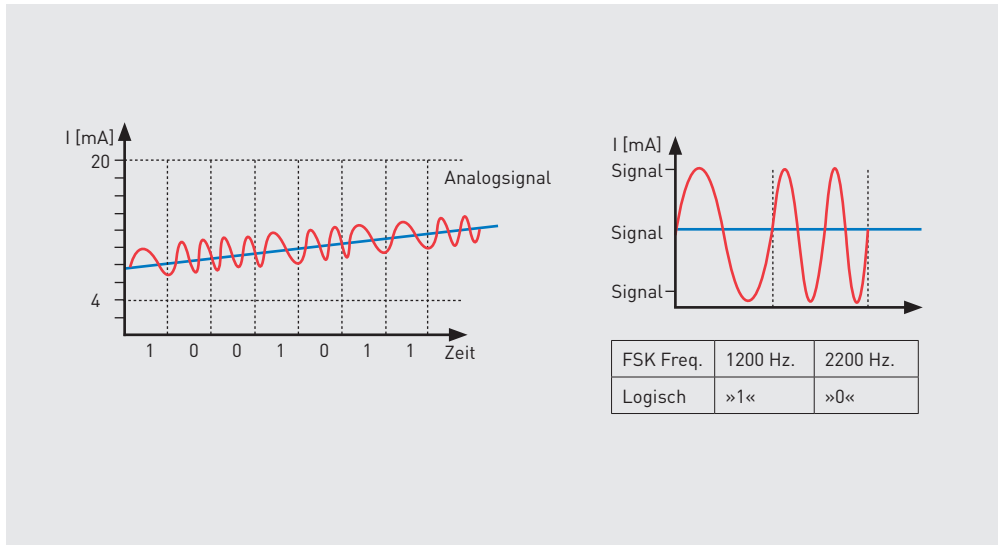
Zu einem vollständigen ZigBee-Protokollstack gehören darüber hinaus noch ein Security-Layer, ein Adaptionlayer für die Anwendungszwischenschicht sowie Geräteobjekte (ZDP Zigbee Device Objects) und deren Anwendungsdefinition in verschiedenen Profilen.

// HART

HART (Highway Addressable Remote Transducer) ist ein Kommunikationsstandard, der sich in den 80er Jahren unter der Federführung der Firma Rosemount entwickelt hat. 1989 wurde die zuerst

proprietäre Technik zu einem Standard erhoben und die HCF (HART Communication Foundation) ins Leben gerufen. Bei HART handelt es sich um eine Erweiterung der klassischen 4 ... 20 mA-Analogtechnik, die in der Prozessindustrie weit verbreitet ist. Inzwischen sind weltweit mehr 24 Mio. HART-fähige Feldgeräte installiert. HART erweitert die analoge Schnittstelle zu einem digitalen Instrumentierungsbus. Zur Übertragung der digitalen Daten wird dem analogen Stromsignal ein mittelwertfreies digitales Signal überlagert. Dies – verbunden mit einer Master-Slave-Kommunikation – erlaubt einen bidirektionalen Datenaustausch. HART lässt bis zu zwei Master zu. In der Regel nutzt man sowohl die Engineering-Konsole in der Leitstation als auch ein sekundäres Gerät vor Ort wie z. B. ein Handterminal oder Laptop als Master.

HART wurde für die Parametrierung von Feldgeräten entwickelt. Das bedeutet, dass eine übergeordnete Station (Master) auf das passive Feldgerät zugreift. Zur Datenaufbereitung wird das digi-



HART überlagert dem Analogsignal ein FSK-kodiertes digitales Teleogramm

tales Signal mit einem HART-FSK-Modem auf den Zweidraht-Leiter angeschaltet und die Steuerbefehle auf das Stromsignal aufmodelliert. Neben diesem Punkt-zu-Punkt-Betrieb ist auch ein Multidrop-Betrieb möglich, wobei bis zu 15 Feldgeräte wie in einem Feldbus betrieben werden. Hierzu ist es jedoch erforderlich, auf die analoge Datenübertragung der Messumformer zu verzichten. Die Multidrop-Betriebsart ist ohnehin nur für Messumformer und nicht für Stellsignale zu verwenden, da der Bus hierfür zu langsam ist. Stellsignale werden prinzipiell als 4 ... 20 mA Einheits-signale übertragen.

HART wird durch die HCF (HART Communication Foundation) vertreten, die als herstellerunabhängige Non-Profit-Organisation den Einsatz von HART sowie seine Spezifikation weiter vorantreibt.

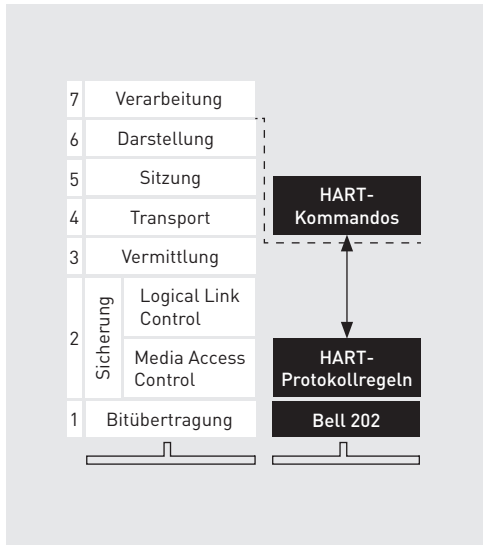
Kabelgebundene HART-Kommunikation

Die Datenübertragung der HART-Komponenten erfolgt nach der Spezifikation Bell 202. Dem ana-

logischen Signal wird ein mittelwertfreies digitales Signal in FSK-Kodierung (Frequency Shift Key) überlagert. Eine logische »1« wird als 1200-Hz-Signal, eine logische »0« als 2200-Hz-Signal mit einer Amplitude von $\pm 0,5$ mA modelliert. Die Spezifikation legt fest, dass ein Master ein Spannungssignal sendet, während die Slaves die Nachrichten über eingepreßte Ströme absetzen. Für einen ordnungsgemäßen Betrieb muss die Gesamtbürde der Stromschleife zwischen 230 und 1.100 Ohm liegen.

Nach Spezifikation eignen sich für kurze Entfernungen ungeschirmte 0,2 mm Zweidrahtleitungen. Mit verdrehten und paarweise geschirmten Leitungen sind Entfernungen von bis zu 3000 m möglich.

Verschiedene herstellereigenspezifische Erweiterungen ermöglichen, wie z. B. beim FSK-Bus (Hartmann & Braun), die Verwendung von HART als Gerätebus mit bis zu 100 Teilnehmern. Durch den Einsatz von Trennverstärkern und die damit er-



HART kann im ISO/OSI-Schema eingeordnet werden.

folgte Entkopplung der Analogsignale wird es möglich, dass Regler und Stellglied weiterhin im Analogmodus miteinander arbeiten, ohne durch andere Geräte beeinflusst zu werden. Bei geeigneter Auslegung der Trennverstärker ist auch ein Einsatz im Ex-Bereich möglich.

Sicherungsschicht

HART verwendet ein reines Master-Slave-Protokoll. Alle Aktivitäten gehen vom Master aus. Ein primärer und ein sekundärer Master sind zugelassen. Der primäre Master ist in der Regel das Leitsystem, der sekundäre Master könnte ein Bediengerät vor Ort sein. Alle HART-Feldgeräte sind passive Slaves. Als Kommunikationsdienste werden eine Standard-Master-Slave-Kommunikation, ein Master-Broadcast und ein Slave-Burstmodus unterstützt.

Bei einer Standard-Kommunikation folgt einem Mastertelegramm umgehend die Antwort vom Slave mit den entsprechenden Daten. Der Burst-Modus ermöglicht es einem Slave, zyklisch Nach-

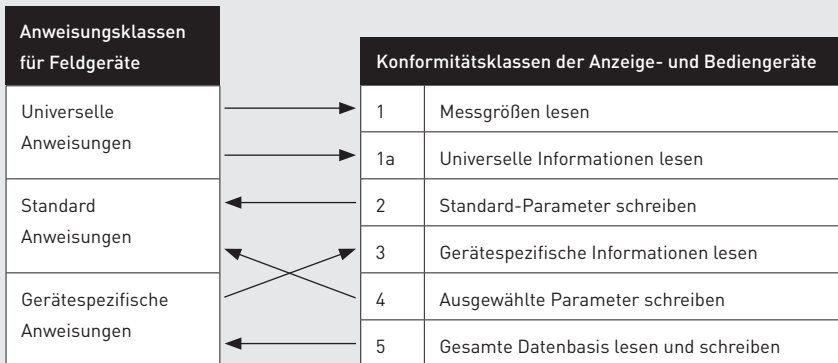
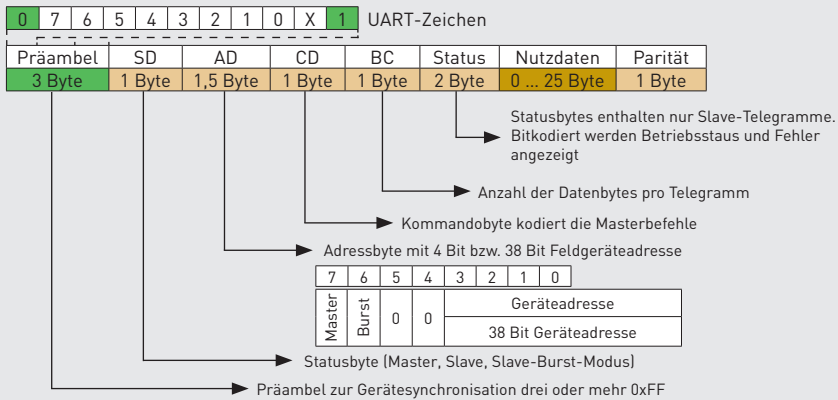
richtentelegramme abzusetzen. Die Anzahl der möglichen Telegramme wird damit auf vier Telegramme pro Sekunde verdoppelt.

Bei einem HART-Telegramm wird jedes Byte als UART-Zeichen mit 11 Bit Länge und einer Geschwindigkeit von 1.200 bps übertragen. Bei einem typischen Telegramm mit 10 Byte Protokoll und 25 Byte Nutzdaten werden für eine Master-Slave-Transaktion inklusive aller Synchronisationsmechanismen durchschnittlich 500 ms benötigt. Es ist offensichtlich, dass HART mit diesem Zeitverhalten keine Konkurrenz für »echte« Feldbusse und ungeeignet für Regelungsaufgaben ist.

Anwendungsprotokoll

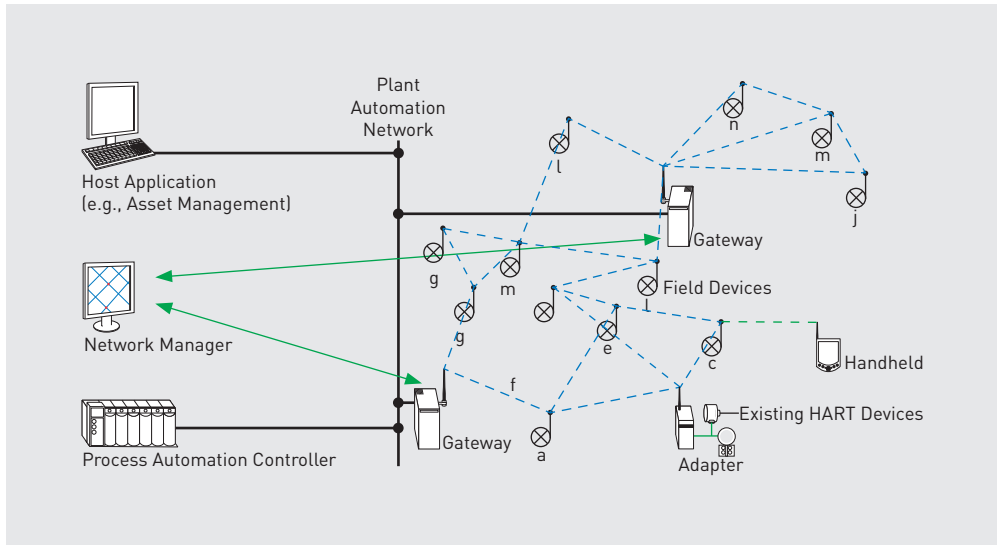
Das Anwendungsprotokoll von HART stellt eine relativ einfache Kommando-Schnittstelle dar. Mit vordefinierten Kommandos kann der Master Befehle oder Nachrichten an das Feldgerät absetzen. Für eine universelle und geräteübergreifende Kommunikation werden die HART-Kommandos in unterschiedliche Gruppen für Feldgeräte (Slaves) und Anzeige- und Bediengeräte gruppiert. Je nach Gerätetyp und Ausprägung sind die jeweiligen Anweisungs- bzw. Konformitätsklassen einzuhalten. Universelle Anweisungen werden von allen HART-Feldgeräten verstanden. Standardanweisungen sind spezifisch für bestimmte Gerätegruppen, und die gerätespezifischen Anweisungen ermöglichen den Zugriff auf spezielle Geräteeigenschaften.

Damit eine unkomplizierte Anpassung der gerätespezifischen Eigenschaften möglich wird und damit eine wichtige Grundlage für die Interoperabilität von Geräten sichergestellt ist, werden HART-Geräte in DDL (Device Description Language) beschrieben. Häufig ist die Gerätebeschreibung im Gerät in binärer Form hinterlegt, so dass die Parametrierwerkzeuge während des Konfigurationsvorgangs einen Zugriff auf die Datenbasis und damit den Funktionsumfang eines Feldgeräts haben.



Oben: Aufbau eines HART-Telegramms

Unten: Anweisungs- und Konformitätsklassen ermöglichen eine Interoperabilität der HART-Geräte.



Struktur eines Wireless HART-Systems als Mesh Network

// Wireless HART

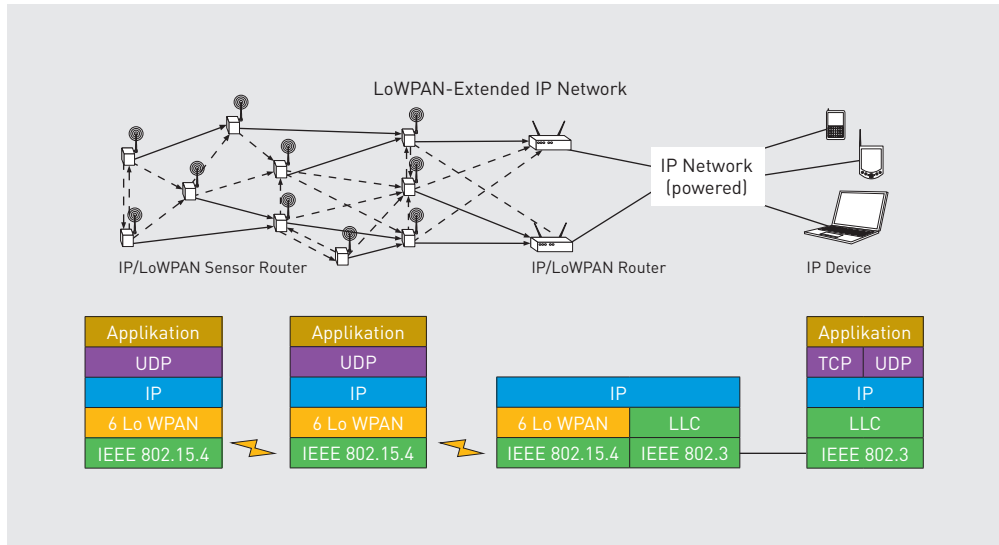
Im Jahr 2005 etablierte das Unternehmen DUST Networks ein Low-Power-Mesh-Netzwerk auf der Basis des 802.15.4 Standards. Mit der Entwicklung des TSMP (Time Synchronized Mesh Protocol) wurde eine stabile Basis entwickelt, die ein sicheres und vor allem zuverlässiges Low Power-Netzwerk mit langen Batteriestandzeiten ermöglichte. 2006 traf Emerson Process die Entscheidung, das von DUST Networks entwickelte Protokoll zunächst im 912 MHz-Band in seine Produkte zu integrieren und damit den ersten Schritt in Richtung »Wireless Sensor Networks« in der Prozessindustrie zu realisieren.

Die folgenden Normungsbemühungen führten zu einer Integration der Funktechnologie – inzwischen basierend auf der IEEE 802.15.4-2006 Spezifikation im 2.4 GHz-Band – in den »Wireless HART« Standard im September 2007. Wireless HART ist Teil der HART 7 Spezifikation gemäß IEC 62591:2010.

Die Besonderheit von Wireless HART ist das TSM-Protokoll. Auf der Basis des IEEE 802.15.4 Standards für den PHY und MAC-Layer erfolgt eine Erweiterung der Zugriffsschicht zu einem zeitlich synchronisierten Netzwerk. Die gesamte Signalübertragung wird in einem 10-ms-Raster geplant. Jeder Station wird zu einer bestimmten Zeit ein Slot zugeteilt, in dem die Kommunikation mit den jeweiligen Partnern abgewickelt werden muss. In der Zeit, in der keine Kommunikation erfolgen soll, kann sich die jeweilige Station »schlafen legen«, was zu einer erfreulich langen Batterielebensdauer führt. In der Regel geht man von Updatezyklen für das gesamte Netzwerk von einigen Sekunden bis Minuten aus.

Um das Störungsverhalten zu verbessern, wird für jeden Datenaustausch eine andere Frequenz nach einem pseudozufälligen Muster verwendet, so dass eine hohe Zuverlässigkeit gewährleistet ist. Insgesamt sind fünf Mechanismen für den zuverlässigen Betrieb verantwortlich:

1. Geplante, zeitsynchrone Kommunikation



6LoWPAN ermöglicht den Aufbau von IPv6 (Sensor)-Netzwerken auf der Basis von IEEE 802.15.4 (siehe Seite 114).

2. Kanalwechsel nach jedem Übertragungsereignis
3. Automatische Verknüpfung der Kommunikationsknoten und Aufbau der Netzwerkstruktur
4. Redundante vermaschte Datenübertragung mit Kanalmonitoring
5. Verschlüsselung der Daten für eine hohe Sicherheit.

zur Verfügung stellt. Im Allgemeinen handelt es sich dabei um einen intelligenten Sensor, der als autarke Messstelle in ein Systemumfeld integriert wird. Endgeräte werden dort eingesetzt, wo aus Kostengründen keine konventionelle Verdrahtung erfolgen kann. Gerade in der Prozessindustrie sind extrem hohe Installationskosten, im Besonderen in den Außenbereichen, üblich.

Um den unterschiedlichen Anforderungen der Geräte gerecht zu werden, gibt es drei unterschiedliche Typen von Wireless-HART-Endgeräten:

Adapter

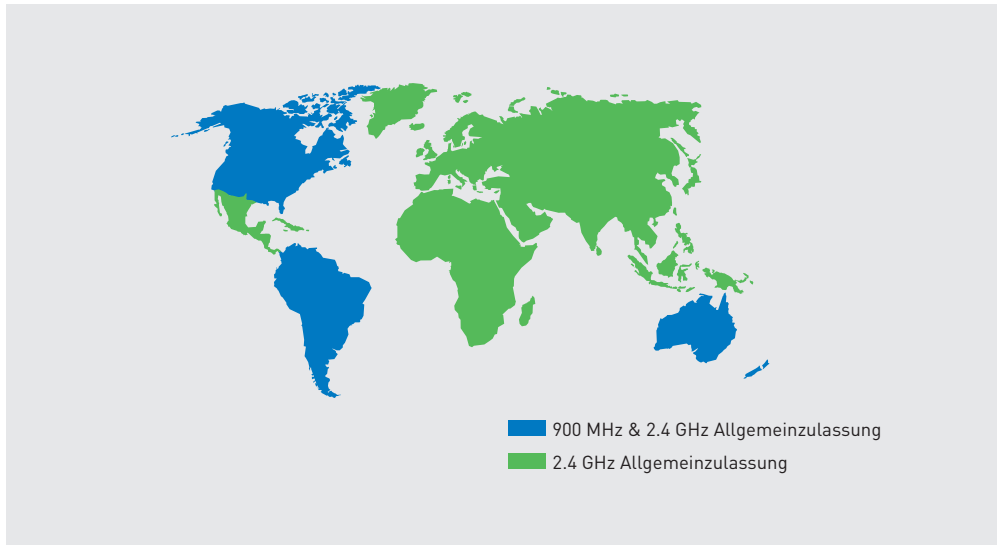
Ein Wireless HART-Adapter nutzt die konventionelle HART-Schnittstelle nach Bell 202-Standard und dient als Datenhub für das Wireless-Netzwerk. Auch mehrere Geräte können per Stromleitung angeschlossen werden.

Endgerät

Ein Wireless HART-Endgerät ist ein Gerät, das in der Regel Mess- und Überwachungsfunktionen

Gateway

Kernstück einer Wireless HART-Infrastruktur ist das Gateway. Gemäß Spezifikation besteht es aus der Funkeinheit, die als Accesspunkt für die Funkdevices dient, dem Netzwerkmanager, der für die Steuerung der Verbindungen, den Aufbau des Netzwerks und der Verwaltung der Sicherheitszertifikate der Endgeräte verantwortlich ist und schließlich dem Gateway, das als Systemschnittstelle zwischen dem Hostsystem, in der Regel ein Ethernetnetzwerk, und dem Wireless HART-Netzwerk dient. Durch den Einsatz mehrerer Gateways kann zusätzliche Redundanz eingebaut werden, um eine höhere Verfügbarkeit zu erzielen.



Nur das 2,4 GHz-Band bietet den Vorteil einer weltweiten Allgemeinzulassung

6LoWPan

Eine andere interessante, auf der Spezifikation IEEE 802.15.4 aufsetzende Kommunikationstechnologie ist 6LoWPan. Die Abkürzung bedeutet »IPv6 over Low power WPAN (Wireless Personal Area Network)«. Ziel der in der durch die IETF (Internet Engineering Task Force) ins Leben gerufenen Spezifikation RFC 4944 ist die effiziente Kommunikation von IPv6 Datenpaketen über IEEE802.15.4 Netzwerke.

Kern von 6LoWPAN ist die Realisierung eines IP-basierten Sensornetzwerks mit einem Minimum an zusätzlichem Aufwand. Der Vorteil liegt auf der Hand: IP-Netzwerke sind heute Stand der Technik, werden sehr gut beherrscht, die notwendigen Protokollstacks sind verfügbar.

Hier liegt auch ein besonderer Anspruch an die Technologie. Sie soll eine bessere Embedded-Integrierbarkeit als IEEE 802.11 WLAN ermöglichen und gleichzeitig einen um den Faktor 100 geringeren Energieverbrauch ermöglichen. Besondere

Herausforderungen ergeben sich in der Notwendigkeit, die ausladenden IPv6 Header auf die Anforderungen der IEEE 802.15.4 anzupassen und ebenfalls die Datenpakete zu segmentieren, um die MTU von 802.15.4-Datenpaketen mit 127 Bytes nicht zu überschreiten. Die RFC 4944 gibt Anleitungen, wie die entsprechenden Header komprimiert werden können, um die Kompatibilität zwischen den Technologien herzustellen.

Mittlerweile sind auch die ersten nicht kommerziellen und kommerziellen Protokollstacks für 6LoWPAN am Markt verfügbar. Der Gedanke, »all-IP« auch auf Sensornetzwerke auszudehnen, hat einen großen Charme und wird sicherlich in Zukunft eine nicht unbedeutende Rolle spielen.

2,4 GHz-Technologien

Das 2.4 GHz-Band ist das wohl interessanteste Frequenzband für alle Bereiche technischer Funksysteme. Dieses hat mehrere Gründe. Erstens steht mit einer Bandbreite von 83,5 MHz hinreichende Kapazität zur Verfügung. Zweitens ist

dieses Frequenzband das einzige, das weltweit weitestgehend harmonisiert ist. Wenn man also Weltmarktprodukte erstellen möchte, bleibt dem Hersteller also kaum eine andere Wahl.

Diese große Attraktivität hat auch einen großen Nachteil. Nahezu alles, was in irgendeiner Weise funkt, ist im 2,4 GHz-Band unterwegs: angefangen von den etablierten Funktechniken wie Bluetooth und WLAN über das schon erwähnte ZigBee und Wireless HART bis hin zu Video-Übertragungssystemen und Babyphones.

In Deutschland existiert eine Allgemeinzuteilung des 2,4 GHz-Bandes für nahezu alle Anwendungen mit einer Sendeleistung von bis zu 10 mW ohne Einschränkung der Bandbreite oder der Frequenzbelegung. Darüber hinaus dürfen Geräte mit bis zu 100 mW für den Anwendungsfall »Lokale Funknetze« (WLAN Wireless Local Area Networks) betrieben werden, bei denen im Frequenzsprungverfahren eine maximale Leistungsdichte von 100 mW/100 kHz bzw. im Spreizspektrumverfahren von 10 mW/1 MHz abgestrahlt wird.

Die aktuelle Frequenzzuteilung gilt bis zum 31.12.2013. Eine Änderung ist sehr wahrscheinlich, da auch andere Systeme wie zum Beispiel digitale Fernsteuerungen für Modellflugzeuge und andere Modelle in diesen Frequenzbereich drängen.

Proprietäre Technologien: steute wireless

Viele proprietäre Funkstandards nutzen eben wegen der internationalen Verfügbarkeit die 2,4 GHz-Technologie. Dazu gehört das von steute speziell für die Anforderungen der Medizintechnik entwickelte »steute wireless« System, das auf Seite 182 ausführlicher beschrieben wird.

// Bluetooth

Bluetooth ist die bisher erfolgreichste kabellose Kommunikationstechnologie: Keine andere kabellose Konsumertechnologie konnte in den vergan-

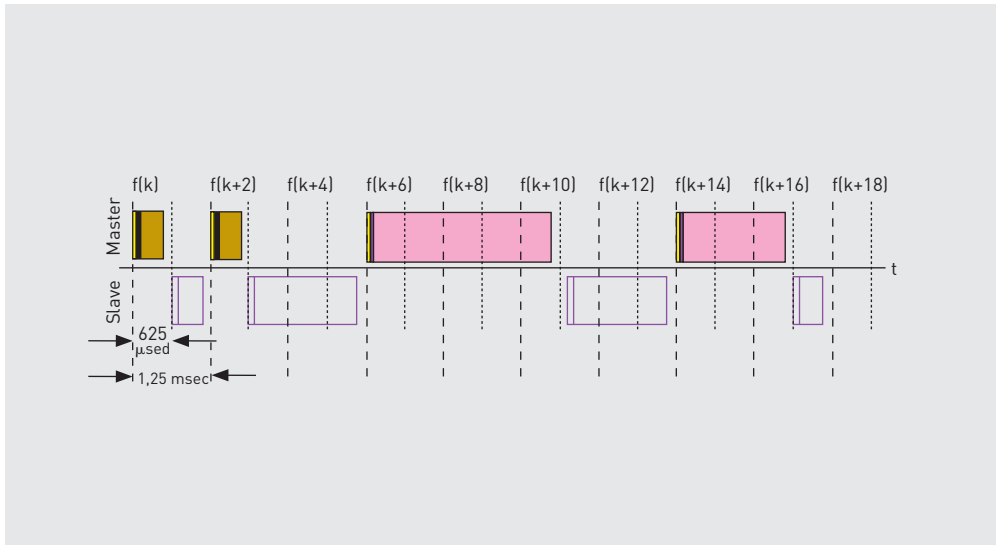
genen zehn Jahren ein ähnlich großes Wachstum in einer so kurzen Zeit erreichen. In der Bluetooth Special Interest Group (SIG) sind über 10.000 Mitglieder versammelt, die den Einsatz der Bluetooth-Technologie aktiv unterstützen. Kaum eine andere Interessengruppe konnte in einer derart kurzen Zeit eine ähnliche Dynamik entwickeln. Gleichzeitig wird bei den Bluetooth-Chipherstellern ein Marktwachstum von um 20 % jährlich realisiert. Kurz: Bluetooth ist eindeutig eine State-of-the-Art-Technologie.

Historie

In den 90er Jahren hat der Mobiltelefon-Hersteller Ericsson in einer Studie erforscht, wie die unterschiedlichen Kommunikationsendgeräte an das Mobilfunknetz angeschlossen werden. Schnell kristallisierte sich heraus, dass Kabelverbindungen zu Gunsten kostengünstiger, effizienter Funkschnittstellen verschwinden werden. Das Projekt fand eine große Resonanz, so dass sich im Mai 1998 die Unternehmen Ericsson, Nokia, Intel, IBM und Toshiba zur Special Interest Group (SIG) zusammenschlossen, um einen gemeinsamen Standard zu entwickeln. Es war offensichtlich, dass ein Funkstandard nur dann erfolgreich sein kann, wenn er auf eine hinreichende Akzeptanz bei den wesentlichen Protagonisten stößt. Drei Ziele wurden von der SIG verfolgt:

1. Entwicklung einer einheitlichen Spezifikation mit dem Ziel einer normungsfähigen Schnittstelle mit Hard- und Software.
2. Schaffung eines Entwicklerforums mit der Möglichkeit der Produktzertifizierung für eine sichere Interoperabilität und
3. Offenlegung des Standards zu Null-Kosten-Lizenzen, bei dem jeder Interessent einen Zugang zu allen relevanten Spezifikationen hat.

Die erste Arbeitsversion (Vo.7) wurde am 19. Oktober 1998 veröffentlicht, bei der nur die rudimentären Funktionen des Basisbands und des Link Managers spezifiziert waren. Im Januar 1999



Der Master sorgt für das slotgenaue Timing in einem Piconet

folgte dann in der Version 0.8 eine detaillierte Spezifikation des Radios und der grundlegenden Softwareschichten für den Datentransport. Der erste offizielle Launch der Bluetooth-Core-Spezifikation in der Version 1.0a erfolgte am 26. Juli 1999 auf den Webseiten der SIG.

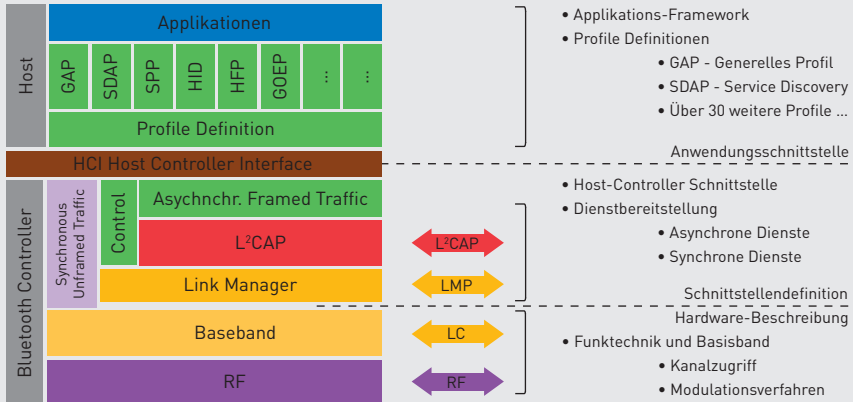
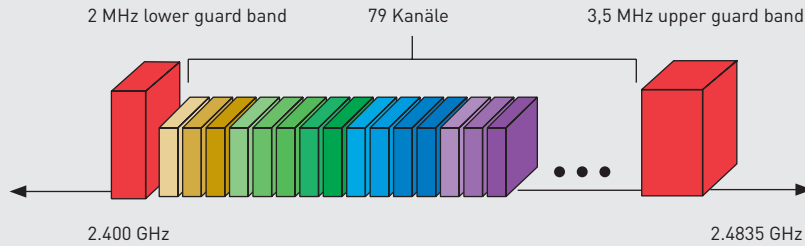
Dieser erste Wurf war nicht fehlerfrei, so dass schon zum Ende des Jahres (12/1999) die Version 1.0B folgte, die vor allem um Interoperabilitätsanforderungen erweitert wurde. Den Durchbruch schaffte die im Februar 2001 veröffentlichte Version 1.1. Auch heute sind Produkte am Markt, die mit diesem Versionsstand ordentlich funktionieren.

Bluetooth gehört zu den sogenannten PANs (Personal Area Network), die in der IEEE 802.15 im Fokus stehen. 2002 erfolgte die Adaption von Teilen des Bluetooth V1.1 Standards an die IEEE-Normen als IEEE 802.15.1-2002. Traditionell spezifiziert die IEEE 802.x Arbeitsgruppe nur die unteren Protokolllayer des PHY und MAC, so dass die

höheren Protokollschichten und Profile von der IEEE-Norm nicht erfasst werden.

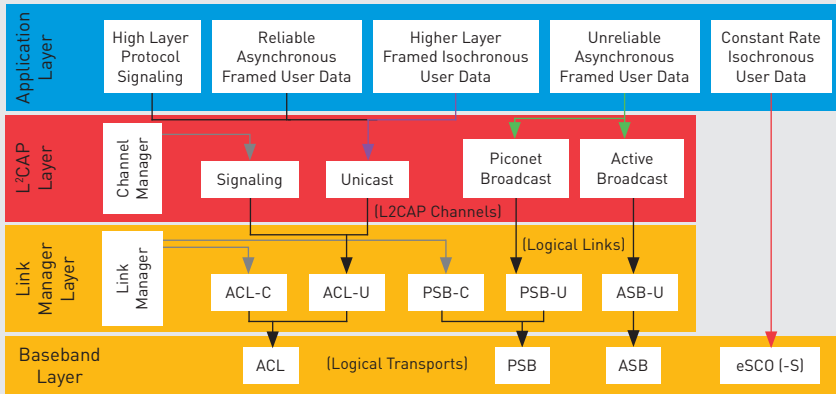
Durch die ansteigende Verwendung von Bluetooth und die hohe Penetration von WLAN-Systemen (IEEE 802.11b/g WLAN) wurde es notwendig, die Koexistenz der weitgehend komplementären Funktechnologien zu optimieren. Das 2,4 GHz-ISM-Band hat schließlich limitierte Ressourcen und das von Bluetooth genutzte hartnäckige Funkverfahren FHSS (Frequency Hopping Spread Spectrum) mit 1.600 Hops pro Sekunde sorgte für eine deutliche Beeinträchtigung der WLAN-Funkverbindungen.

Um diesen Tatsachen Rechnung zu tragen, erfolgte in der Version 1.2 im November 2003 die erste Rundumerneuerung von Bluetooth. Schwerpunkt der neuen Spezifikation war ein verbesserter Verbindungsaufbau, ein adaptives Frequenz-Hopping für eine bessere Koexistenz, verbesserte Mechanismen zur Synchronisation und Datenflusssteuerung sowie die Datenübertragung über die



Oben: Bluetooth nutzt 79 Kanäle mit 1 MHz Bandbreite im 2.4 GHz-ISM-Band

Unten: Übersicht des Bluetooth-Protokoll-Stacks



Überblick über die Bluetooth-Datenkanäle der Version 2.1

synchronen SCO (Synchronous Connection Oriented) Links.

Diese nachhaltigen Verbesserungen hätten eigentlich einen ganzen Versionsschritt gerechtfertigt, was dann auch in der Version 2.0 vom 1. August 2004 erfolgte. Eine wichtige Neuerung in der Version 2.0 gegenüber 1.2 ist der Zusatz »EDR« für Enhanced Data Rate. Während das klassische Bluetooth-Piconet gerade einmal 1 Mbps Bruttodatenrate ermöglicht, sind in den Highspeedmodi Bruttoraten von 2 bzw. 3 Mbps möglich.

In der Version 2.1 + EDR vom Juli 2007 kommen noch etliche neue Features, wie z. B. das »Secure Simple Pairing«, hinzu, die Bluetooth im Wesentlichen eine bessere Handhabbarkeit und schnellere Zugriffszeiten ermöglichen.

Aktuelle Bluetooth-Spezifikationen

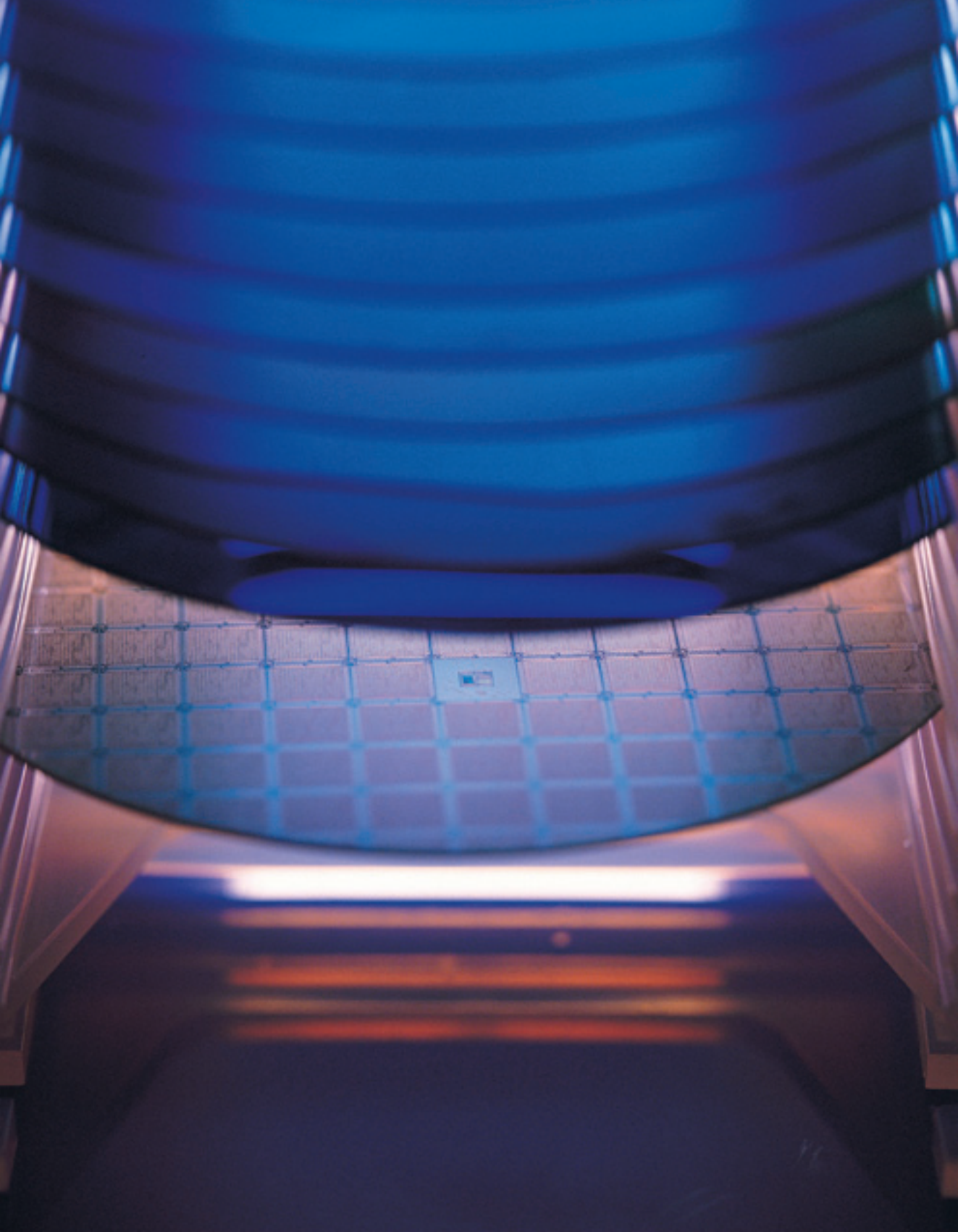
Im April 2009 wurde die Version Bluetooth 3.0 + HS (High Speed) ratifiziert. Der High-Speed-Kanal basiert auf WLAN 802.11 und ermöglicht einen

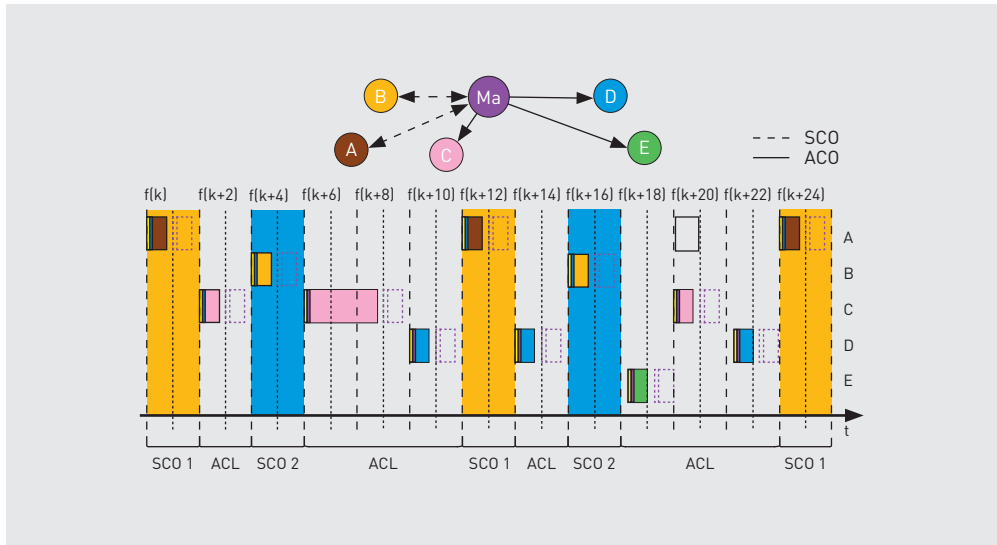
schnellen Datenkanal über die zweite Funktechnik. Der Verbindungsaufbau und die Dienstbereitstellung wie auch die Sicherheit werden weiter durch den Bluetooth-Kanal realisiert. Durch die Integration von WLAN ist eine Datenrate von bis zu 24 Mbps möglich. Ursprünglich wurde der Highspeed-Kanal unter der Verwendung von UWB (Ultra Wide Band – ECMA 0368) geplant, dies wurde später jedoch wieder aufgegeben.

Die aktuelle Spezifikation ist Bluetooth 4.0 EDR. Mit ihr sollen weitere Optimierungen verbunden sein, die vor allem einen extrem schnellen Verbindungsaufbau (< 5 msec) und eine höhere Sicherheit ermöglichen. Darüber hinaus ist die Reduzierung des Stromverbrauchs bei den neuen Versionen ein wesentlicher Meilenstein. Ziel ist der jahrelange Betrieb eines Bluetoothgerätes mit einem Energiespeicher.

Technologischer Überblick

Technologisch unterscheidet sich Bluetooth wesentlich von anderen Funktechnologien, da schon





Master- und Slave-Kommunikation in einem Piconetz

bei der Spezifikation auf die Embedded-Integration geachtet wurde. Das bedeutet, dass nicht ein TCP/IP-basierter Ansatz für die Datenübertragung gewählt wurde. Vielmehr ermöglicht ein dienstleistungsorientiertes Framework eine skalierte Bereitstellung von Diensten. Über 30 unterschiedliche Profile sind bereits definiert oder stehen in Spezifikation, um spezielle Lösungen zu realisieren. Entsprechend der Vielzahl der unterschiedlichen Einsatzmöglichkeiten sind auch die technischen Randbedingungen.

Die Bluetooth-Technologie kann in drei logische Abschnitte unterteilt werden:

Funktechnik und Basisband

stellen die Low-Level-Funktionalität des Systems bereit. Hier sind prinzipielle Funktionsweisen hinterlegt, die auf nahezu allen Geräten ausnahmslos identisch funktionieren müssen.

Linkmanager und Host-Controller-Interface

bilden die Schnittstelle zwischen Applikation und

Funktechnik. Der Linkmanager ist für das Verbindungsmanagement verantwortlich, das HCI (Host Controller Interface) bietet eine standardisierte Schnittstelle zum Host-Computer.

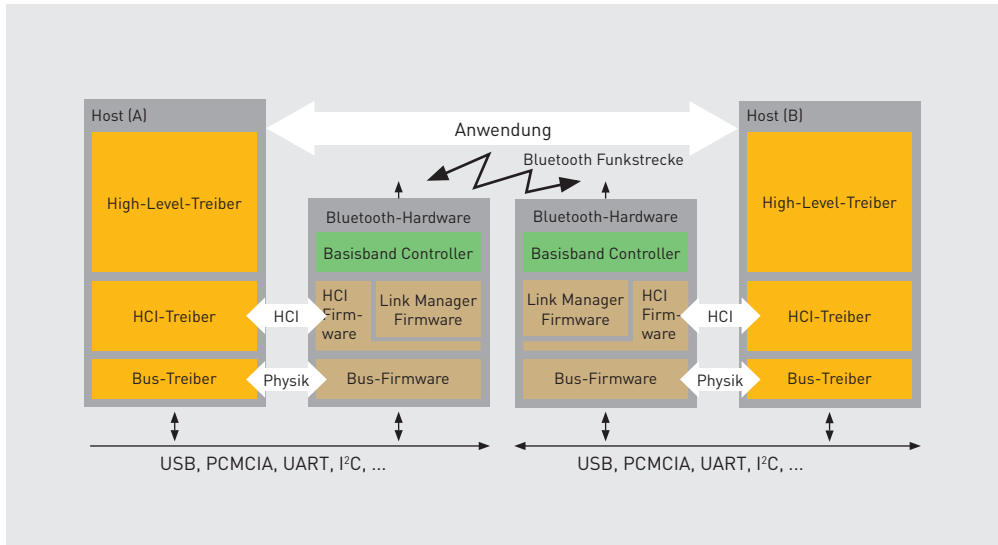
Anwendungsschicht

Aufgrund der unterschiedlichen Einsatzmöglichkeiten werden in Bluetooth verschiedene Anwendungsmodelle, so genannte Profile, definiert. Sie bilden die Anwendungsschnittstelle von Bluetooth.

Bluetooth-Protokolle:

Funktechnik und Basisband

Aus der Sicht der Funktechnik verwendet Bluetooth ebenfalls das 2,4 GHz-ISM-Band. Im Gegensatz zu WLAN wird jedoch ein Frequency-Hopping-Verfahren mit bis zu 79 Kanälen von 1 MHz Bandbreite gewählt. Die Kanäle werden pseudozufällig mit einer Hopping-Rate von 1.600 Hop/s durchlaufen. Die Hopsequenz ist für ein Piconet charakteristisch und im Wesentlichen von einer Clock und der Geräteadresse (Bluetooth



Die HCI-Schnittstelle abstrahiert die Bluetooth-Hardware zum Host.

MAC-ID) abhängig. Aufgrund des Hoppingverfahrens ist Bluetooth im Vergleich zu anderen Funksystemen sehr robust gegenüber schmalbandigen Störern. Seit der Version 1.2 kommt noch ein adaptives Frequenzhopping hinzu, das Frequenzbereiche explizit ausblenden kann, so dass eine konfliktfreie Koexistenz von Störern bzw. anderen Funksystemen im selben Frequenzband möglich wird.

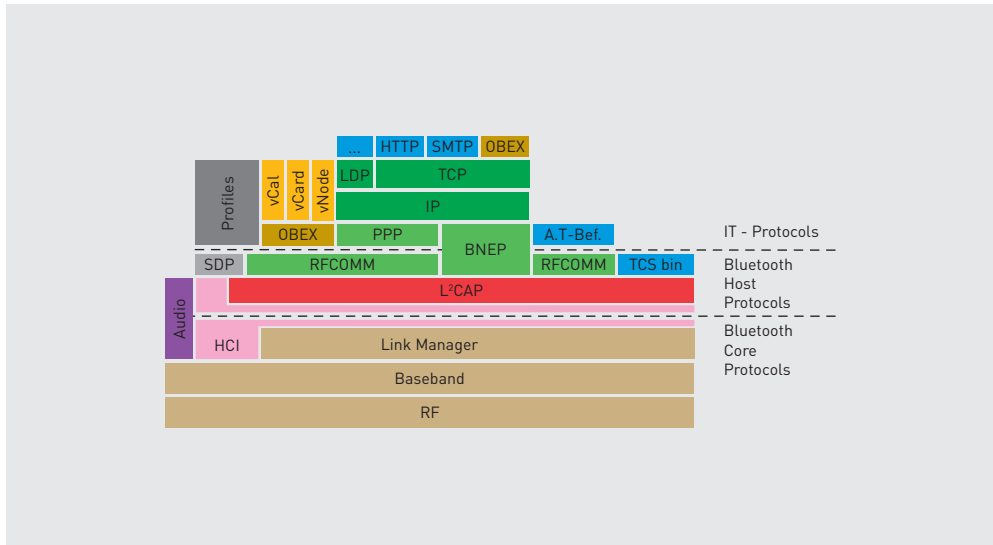
Drei Leistungsklassen

Bluetooth definiert drei Leistungsklassen für Funkmodule. Klasse 3-Module kennzeichnen das untere Leistungsende mit einer Sendeleistung von 1 mW und einer typischen Reichweite von 10 Metern. Klasse 2-Module haben eine Sendeleistung von 2,5 mW und eine Reichweite von ca. 30 Metern. Das obere Leistungsspektrum wird durch 100 mW-Module mit Reichweiten bis zu 100 Metern erreicht. Klasse 2- und Klasse 1-Module sind mit einer Leistungsregelung ausgestattet, so dass nur mit der maximal notwendigen Leistung gesendet wird. Die tatsächlich erreichbare Reich-

weite hängt wesentlich vom HF-Design, der verwendeten Antenne und der gesamten Qualität der Komponenten ab.

Ein Bluetooth-Netzwerk formt sich als so genanntes Piconetz. Ein Knoten übernimmt hierbei die Rolle des Netzwerkmasters und prägt den angeschlossenen Slaves mit seiner Bluetooth-ID und seinem Timing die Hopsequenz ein. Bis zu sieben Slaves können aktiv mit dem Master kommunizieren. Weitere 255 können, je nach Implementierung, als Parked-Member zu dem Piconetz gehören. Durch diese Form der Netzbildung können rein theoretisch fast 20.000 Teilnehmer in einer Funkzelle in 79 Piconetzen konfliktfrei koexistieren. Bluetooth bietet damit eine extrem hohe Dichte an Kommunikationsknoten.

Durch das Master-Slave-Kommunikationsschema wird ein exakt durch den Master vorgegebenes Timing erreicht. Ein Kommunikationszeitslot beträgt 625 µs. Ein kompletter Datenrahmen bestehend aus Master-Anfrage und Slave-Antwort



Bluetooth-Profile definieren das komplexe Zusammenspiel zwischen Protokollen und Anwendungen

dauert 1,25 ms. Zur Steigerung der Nutzdatenrate sind auch 3- bzw. 5-Slot-Datenpakete möglich. Hierdurch werden bis V 1.2 maximale Datenraten von 433 kbps symmetrisch bzw. 723,2/57,6 kbps asymmetrisch erreicht. Bei der EDR-Definition ab Bluetooth V 2.0 ist eine maximale Datenrate von asymmetrisch 2178,1/ 177,1 kbps möglich.

Bluetooth verwendet bis zur Version 1.2 ein Gaußsches Frequenz-Shift-Keying-Verfahren (GFSK) zur Modulation. Ab der Version 2.0 kommt für die Übertragung von EDR-Datenpaketen noch eine $\pi/4$ -DQPSK (2-Mbps)- und 8DPSK (3-Mbps)-Modulation hinzu. Nur der Nutzdatenanteil der Daten wird mit der PSK-Modulation versendet.

Physikalisch werden im Bluetooth-Controller synchrone (SCO – Synchronous Connection Oriented) und asynchrone (ACL – Asynchronous Connection Less) Datenkanäle zur Verfügung gestellt. Synchrone Datenkanäle werden für das Versenden von Streamingdaten verwendet. SCO-Kanäle ermöglichen die getaktete Datenübertragung ohne

Sendewiederholung. Erweiterte SCO-Kanäle (eSCO) lassen eine Sendewiederholung bis zu einem gewissen Grad zu. Die asynchronen Kanäle unterliegen im Wesentlichen einem ARQ-Schema (Automatic Repeat Request).

Linkmanager und Linkcontroller

Der Linkmanager ist verantwortlich für das Aufsetzen der Verbindung und der Zuteilung der Kanalbandbreite. Für SCO- bzw. eSCO-Kanäle werden feste Zeitslots reserviert. Die übrig bleibenden Zeitschlitze können für die asynchrone Kommunikation verwendet werden.

Neben der Verwaltung der Datenkanäle stellt der Linkmanager Dienste für die Synchronisation der Datenpakete, für die Definition und Überwachung von Dienstgütern (QoS – Quality of Service) sowie für die Sicherheit zur Verfügung.

Das Sicherheitsmodell

Bluetooth unterstützt ein skalierbares mehrstufiges Sicherheitsmodell, das neben drei unter-

schiedlichen Sicherheitsmodi verschiedene Sicherheitsmechanismen anwendet. Alle Mechanismen sind in den Bluetooth-Controllern integriert, so dass keine weitere Sicherheits-Hardware oder -Firmware verwendet werden muss.

Der schwächste Sicherheitsmodus ist Security-Mode 1. Hier ist keine Authentifizierung erforderlich, und die Daten werden generell unverschlüsselt übertragen. Bei Konsumergeräten am häufigsten anzutreffen ist Mode 2. Die Sicherheitsprozeduren werden hier vom Host abgehandelt, so dass in jedem Fall eine Verbindung zum Bluetooth-Controller erforderlich wird. Dem Vorteil der skalierbaren Sicherheit auf Anwendungsebene stehen potentielle Sicherheitslücken gegenüber. Alle bekannten Lücken bei Bluetooth-Attacken basieren auf dieser Mode-2-Problematik.

Eine Sicherheit auf Modulebene garantiert der Security-Mode 3. Hier werden alle Sicherheitsfunktionen des Bluetooth-Chips verwendet, und es sind keine zusätzlichen Maßnahmen auf dem Host notwendig. Mode 3 stellt sicher, dass nur zuverlässige Quellen einen Zugang zum System erlangen. Die Sicherheitsmechanismen, die Bluetooth bereitstellt, bieten darüber hinaus auch die Etablierung von unsichtbaren Punkt-zu-Punkt-Verbindungen, Authentifizierung durch Master und Slave sowie die Änderung des Verbindungs-codes, die auch nach jedem Datenpaket erfolgen kann. Eine Verschlüsselung mit bis zu 128 Bit und das entsprechende Schlüsselmanagement sind ebenfalls in der Technologie integriert.

HCI – Host Controller Interface

Die Anbindung der Bluetooth-Controller an das Host-System erfolgt über das so genannte Host-Controller-Interface. Die HCI-Schicht stellt eine abstrakte Schnittstelle zur Verfügung, die alle relevanten Basisband- und Linkmanager-Funktionen in einer API dem Host anbietet. Typische physikalische Schnittstellen auf dieser Ebene sind USB (Universal Serial Bus) und UART.

High-Level-Host-Software

Bluetooth bietet im Vergleich zu anderen Funksystemen einen sehr mächtigen Protokollstapel. Nicht nur der Datentransport, die Dienstgüte und die Sicherheit werden durch den Bluetooth-Controller implementiert. Vielmehr ist auch der darüber liegende Protokollstapel auf hostseitiger Treiber- und Anwendungsebene definiert. Grundlegende Protokolle hierzu sind SDP, TCP, BNEP sowie AVCTP und AVDTP.

Das Service Discovery Profile (SDP)

stellt grundlegende Dienste für das Finden und Bereitstellen von Dienstmerkmalen auf einem Rechner zur Verfügung. Dies ist notwendig, da nicht alle Bluetooth-Geräte alle Dienste zur Verfügung stellen müssen und in der Implementierung der einzelnen Ausprägungen gewisse Freiheitsgrade zur Verfügung stehen. Bildlich gesprochen übernimmt SDP die Funktion der »Gelben Seiten« eines Bluetooth-Geräts und ist für alle Geräte verbindlich vorgeschrieben.

TCP ist das Telephony Control Protocol,

das für die Verwaltung und Anwendung von Telefondiensten verantwortlich ist. Nur Geräte mit Telefondiensten benötigen dieses Protokoll.

BNEP (Bluetooth Network Encapsulation Protocol)

stellt grundlegende Dienste für die Übertragung von Layer-3-Protokollen über Bluetooth zur Verfügung. Dieses Protokoll ist notwendig in Access-Points und zur Ankopplung beispielsweise an das Ethernet.

AVCTP (Audio Video Control Protocol) und AVDTP (Audio Video Distribution Transport Protocol)

sind neuere Protokolle für den Transport und die Steuerung von Video- und Audiodaten.

Oberhalb dieser Bluetooth-Protokolle können etablierte IT-Protokolle wie OBEX oder TCP/IP angebunden werden und das jeweilige Anwen-

A2DP	Advanced Audio Distribution Profile	Übertragung von High-Quality Stereo Audiodaten
AVRCP	Audio Video remote Control Profile	Fernbedienung von Audio/Videogeräten
BIP	Basic Image Profile	Übertragen von Bilddaten
BPP	Basic Printing Profile	Drucken
CIP	Common ISDN Profile	ISDN Verbindung über CAPI
CTP	Cordless Telephony Profile	Schurlose Telefonie
DUN	Dial-Up Networking Profile	Internet Einwahlverbindung über PPP
DI	Device Identification	Identifikation von Geräte bestimmter Hersteller/Dienste
ESDP	Extended Service Discovery Profile	Erweiterte Diensterkennung für uPnP
FAX	Fax Profile	Faxdienste
FTP	File Transfer profile	Dateiübertragung
GAVDP	Generic Audio Video Distribution Profile	Übertragen von Audio-/Videodaten
GOEP	Generic Object Exchange Profile	Datenaustausch von OBEX-Objekten
HCRP	Hardcopy Cable Replacement Profile	Druckeranwendungen
HFP	Hands Free Profile	Kabellose Anbindung von Mobiltelefone im Auto
HID	Human Interface Device Profile	Eingabegeräte wie Tastatur und Maus
HSP	Headset Profile	Sprachausgabe über Headset
OPP	Object Push Profile	Austausch von Kalender- und Visitenkarten
PAN	Personal Area Network	Virtuelle Netzwerkverbindung
PBAP	Phonebook Access Profile	Zugriff auf das Telefonbuch des Mobiltelefons
SAP	SIM Access Profile	Zugriff auf die SIM-Karte des Mobiltelefons und ausschalten des GSM-Teils für Fahrzeugnutzung
SDAP	Service Discovery Application Profile	Ermittlung der Diensterkennung und Profile
SPP	Serial Port Profile	Serielle Datenübertragung
SYNCH	Synchronisation Profile	Datenabgleich von OBEX-Objekten
VDP	Video Distribution Profile	Verteilen von Videodaten

Physikalische Datenrate	1 Mbps
Reichweite	typ. 10 m (2 ... 300 m)
Frequenzband	2,4 GHz (ISM-Band)
Stromverbrauch	Standalone BT x 0,1 ... 0,25 Dual mode BT x 0,8
Modulation	GFSK $h=0,5$ (BT)
Zugriffsverfahren	TDD (Time Division Duplex)
PDU Nutzdaten	Variable Länge 1 ... 31 Byte
Netto Datenrate	Unidirect. 350 (816) kbps Bidirect. 2 x 259 (2 x 449) kbps

Leistungsdaten von Bluetooth LE

dungslayer zur Verfügung stellen. Wie die einzelnen Protokolle angewendet werden, wird in den Profilen geregelt.

Bluetooth-Profile

Die Verwendung der Transportschicht des Linkmanagers wird durch Profile geregelt. Profile definieren genau, welche Rolle und Aufgabe ein Master- und Slave-Gerät in einem speziellen Anwendungsfall hat. Hierdurch ist eine sehr differenzierte Skalierung der Funktionalität von Bluetooth-Geräten möglich, was den größten Nutzen dieses Funkstandards ausmacht.

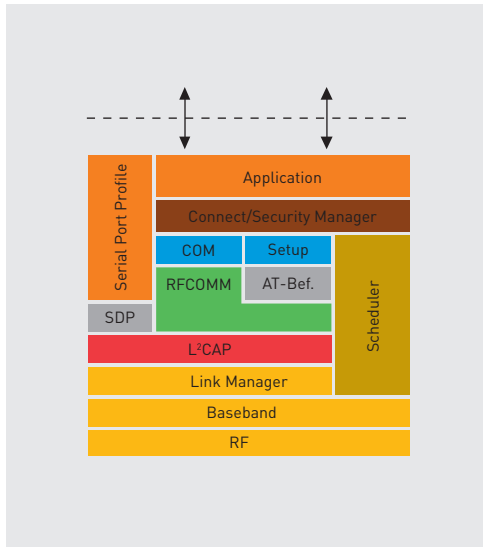
Die Profile GAP und SDAP müssen bei allen Bluetooth-Geräten implementiert sein. GAP (Generic Access Profile) definiert den generellen Zugang zum Bluetooth-Gerät mit den Sicherheitsmodi, der Sichtbarkeit und der Untersuchbarkeit (Inquiry). Das SDAP (Service Discovery Application Profile) regelt den Zugriff auf die Dienstdatenbank der Bluetooth-Geräte, aus der die wesentlichen Kommunikationsparameter und die unter-

stützten Dienste und Profile identifiziert werden können.

Die Basis für viele andere Profile bildet das SPP (Serial Port Profile), das auch als universelle serielle Schnittstelle verwendet wird. SPP kann mehrere virtuelle serielle RS-232-Kanäle über eine Bluetooth-Schnittstelle übertragen und ist damit die Basis für Cable-Replacement.

Bluetooth Low Energy (LE)

Bluetooth Low Energy (LE) rundet die Bluetooth-Funkpalette nach unten hin ab. Gerade für kleinere, energiearme Sensoren ist Bluetooth viel zu mächtig. Durch eine geringere Funktionalität und einen schlanken Protokollstack kommt LE mit gerade einmal 10 – 30 % der Energie eines konventionellen Bluetooth-Bausteins aus. Keine Unterschiede gibt es in der Nutzung des 2,4 GHz-ISM-Bandes mit dem bewährten Frequency Hopping und einfacher GFSK (Gaussian Minimum Shift key)-Modulation, was mit einem nahezu unveränderten Radio möglich ist. Damit sind Netto-



Implementierung von Embedded-Geräten mit Embedded-Stack

datenraten bis 1 Mbps erreichbar. Je nach technischer Realisierung sind Reichweiten von 2 bis 300 m möglich.

Die größten Unterschiede finden sich in dem deutlich einfacheren Protokollstack ab dem Linkmanager. Die Rollen sind eindeutig als Master und Slave definiert. Ein Rollenwechsel ist nicht möglich. Der Slave wird als Advertiser bezeichnet. Durch periodische Broadcasts erfolgt eine Dienstanzeige, auf die ein Master reagieren kann. Master werden auch als Scanner bezeichnet, die nach Dienstanzeigen suchen. Wurde eine Dienstanzeige gefunden, übernimmt der Master das gesamte Verbindungsmanagement. Bis zu 255 Slaves kann der Scanner in einem TDD (Time Division Duplex) -Verfahren verwalten.

Da nur noch 3 statt 32 Aufruffrequenzen verwendet werden, ist ein deutlich schnellerer Verbindungsaufbau möglich, so dass Verbindungszeiten von wenigen zehn Millisekunden möglich werden.

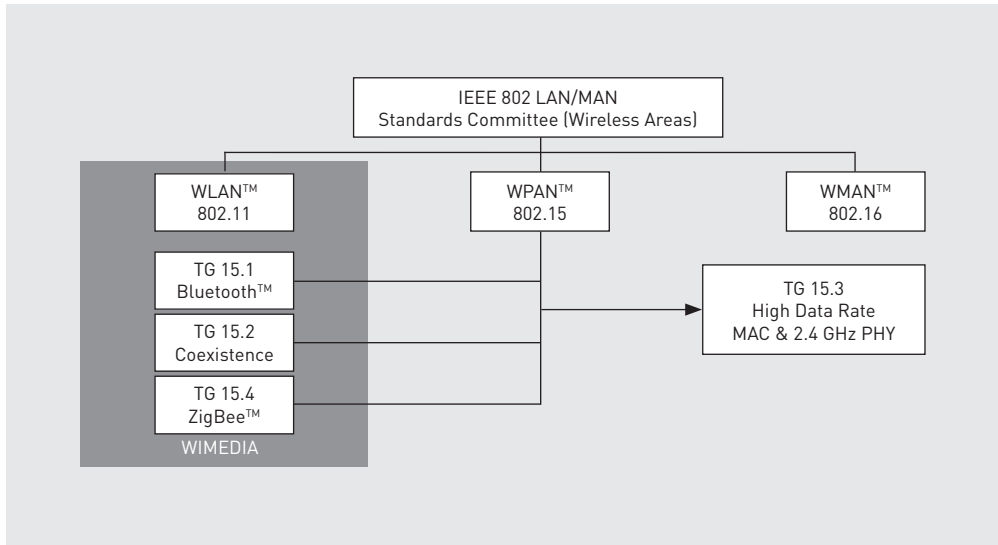
Da das Radio für konventionelles und LE-Bluetooth weitestgehend identisch ist, liegt der Schritt nahe, Dual-Mode Bluetooth-Geräte zu bauen. Für ein konventionelles Bluetooth-System ist der Mehraufwand äußerst gering.

Embedded Integration

Aufgrund des mächtigen Protokollstacks erscheint Bluetooth oft als kompliziert. Dies ist jedoch nicht der Fall. Erstens ist durch die Bildung von Profilen eine saubere Abgrenzung von Funktionalitäten in der Regel sehr einfach möglich. Zweitens ermöglichen heute viele Anbieter die Integration der Upper-Layer-Protokoll-Stacks auf dem Bluetooth-Controller. Hierdurch kann die gesamte Anwendung auf dem Bluetooth-Controller untergebracht werden, bzw. das Embedded-Gerät benötigt nur eine einfache UART-Schnittstelle zum Prozessor für die Integration einer entsprechenden kabellosen Verbindung. Als bevorzugte Profile sind SPP und HID für einfache Embedded-Geräte möglich.

WLAN – WIFI – IEEE 802.11

Die unterschiedlichen Sendeleistungen, die eingesetzten Kodierungsverfahren und die Bandbreite eines Kanals bestimmen im Wesentlichen die Reichweite und den Datendurchsatz bei Funktechnologien. Gerade in diesen Punkten unterscheiden sich die verfügbaren Technologien deutlich. Eine Diskussion, ob Bluetooth oder WLAN eingesetzt werden soll, ist in diesem Sinn in keiner Weise zielführend. Eine gute Sicht auf die gesamte Problematik wird beim Blick auf die Normungssituation deutlich. Das IEEE spielt dabei als normungsgebendes Institut eine wichtige Rolle. Unter der Arbeitsgruppe 802 arbeiten unterschiedliche Arbeitsgruppen an der Standardisierung von kabelloser und kabelgebundener Kommunikation. Die als WLAN bekannten Spezifikationen der Arbeitsgruppe 802.11 spiegeln nur einen Teil der kabelfreien Kommunikation wider. Um nicht zu weit auszuholen, sollen folgende Klassifizierungen ausreichen:



Wireless-Technologien nach IEEE 802

802.11 WLAN

Unter dieser Arbeitsgruppe werden im Wesentlichen Aktivitäten für ein kabelloses Ethernet zusammengefasst. Die Standardisierung ist in vollem Gang, und es werden unterschiedlichste PHY- und MAC-Layer für eine Kommunikation mit hoher Geschwindigkeit im 2,4 GHz- und 5 GHz-Band definiert. Die Dynamik der Arbeitsgruppe wird dokumentiert durch das Buchstabeninkrement, das mittlerweile bei 802.11n angekommen ist.

802.16 WMAN

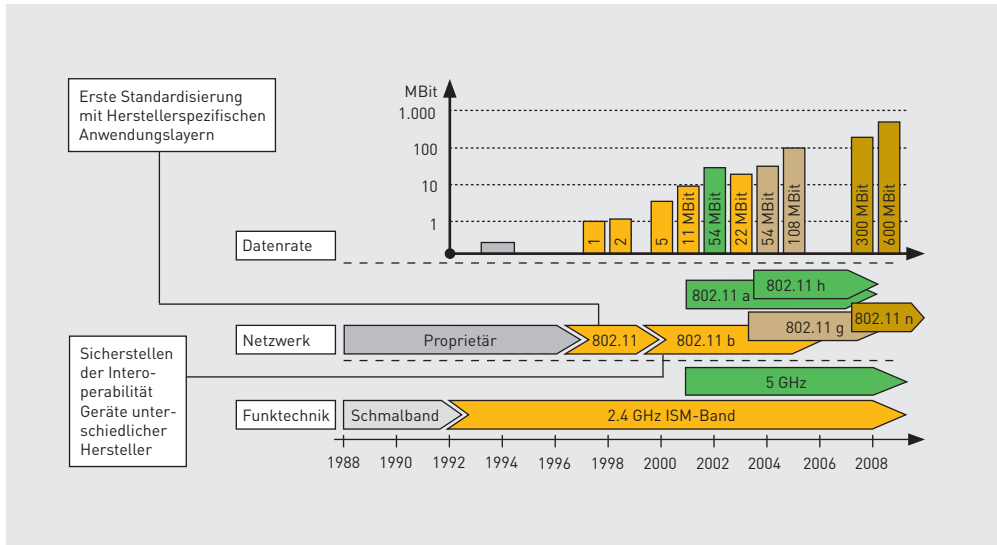
bezeichnet das Wireless Metropolitan Area Network. Diese Art von Netzwerk beschreibt einen Standard für die Weitverkehrskommunikation, die zumindest in Europa durch GSM- und UMTS-Funktechnik abgedeckt wird.

802.15 WPAN

Wireless Personal Area Network beschreibt Netzwerke für die Kommunikation im Nahbereich. WPANs spielen eine besondere Rolle für das Ad-

hoc-Networking und den Datenaustausch zwischen mobilen Endgeräten wie PDAs (Personal Data Assistant) oder Mobiltelefone. Dieser Bereich wird heute durch Bluetooth abgedeckt. In der Arbeitsgruppe 802.15.1 bemüht man sich um die Integration von Bluetooth als IEEE-Standard. Bluetooth MAC und PHY wird bereits von IEEE spezifiziert. Aufgrund der hohen Komplexität und dem damit verbundenen nicht optimalen Low-Power-Verhalten sorgt 802.15.4 mit ZigBee für eine Abrundung der Wireless-Kommunikation nach unten hin. ZigBee ist als reines Master-Slave-System mit Datenraten bis zu 128 kBit optimiert auf Low-Power und die Übertragung auch kleinster Datenpakete. Darüber hinaus beschäftigt sich die Arbeitsgruppe mit der Interoperabilität der unterschiedlichen Funktechniken in 802.15.2 und der optionalen Steigerung der Datenrate in der Untergruppe 802.15.3.

Die häufig anzutreffende Meinung, WLAN, Bluetooth und ZigBee sind austauschbare Technologien, ist demnach nicht richtig. Vielmehr ver-



Entwicklung der Technologien nach IEEE 802.11

bergen sich hier Standards, die sich aufgrund der unterschiedlichen Charakteristik ergänzen bzw. für spezialisierte Anwendungsfälle besonders geeignet sind. Dieser Erkenntnis folgt auch die Industrie, die sich bemüht, durch die WIMEDIA-Allianz (www.wimedia.org) eine Plattform zu schaffen, um eine zukünftige Interoperabilität zwischen den einzelnen Systemen sicherzustellen.

Die Historie von IEEE 802.11

Spricht man von WLAN, dann ist zumeist Wireless LAN nach IEEE 802.11 gemeint. Hinter dieser Zahlenabkürzung findet sich heute ein ganzer Zoo unterschiedlichster und zum Teil nicht einmal kompatibler Technologien wieder.

Historisch gesehen entwickelte sich WLAN aus den Anfang der 90er Jahre freigegebenen 2,4 GHz-ISM-Band und den Bemühungen des IEEE, einen Standard für den MAC und PHY-Layer zu entwickeln. 1997 wurde schließlich der 802.11 Standard verabschiedet, der neben einer diffusen Infrarot-Übertragung ein technisch wenig an-

spruchsvolles Frequenzsprungverfahren (FHSS – Frequency Hopping Spread Spectrum) nutzte und eine Datenrate von 1 bzw. 2 Mbps ermöglichte. Durch ein geändertes Modulationsverfahren, das DSSS (Direct Sequence Spread Spectrum), wurde schließlich 1999 unter der 802.11b eine am Markt äußerst erfolgreiche WLAN-Alternative mit Datenraten von 11 Mbps im 2,4 GHz-Band entwickelt. Dieser Standard ist heute die Mutter aller WLAN-Implementierungen.

Schnell wurde deutlich, dass die erreichbare Nettodatenrate für hochwertige Anwendungen nicht ausreicht und dass gerade das 2,4 GHz-Band zu wenig Kanalkapazität für eine hohe Anzahl von Funkknoten bereitstellt. In Europa arbeitete man an den HyperLAN-Standards und antwortete aus dem amerikanischen Sprachraum mit dem 802.11a Standard. Durch die Nutzung des 5 GHz-ISM-Bands, verbunden mit einer OFDM (Orthogonal Frequency Division Multiplexing)-Modulation konnten Datenraten von typisch 54 MBps erreicht werden. Aufgrund der schwierigen

	Funktion	Layer
802.11	1–2 Mbit, FHSS, DSSS, IR	MAC, PHY
802.11a	Bis 54 MBit, OFDM, 5 GHz	PHY
802.11b	Bis 11 Mbit, DSSS, 2.4 GHz	PHY
802.11c	MAC-Bridge	MAC
802.11d	International Roaming	MAC
802.11e	QoS Quality of Service	MAC
802.11f	Interaccess Point Protocol	MAC
802.11g	Bis 54 Mbit, DSSS/CFDM, 2.4 GHz	PHY
802.11h	Transmit Power Control/Dynamic Frequency Selection	MAC
802.11i	Security	MAC
802.11k	Radio Ressource Management	PHY
802.11m	Maintenance of Standart	MAC, PHY
802.11n	High Troughput (>100 Mbit)	MAC, PHY

Übersicht der wesentlichen 802.11-Technologien

Harmonisierung des 5 GHz-Bandes wurde das Modulationsverfahren in den 2.4 GHz-Bereich übertragen und als 802.11g-Norm festgeschrieben. 802.11 g stellt den Stand der Technik bei WLAN-Technologie der 802.11-Gruppe dar.

Im Nachfolgenden werden die wesentlichen Aspekte des 802.11-Alphabets in Kürze beschrieben, wobei die Reihenfolge der Buchstaben nichts mit der zeitlichen Entwicklung zu tun hat. Heute aktuell sind 802.11g und h für die Übertragung sowie 802.11i für die Sicherheit und 802.11d, e und f für die Koordinierung von WLAN-Systemen.

Protokolle

Zunächst sind noch einige grundsätzliche Verfahren zum Kanalzugriff in 802.11 Netzwerken vorwegzuschicken, um die grundlegende Funktionsweise deutlich zu machen. IEEE 802.11-Netzwerke

können unterschiedliche MAC-Zugriffe implementieren.

Standard bei WLAN ist die Bereitstellung von asynchronen Datendiensten. Anstehende Datenpakete werden nach dem »Best-Effort«-Prinzip versendet. Prinzipiell ist zusätzlich sowohl Broadcast als auch Multicast möglich. Für die asynchronen Datendienste wird ein DFWMAC-DCF- oder CSMA/CA-Verfahren für den Kanalzugriff implementiert.

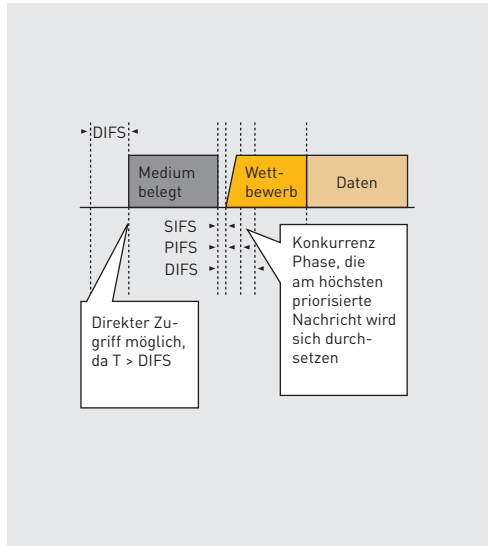
Eine sendewillige Station beobachtet die Luftschnittstelle daraufhin, ob ein Träger vorhanden ist. Ist für eine Zeit großer DIFS (Distributed Coordination Function Interframe Spacing) der Kanal nicht belegt, kann sofort mit dem Senden begonnen werden. Ist das Medium belegt, warten die Stationen, bis der Kanal frei ist. Für eine zerstö-

rungsfreie Arbitrierung warten die konkurrierenden Stationen den SIFS (Short Interframe Space) ab, der für Arbitrierungsnachrichten wie Bestätigungsmeldungen reserviert ist. Dann können zeitlich begrenzte Dienste mittels PCF (Point Coordination Function) innerhalb des PIFS (Point Coordination Function Interframe Space) gestartet werden. Anschließend beginnt, nach Ablauf des DIFS, die Konkurrenzphase der niedrig priorisierten Stationen. Um ein gleichzeitiges Senden zu vermeiden, wird ein Zufallszähler gestartet (Backoff-Algorithmus), der einen zufälligen Medienzugriff garantiert.

Neben dieser Standard-Zugriffsart können optional noch RTS-CTS gesteuerte CSMA-CA-Zugriffe, oder Polling-Verfahren (MAC-PCF) implementiert sein, die jedoch nicht mit jeder Hardware verfügbar sind.

Das DFWMAC-DCF-Verfahren mit RTS-CTS-Steuerung dient der Vermeidung des Hidden-Station-Problems. Möchte eine Station Daten transferieren, sendet sie zuerst ein RTS-Signal (Ready To Send) aus. Innerhalb des SIFS wird der empfangswillige Knoten ein CTS-Signal (Clear To Send) aussenden, wodurch alle in der Reichweite der beiden Knoten befindlichen Stationen über den Datentransfer unterrichtet sind. Nach dem Empfang des CTS gehen die Stationen in den NAV-CTS-Mode in dem sie nur noch ein Acknowledge (ACK) der Kommunikation abwarten und erst dann wieder aktiv werden.

Beim MAC-PCF (Point Coordination Function) handelt es sich um ein optionales Verfahren für die Bearbeitung von zeitkritischen Diensten mit einem priorisierten Zugriff. PCF ist nur im Infrastrukturmodus verfügbar. Der Access-Point koordiniert den Zugriff auf das Medium in festen Zeitintervallen. Innerhalb des CFP-Zeitrahmens arbeitet der Access-Point eine Pollingliste mit verschiedenen explizit angemeldeten Knoten innerhalb eines priorisierten Zeitrahmens ab. Für die



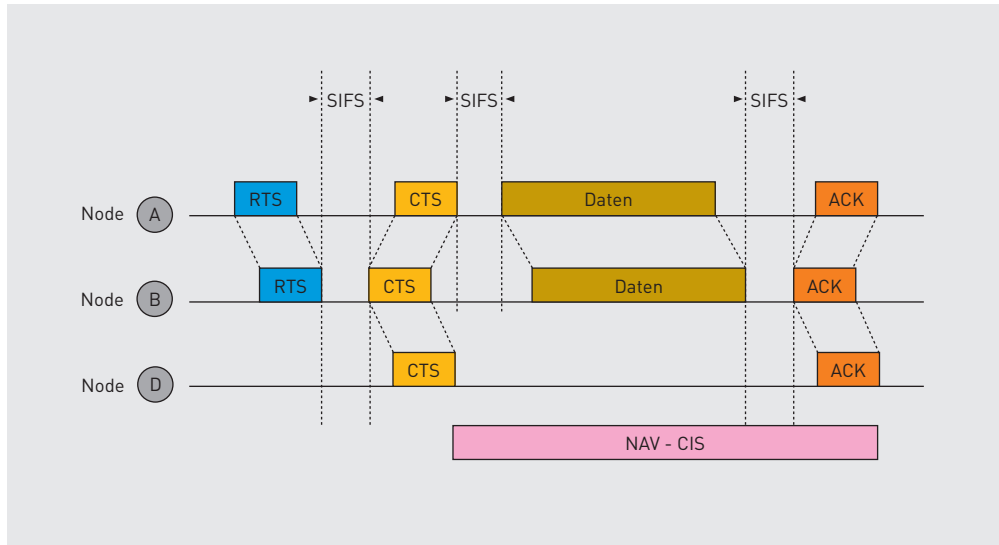
Medien-Zugriff mit CSMA/CA-Verfahren

Dauer des Pollzyklus sind die anderen Stationen von der aktiven Kommunikation ausgeschlossen. Nach Abschluss des PCF können die wettbewerben Knoten am Datenaustausch teilnehmen. Die MAC-PCF-Funktion wird nicht von allen Geräten unterstützt und muss explizit angewendet werden.

IEEE 802.11a

Die Norm 802.11a für bis zu 54 Mbps im 5 GHz-Band wurde 2002 ratifiziert. Erste Produkte waren ab Mitte 2003 verfügbar. Die besonderen Vorteile von 802.11a liegen in der Nutzung des wenig verwendeten 5 GHz-Bandes, das weitaus weniger belastet ist als das 2,4 GHz-Band sowie am OFDM-Modulationsverfahren, das eine bis zu fünfmal höhere Symbolrate als DSSS zulässt, allerdings auf Kosten des Störschutzes bei der Koexistenz der Systeme.

Die Norm bietet weitaus mehr parallel existierende Datenkanäle als die 802.11b Norm mit nur drei nicht überlappenden Kanälen. Doch auch hier er-



Vermeidung von Hidden-Station Problemen durch RTS-CTS-Signale

geben sich einige Probleme. In den Hauptmärkten USA und Europa sind die Kanäle und Sendeleistungen nicht harmonisiert, so dass mit sehr starken Unterschieden in den Produkteigenschaften innerhalb der jeweiligen Produktzonen gerechnet werden muss.

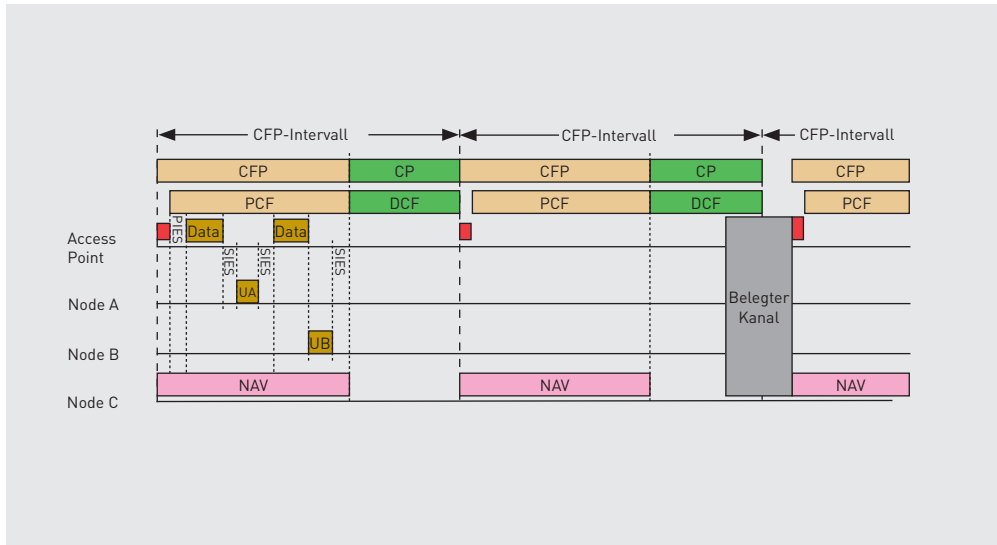
Darüber hinaus darf nicht vergessen werden, dass die Datenrate stark entfernungsabhängig ist. Eine Brutto-Datenrate von 54 Mbps ist nur in einem Umfeld von wenigen Metern erreichbar. Bei großen Entfernungen (größer 70 m) ist ohnehin nur noch mit einer Datenrate von wenigen Mbps zu rechnen. Schließlich darf nicht nur die Bruttodatenrate betrachtet werden: 802.11a bietet eine maximale Netto-Datenrate von 15 Mbps im Hochgeschwindigkeitsmodus.

Betrachtet man die Entwicklung, so steht 802.11a deutlich im Wettbewerb zu den Highspeed-Varianten 802.11g und dem europäischen HyperLAN2, das bei gleicher Symbolrate einen wesentlich höheren Nettodurchsatz von bis zu 40 Mbps zulässt.

IEEE 802.11b

802.11b stellt den De-facto-Standard für Wireless LAN dar und wurde 1999 fertig gestellt. Heute findet man WLAN-Komponenten nach 802.11b standardmäßig in mobilen Endgeräten mit Centrino-Technologie oder in vielen kompakten Endgeräten bis hin zum PDA und Mobiltelefon. Die Datenübertragung erfolgt in bis zu 14 überlappenden, 25 MHz breiten Kanälen im 2,4 GHz-ISM-Band. Je nach Modulationsverfahren können Datenraten von bis zu 11 Mbps erreicht werden. Erweiterungen der Spezifikation lassen auch Übertragungsraten bis zu 22 Mbps zu.

Um eine große Störfestigkeit zu erreichen, werden die Signale im DSSS-Verfahren übertragen. Das bedeutet, dass die Nutzinformationen mit einer 11-Bit Pseudo-Zufallsfolge aufgespreizt werden, so dass potentielle Störungen beim Empfänger um 10,4 dB unterdrückt werden können. Den Vorteilen der Kanalspreizung stehen die Einschränkung von nur drei überlappungsfreien Kanälen gegenüber.



PCF ermöglicht eine Bearbeitung priorisierter zyklischer Nachrichten

Häufig erwähnte Vorteile von WLAN sind die hohe Datenrate und die große Reichweite. Hier muss man sehr vorsichtig sein. Auch bei WLAN nach 802.11b ist die Datenrate sehr stark von dem verwendeten Modulationsverfahren und der Entfernung abhängig. Darüber hinaus ist auch die Nettodatenrate wesentlich von der Modulation abhängig.

Ein weiterer wesentlicher Vorteil von 802.11b ist die Möglichkeit der Zertifizierung der Interoperabilität von Geräten unterschiedlicher Hersteller. Hierzu haben sich etliche WLAN-Hersteller zur WECA (Wireless Ethernet Compatibility Alliance) zusammengeschlossen. Die WECA ermöglicht durch genau definierte Testszenarien den Nachweis der Interoperabilität und weist diese durch das Wi-Fi-Logo nach (Wi-Fi – Wireless Fidelity). Wi-Fi wird häufig synonym mit 802.11b verwendet, was aber nicht richtig ist. Wikipedia widerspricht der Definition, daß Wi-Fi Wireless Fidelity bedeutet. Zitat: »Wi-Fi ist ein für Marketingzwecke erfundener Kunstbegriff, er steht nicht für »Wireless Fide-

lity«, wie man gemäß populärer Analogie z. B. zu Hi-Fi annehmen könnte. Allerdings wurde er von der Wi-Fi Alliance sehr wohl als Wortspiel zu »Hi-Fi« aufgefasst.«

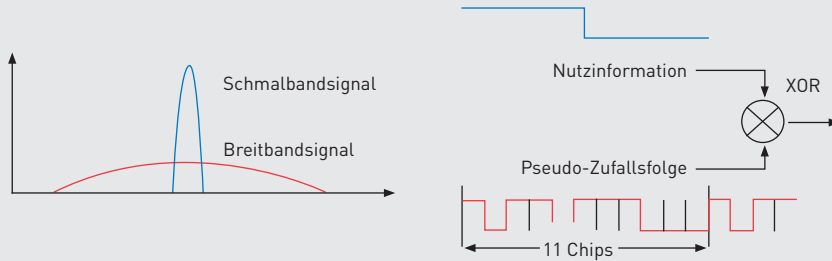
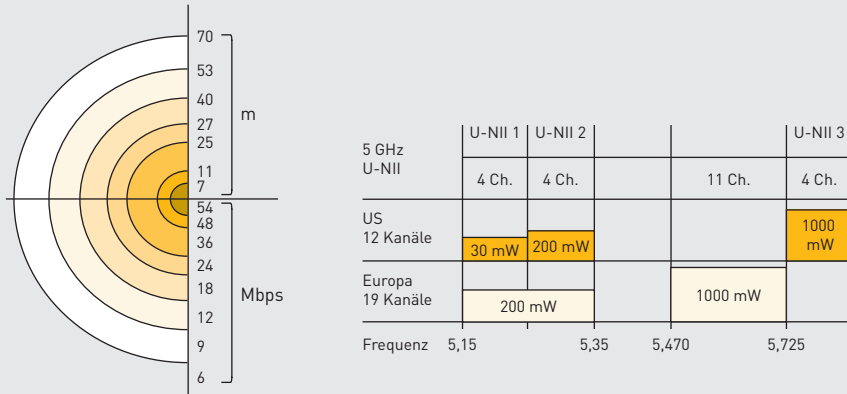
Spezielle Entwicklungen werden in den 802.11b+-Standards definiert. Hierbei werden u. a. rückwärts kompatible Übertragungsstandards mit einer Datenrate bis hin zu 108 Mbps realisiert.

IEEE 802.11d

Um die nationalen Besonderheiten hinsichtlich der Frequenzeinteilung und der Sendeleistung zu berücksichtigen, wurde der d-Standard formuliert. Ziel ist es, weltweit dieselben Access-Points durch Länderkennung zu parametrieren, so dass nur durch eine Softwareanpassung die regional zulässigen Betriebsparameter eingehalten werden.

IEEE 802.11e

Die 802.11e-Spezifikation ist eine geplante Erweiterung für die Bereitstellung von definierten

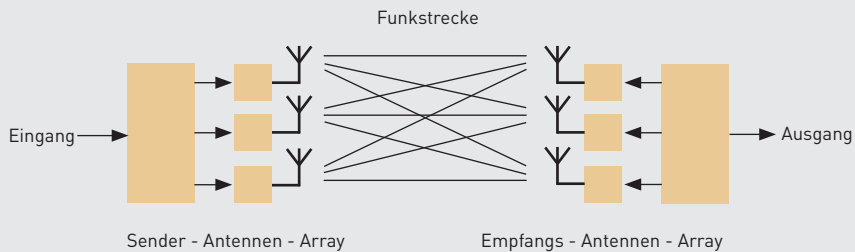


Oben: Frequenzbereiche und Datenraten bei IEEE-802.11a-Netzwerken

Unten: IEEE 802.11b nutzt ein 22 MHz-DSSS-Signal

Rate	Modulation
1 MBps	DBPSK Differential Binary Phase Shift Keying
2 MBps	DBQSK Differential Quadrature Phase Shift Keying
5,5 MBps	CCK Complementary Code Keying
11MBps	CCK+DQPSK
22 MBps	OFDM Orthogonal Frequency Division Multiplexing

	11 Mbps	5 Mbps	2 Mbps	1 Mbps
Freifeld	150 m	250 m	300 m	400 m
Gebäude	30 m	35 m	40 m	50 m
Nettorate	5,04 Mbps	4,33 Mbps	1,59 Mbps	0,82 Mbps
Effizienz	46%	62%	79%	82%



Oben: Modulation und Nettodatenraten bei IEEE 802.11b

Unten: IEEE 802.11n nutzt ein MIMO-System für eine bessere korrelierte Signalstärke

Dienstgütern für Voice over IP (VoIP) oder andere zeitkritische Dienste, die einen isochronen Datentransfer benötigen. Die MAC-Erweiterung 802.11e ermöglicht eine erweiterte PCF-Funktionalität, wobei den Stationen eine definierte Bandbreite zugewiesen wird. Im Wesentlichen erfolgt die Adaption der ETSI-Hiperlan/2-Spezifikation auf die IEEE 802.11-Standards.

IEEE 802.11f

Das Finden von mobilen Stationen in einem Infrastrukturnetzwerk war lange Zeit der Implementierung einzelner Hersteller vorbehalten. Erst der 802.11f-Standard ermöglicht durch die Definition eines Inter-Access-Point-Protokolls (IAPP), den standardisierten Datenaustausch zwischen den Infrastrukturkomponenten.

IEEE 802.11g

Eine bedeutende Entwicklung zeichnete sich 2003 durch die Verabschiedung des 802.11g-Standards ab. Er bietet eine Kompatibilität zum bisherigen 802.11b-Standard. Hierzu gehört die Rückwärtskompatibilität zu den bisherigen Infrastrukturkomponenten als auch die Nutzung des weltweit verfügbaren 2,4 GHz-ISM-Bands. 802.11g übernimmt Signalkodierungsverfahren aus der 802.11a-Welt (OFDM) und ermöglicht damit zusätzliche 22 bis 54 Mbps-Betriebsmodi.

IEEE 802.11h

Beim 802.11h-Standard handelt es sich im Wesentlichen um eine Erweiterung des bisherigen 802.11a-Standards im 5 GHz-Band um die technischen Eigenschaften der europäischen ETSI HiperLAN/2-Spezifikation. In erster Linie werden zusätzliche Modulationsverfahren mit einer höheren Kanaleffizienz, ein Spektrum-Management für das Ausblenden von Radarfrequenzen sowie das Management der Sendeleistung vorgesehen.

IEEE 802.11i

Der Sicherheit von WLAN könnte man ein eigenes Buch widmen, so viel wird über Sicherheitslücken

und Gegenmaßnahmen diskutiert. Generell kann man feststellen, dass es mit der WLAN-Sicherheit nicht zum Besten steht. Hierzu tragen im Wesentlichen zwei Aspekte bei.

- Die Zugriffskontrolle ist unsicher, da die MAC-Adressen bei der Kommunikation unverschlüsselt übertragen werden und damit eine eindeutige Sender-Empfänger-Zuordnung identifizierbar ist. Angreifer können sich durch das Vorspielen »richtiger«-MAC-Adressen in ein Netz einschleichen.
- WEP-Schlüssel können mit verhältnismäßig wenig Aufwand ersniffed/aufgeklärt werden, da sie statisch sind. Durch das Mitschneiden mit entsprechenden Tools ist der Schlüssel ohne großen Aufwand innerhalb weniger Minuten rekonstruierbar.

Die 802.11i beschreibt eine Erweiterung der Standards 802.11 a, b und g, um die Lücken des WEP-Verfahrens (Wired Equivalent Privacy) zu schließen. Hierzu gehört die Authentifizierung der Stationen mittels EAP (Extensible Authentication Protocol). EAP verwendet verschiedene Authentifizierungsmechanismen, wobei ein RADIUS-Server (Remote Authentication Dial In User Service) erforderlich ist. Für die Sicherung der Schlüssel wird in 802.11i die Verwendung von TKIP (Temporary-Key-Integrity-Protocol) empfohlen. Hierbei wird der statische Schlüssel umgangen, indem pro Datenpaket ein neuer Schlüssel erzeugt wird. Ein Abhören ist zwar weiterhin möglich, nicht jedoch die Rekonstruktion des Schlüssels. WIFI-konforme Systeme setzen eine Sicherung nach 802.11i voraus. Sie muss jedoch auch eingeschaltet werden, denn Sicherung ist immer optional.

IEEE 802.11n

Aktueller Stand der Technik bei IEEE 802.11 ist der Standard n. Der erste Entwurf wurde im Januar 2006 verabschiedet und sofort in unterschiedlichen Produkten übernommen, noch bevor der Standard abschließend ratifiziert wurde. Dieses



37

101

101

R41

101

R46

101

C2

R54

R55

R56

102

153

35

R112

35

R57

C65

47P

R47

47P

C77

100

C78

C80

100

C88

100

L12

C53

C50

C157

C158

führte zu so genannten Draft-n-Produkten. Seit Oktober 2009 ist der Standard endgültig veröffentlicht und bietet eine Übertragungsgeschwindigkeit von bis zu 600 MBps.

Eine deutliche Verbesserung gegenüber den bisher etablierten 802.11 g- oder a-Standards erfolgte durch die Nutzung von so genannten MIMO-Antennenarrays. MIMO (Multiple Input Multiple Output)-Anordnungen ermöglichen eine Mehrfachnutzung eines Datenkanals im selben Frequenzbereich, was zu einer größeren Reichweite oder einer höheren Datenrate führt.

Für die Modulation nutzt der n-Standard OFDM (Orthogonal Frequency Division Multiplex) mit bis zu 58 OFDM-Trägern. Die einzelnen Träger können, je nach Leitungsqualität, mit BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying) oder mit QAM (Quadrature Amplitude Modulation) moduliert werden. Während konventionelles WLAN auf eine spektrale Effizienz von bis zu 5 Bit pro Hz kommt, erreicht IEEE 802.11n bis zu 20 Bit pro Herz. Durch die Option der Kanalbündelung auf 40 MHz-Bandbreite kann eine Bruttodatenrate von bis zu 600 Mbps erreicht werden. Die erreichbare Nettodatenrate liegt allerdings deutlich niedriger. Durch die zusätzlich erforderliche Redundanz ist eine realistische Nettodatenrate von maximal 74 bis 248 Mbps möglich.

Außerdem nimmt mit der steigenden spektralen Effizienz die Verwundbarkeit gegenüber Störern in gleichem Maße zu, wodurch die Simultanzahl gleichartiger Netze, die Koexistenz im selben Frequenzband sinkt.

// Koexistenz und Sicherheit

09

Koexistenz im 2,4 GHz-Band

Echtzeit in kabellosen Netzwerken

IEEE 802.11 – WLAN

WLAN-Seitenbandverhalten

Bluetooth® und WLAN

Koexistenzmanagement

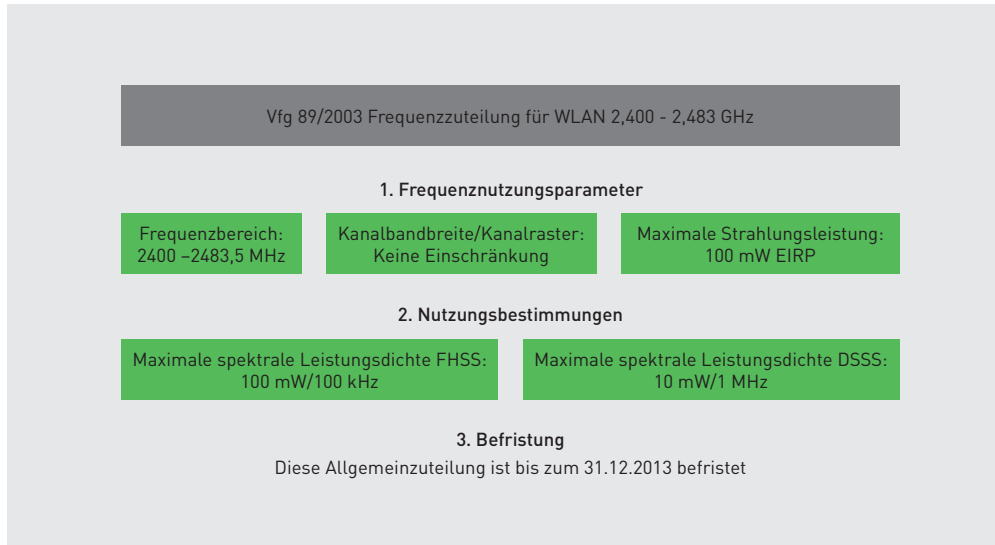
Leistungsparameter

Koexistenzplanung

Sicherheit

Funktionale Sicherheit

Informationssicherheit - Security



Frequenzzuteilung für WLAN

// Koexistenz im 2,4 GHz-Band

Unter Koexistenz versteht man im Allgemeinen die konfliktfreie Anwesenheit und den störungsfreien Betrieb unterschiedlicher Systeme an einem Ort. Häufig wird hierfür auch der Begriff Kompatibilität genannt. Beim Funk ist dies gar nicht so einfach zu realisieren. Funksignale sind mit den menschlichen Sinnen nicht wahrnehmbar, und vor allem sind eine Vielzahl unterschiedlicher Systeme im selben Frequenzband unterwegs. Um eine konfliktfreie Koexistenz sicherzustellen, hat der Betreiber der Funkanlagen die Verantwortung, den Einsatz der unterschiedlichen Systeme im Vorfeld zu bewerten und zu planen. Das heißt, an Stelle der Funkkoordinierung durch die Bundesnetzagentur tritt hier die Pflicht zur Koordinierung durch die Betreiber.

Die gleichzeitige Anwesenheit der zwölf in der Tabelle aufgeführten Funkdienste im gleichen Frequenzbereich muss aber nicht zwingend und unmittelbar zu Störungen führen. Verschiedene

Maßnahmen können getroffen werden, um das Spektrum mehrfach zu nutzen. Viele Techniken nutzen von sich aus schon die unterschiedlichsten Mechanismen. Die Möglichkeiten der Diversifikation von Frequenz, Zeit und Code wurden bereits vorgestellt, ebenso die räumliche oder zeitliche Trennung. An dieser Stelle soll nun auf besondere Aspekte des WLAN eingegangen werden.

Die Bundesnetzagentur hat mit Verfügung 89 / 2003 spezielle Regelungen für solche WLAN-Funknetze erlassen, die Frequenzsprung- oder Frequenzpreisverfahren anwenden.

Darauf aufbauend wurden für Short Range Devices SRD-Technologien entwickelt und standardisiert, die nun im Frequenzband 2400 – 2483,5 MHz miteinander konkurrieren.

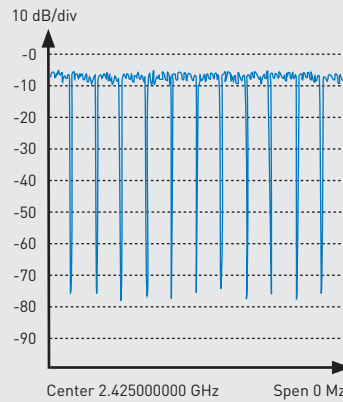
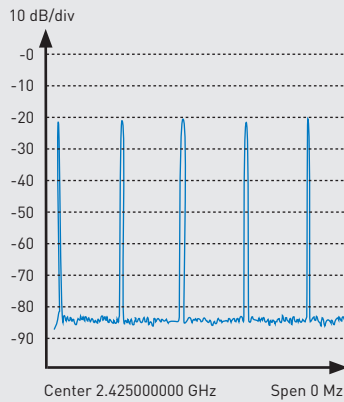
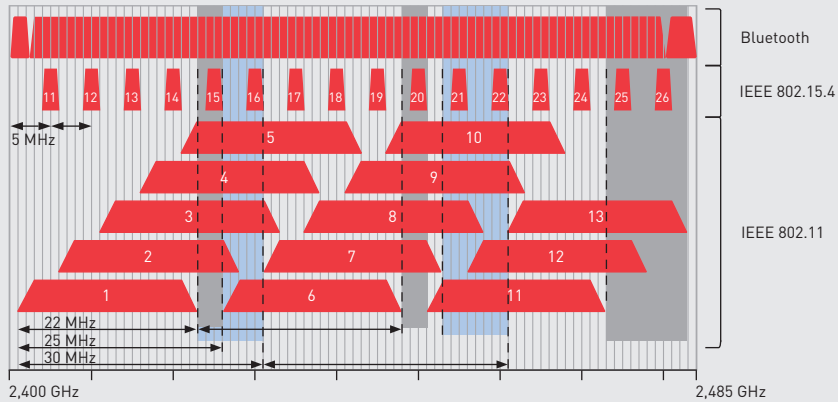
Die Frequenzsprungverfahren setzen sich einmal mit ihrer relativ hohen spektralen Leistungsdichte und zum anderen mit ihrer Frequenzagilität gut durch. Hierbei können sie im teilbelegten

Funkdienste	Maximal zulässige äquivalente Strahlungsleistung	Auflagen
Allgemeine Funkanwendungen geringer Reichweite;	10 mW EIRP	
Demonstrationsfunk für Bildungseinrichtungen	5 W ERP	
Fernwirkfunk Übertragung von Datensignalen	10 W ERP	Kanalraster 2,5 MHz Kanalbandbreite 2,5 MHz
WLAN Breitbandige Datenübertragung	100 mW EIRP	bezogen auf das Band 2400-2483,5 MHz
Amateurfunkdienst		Amateurfunkgesetz § 6 Satz 1
Amateurfunkdienst über Satelliten		Amateurfunkgesetz § 6 Satz 1
Militärischer Mobilfunkdienst		
Reportagefunk Übertragung von Bild- und Ton	27 dBW EIRP (500 W);	üblich 13 dBW Senderausgang (20 W)
Funkbewegungsmelder geringer Reichweite, Geschwindigkeits-, Abstandsmessung	25 mW EIRP	
Mil. Nichtnavigatorischer Ortungsfunkdienst		
Identifizierungszwecke	500 mW EIRP ausserhalb 4 W EIRP innerhalb Gebäuden	
Öffentliche Eisenbahnen Automatische Fahrzeugidentifizierung	500 mW EIRP	B= 1,5 MHz

Frequenznutzung im 2,4 bis 2,5 GHz Bereich gemäß FreqNPI, Teilpläne 276 und 277

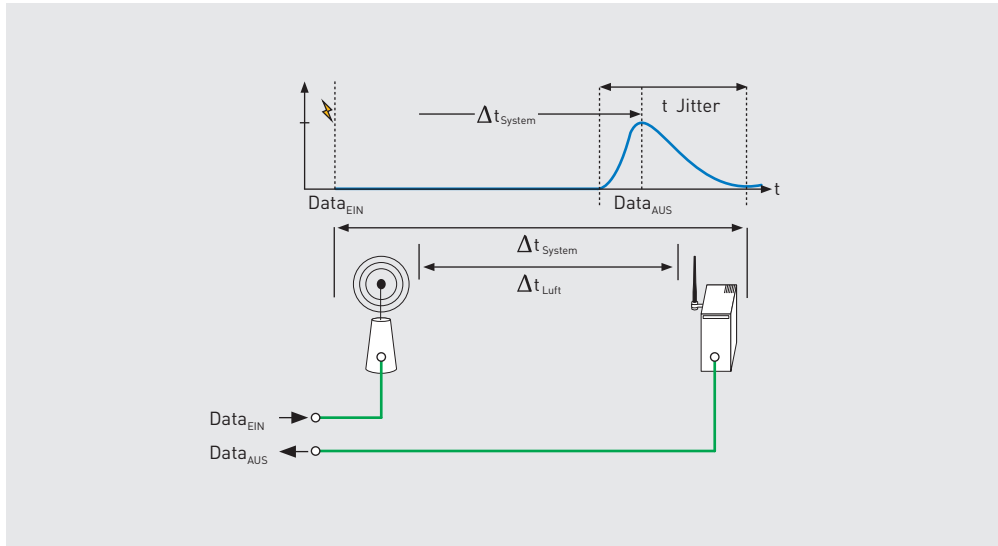
2,4 GHz-Band freie Lücken bevorzugt ausnutzen. Allerdings können sich die FHSS-Netze gegenseitig stören, da sie durch ihre stochastische Frequenz-/Kanalwahl bei steigender Netzzahl mit zunehmenden Kollisionen rechnen müssen, die erfahrungsgemäß bei einer Auslastung von 40 % der theoretisch 79 möglichen Piconetze deutlich spürbar werden.

Im Gegensatz dazu besteht der Vorteil der Direktsequenz-Spreizverfahren darin, dass sie beim Entspreizen ihres Nutzsignals im 22 MHz breiten Kanal zugleich alle Störsignale im gleichen Spreizverhältnis unterdrücken. Das sind bei den gängigen Spreizverfahren mit 11 bis 32 Chips pro Nutzbit Werte von 10,5 bis 15 dB als Spreizgewinn. Daher stören sich die DSSS-Netze gegenseitig



Oben: Frequenzbelegung einiger populärer Techniken im 2,4 GHz-Band

Unten: Oszillogramme von 10 % (links) und nahezu 100 % (rechts) Kanalnutzung (Duty-Cycle)



Bei Funksystemen muss das Gesamtsystem und nicht nur die Luftschnittstelle betrachtet werden.

erst dann, wenn der Summenpegel des »Störteppichs« um diese 10,5 bis 15 dB über dem Empfangspegel des Nutzempfängers liegt. Die DSSS-Netze gelten daher als sehr robust gegenüber Störungen. Eine wichtige Rolle spielt hierbei noch die Auswahl eines günstigen Spreizcodes, weil dieser zugleich über die Kreuz- und Autokorrelation der digitalen Signalverarbeitung die dem Nutzsignal gleichartigen Störsignale unterdrücken hilft.

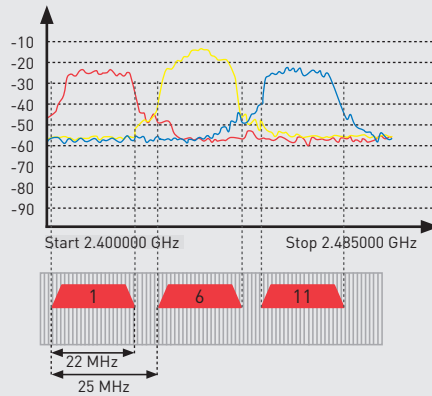
In dem Störszenario FHSS gegen DSSS wird FHSS wegen der um 20 dB höheren spektralen Leistungsdichte wohl nur unwesentlich beeinflusst. Ebenso wird DSSS durch FHSS auch nur unwesentlich gestört, hier wirken sich der Spreizgewinn, die auf die 22 MHz entfallende geringere Kanalzahl von FHSS und dessen kurze Verweilzeiten auf der jeweiligen Frequenz günstig aus. Eine belastbare Bewertung des Störverhaltens in beiden Szenarien hängt aber von weiteren ungünstigen Rahmenbedingungen, vor allem von dem tatsächlich örtlich vorliegenden Szenario und sei-

ner Funkfeldbelastung ab. Man darf aber davon ausgehen, dass im allgemeinen Fall die beiden Systeme FHSS und DSSS miteinander koexistieren werden. Das wird nun näher betrachtet.

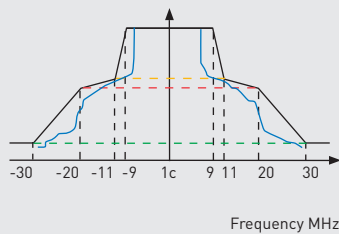
Zunächst erscheint es erschreckend, dass eine Überlappung unumgänglich ist. Selbst innerhalb einer Technologie wie z. B. WLAN nach IEEE 802.11 überschneiden sich die verfügbaren Kanäle.

Störend ist die Überlappung nur dann, wenn die Kanäle auch wirklich für die Datenübertragung genutzt werden. Die pure Existenz sich potenziell überlappender Kanäle ist nicht schädlich.

Ein wichtiges Kriterium ist hierbei die Kanallast, die auch mit dem Duty-Cycle beschrieben wird. Bei einer geringen Kanallast ist rein statistisch die Wahrscheinlichkeit der Interferenz zwischen unterschiedlichen Funksystemen im selben Frequenzbereich sehr gering. Erst bei einer großen Kanalauslastung erfolgt eine signifikante Beeinflussung der jeweiligen Funktechnologien. Das



-20 dBr - - - -
 -25 dBr - - - -
 -40 dBr - - - -



Oben: WLAN-Kanäle 1,6 und 11 im Frequenzscan

Unten links: WLAN-Kanalmaske für den IEEE-802.11g-Standard

Unten rechts: Störungsverhalten IEEE 802.15.4 auf Kanal 15 und 20 parallel zu IEEE 802.11g Kanal 6

wird in den weiteren Betrachtungen noch deutlich werden.

// Echtzeit in kabellosen Netzwerken

Neben der Duty-Cycle-Betrachtung spielt bei der Bewertung der Performance von Funkstrecken das Gesamtsystem eine bedeutende Rolle. Die Systemlaufzeit setzt sich hierbei zusammen aus der Übertragung über die Luftschnittstelle und der Bearbeitung der Datenpakete durch das technische System. Es wird also immer eine systembedingte Verzögerung sowie eine Jitter-behaftete Übertragung vorliegen. Der Jitter ist im Wesentlichen durch Sendewiederholungen auf der Luftschnittstelle bedingt und wird in einer mit Störungen belasteten Umgebung steigen. Da hier zwei asynchrone Prozesse miteinander arbeiten, wird die Verteilungsfunktion voraussichtlich einer Raleigh-Verteilung folgen.

Für eine deterministische Übertragung muss in einem System sichergestellt werden, dass der Jitter im Verhältnis zu der Systemzeit t_{system} sehr klein ist. Darüber hinaus sollte die Systemzeit deterministisch und im Verhältnis zur Systemdynamik zu vernachlässigen sein.

// IEEE 802.11 – WLAN

Wie aus einer vorhergehenden Abbildung deutlich wird, sind von den dreizehn WLAN-Kanälen nur drei nicht überlappend. Das sind entweder die Kanäle 1, 6 und 11, 2, 7 und 12 oder 3, 8 und 13. Eine entsprechende Frequenzplanung würde sicherstellen, dass sich die Kanäle theoretisch nicht stören. In der Realität sieht das etwas anders aus. Schon das folgende Oszillogramm realer Funkssysteme zeigt eine deutliche Überlappung der Frequenzbänder.

Dabei stören sich die DSSS gespreizten 22 MHz-Kanäle nicht gegenseitig, wohl aber die anderen Nutzer. Diese gespreizten Kanäle werden durch

digitale Kreuzkorrelation und Autokorrelation gut voneinander getrennt.

Es ist offensichtlich, dass die 22 MHz-Bandbreite eines WLAN-Kanals reine Theorie sind. In der Realität ist die Kanalmaske deutlich breiter und dazu noch von der Modulationsart abhängig. Ein 802.11b-Kanal hat damit eine deutlich andere Maske als ein 802.11g-Kanal. Diese unterschiedlichen Eigenschaften kann man sich zunutze machen – oder man muss mit den Einschränkungen leben.

// WLAN-Seitenbandverhalten

Betrachtet man die theoretische Kanalnutzung im 2,4 GHz-Band, dann müssten die IEEE-802.15.4-Kanäle 15 und 20 vollkommen störungs- und interferenzfrei zum WLAN Kanal 6 betrieben werden können (siehe Bild Seite 144 Mitte).

In einer Referenzmessung wurden die Round-Trip-Zeiten von einem Steuerungssystem mit einer Zykluszeit knapp oberhalb einer Millisekunde über eine IWLAN-Strecke auf Kanal 6 im Betriebsmodus g – also mit OFDM-Modulation – betrieben. Die Statistik zeigt eine erfreulich kurze Reaktionszeit.

Werden nun die IEEE 802.15.4-Systeme parallel mit unterschiedlichen Duty-Cycles betrieben, ändert sich das Antwortverhalten signifikant. Während bei einem Duty-Cycle von 10 % eine Veränderung kaum spürbar ist, tritt bei 50 % Duty-Cycle ein deutlich merkbarer Anstieg der Round-Trip-Zeit auf. Senden die IEEE 802.15.4-Systeme mit einer maximalen Netzlast, kann das WLAN-System komplett zum Abbruch gebracht werden.

In der vorhergehenden Tabelle ist deutlich der Verlauf bis hin zum Kanalabbruch zu bemerken. Allerdings sind die vorgestellten Ergebnisse nicht repräsentativ für alle WLAN-Systeme und alle IEEE 802.15.4 Systeme. Generell soll hier nur ein

Aktive Störer	-	802.15.4	802.15.4	802.15.4
Kanal	-	15	15	15
Kanallast	-	Max	50%	10%
# sent	4500	4500	4500	4500
# error	0	0	0	0
# lost	0	4500	0	0
min [ms]	1,48	-	1,5	1,5
max [ms]	2,59	-	12,67	5,89
avg [ms]	1,57	-	2,7	1,69

Statistische Auswertung bei unterschiedlichen Duty-Cycles

Trend aufgezeigt werden. Eine große Netzbelastung, auch im Seitenband, kann zu einem Abbruch einer Verbindung führen, die eigentlich von der theoretischen Betrachtung her gar nicht stören dürfte. Das ist die schlechte Nachricht. Die gute Nachricht ist, dass eine geringe Netzlast < 10 % so gut wie keinen Einfluss auf die Übertragung hat. Auch überlappende Kanäle mit einem kleinen Duty-Cycle werden rein statistisch keine dramatische gegenseitige Störung erzeugen.

Daraus die Konsequenz zu ziehen, dass man einen größeren Mindestabstand zwischen Funkkanälen definiert, wäre nicht hilfreich. Das soll ein weiteres Extrembeispiel zeigen. Werden die WLAN-Kanäle 5 und 6 parallel betrieben, dann könnte man meinen, dass nur eine unzureichende Kommunikation möglich ist.

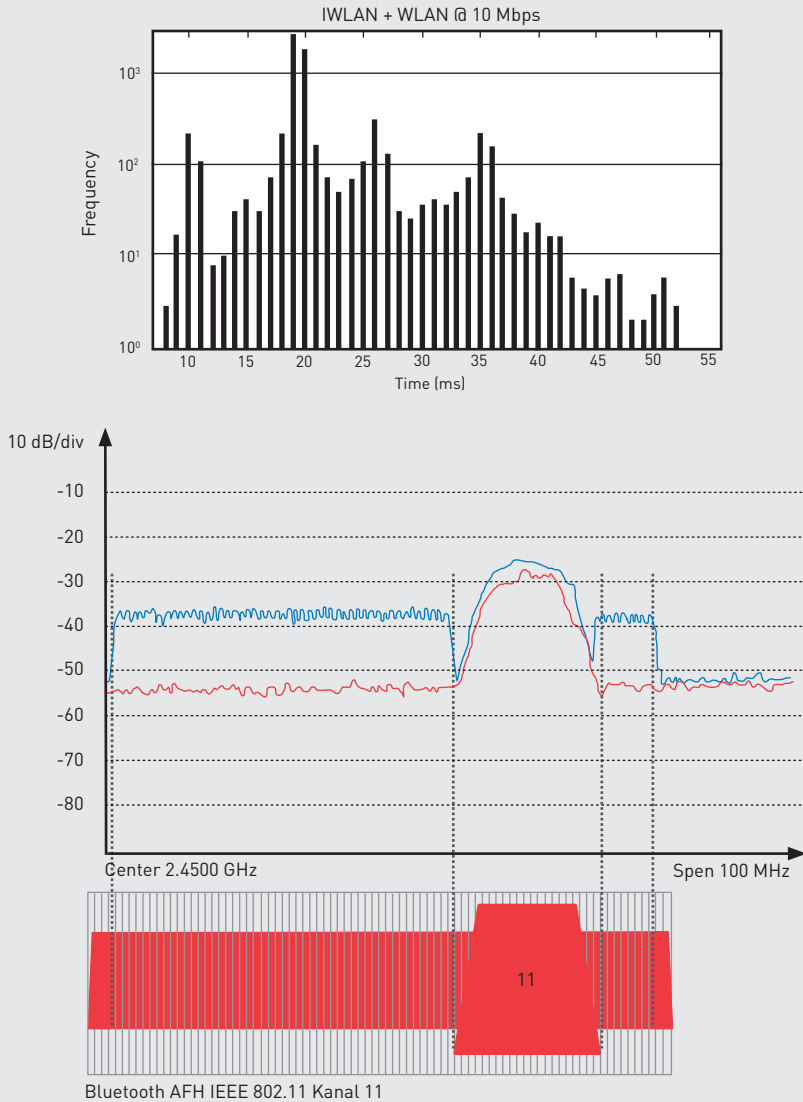
Das ist aber nur zum Teil richtig. So lange die beiden Funkstrecken nur einen hinreichend kleinen Duty-Cycle haben, wird kaum ein Kommunikationseinbruch bemerkt. Selbst die Steigerung der

Kommunikationslast auf 50 % Duty-Cycle (10 Mbps netto @ 54 Mbps brutto) führt gerade einmal zu einer Verdopplung des Kommunikationsjitters.

Diese Werte können nicht verallgemeinert werden. Sie zeigen jedoch, dass auch bei sich überlappenden Kanälen und moderatem Duty-Cycle eine fehlerfreie Kommunikation möglich ist. Würde man jedoch die Kommunikationslast weiter steigern, können ab etwa 75 % beliebige Busfehler und Verbindungsabbrüche generiert werden.

// Bluetooth® und WLAN

Bluetooth nutzt als Modulationsverfahren FHSS (Frequency Hopping Spread Spectrum). Jede Bluetooth-Station wechselt ihre Frequenz mit 1.600 Hops pro Sekunde. Diese Frequenzwechsel erfolgen in einer pseudozufälligen Sequenz, die durch die 48 Bit-Bluetooth-Adresse und einem internen 23 Bit-Zähler bestimmt ist und eine Peri-



Oben: Auch bei überlappenden Kanälen steigen der Jitter und die Round-Trip-Zeit mit der Kanallast an.

Unten: Bluetooth AFH ermöglicht automatisch das Ausblenden belegter Kanäle. Hier wird deutlich sichtbar der WLAN-Kanal 11 ausgeblendet.

ode von fast 24 Stunden aufweist. Jedes Bluetooth-Gerät hat damit seinen eigenen Datenkanal. Eine Kommunikation kommt nur dann zustande, wenn ein Gerät mit anderen ein Piconetz bildet. Das bedeutet: Der Master gibt den anderen Kommunikationsteilnehmern seine Bluetooth-Adresse und sein Timing mit.

Frequency Hopping vermeidet Störungen

Aufgrund der Kanaldefinition könnten innerhalb der Funkreichweite theoretisch 78 Piconetze konfliktfrei koexistent sein. Tatsächlich aber stören sich die stochastisch über die 78 Kanäle springenden Netze gegenseitig zunehmend, bis bei einer Ausnutzung von ca. 40 %, entsprechend 32 Piconetzen, eine kritische Grenze erreicht wird. Trotzdem hat Bluetooth eine sehr große Kommunikationsdichte und durch den schnellen Frequenzwechsel eine große Robustheit gegenüber schmalbandigen Störern.

Wird das Bluetooth-Piconetz stark ausgelastet, wirkt dies für andere Funkssysteme wie ein stochastischer breitbandiger Störer, im schlimmsten Fall wie ein 78 MHz breites Funksystem mit einem Duty-Cycle von gut 1,28 %. Jedes weitere Piconetz vergrößert den Duty-Cycle um ebenfalls 1,28 %. Bluetooth wird sich in diesem Szenario durchsetzen, aber die anderen Funktechniken werden gestört (siehe Seite 147).

Um dies zu umgehen, ist ab der Version 1.2 AFH (Adaptive Frequency Hopping) in jedem Bluetooth-Gerät implementiert. Wenn Bluetooth durch einen Anstieg der Paketfehler merkt, dass ein Kanal permanent belegt ist, sorgt AFH dafür, dass das belegte Frequenzspektrum vollständig im Hopschema ausgeblendet wird. Wichtig ist hierbei der Begriff »permanent«. Ist eine Funkstrecke nur sporadisch belegt, wird der AFH-Algorithmus nicht zuschlagen und damit auch keine Verbesserung der Kommunikation bewirken. Um eine größere Vorhersagbarkeit zu garantieren, ermöglichen industrielle Bluetooth-Lösungen auch

ein Blacklisting (manuelles Ausblenden potentiell belegter Kanäle) oder Whitelisting (manuelles Erlauben bestimmter Frequenzbereiche).

Referenzmessungen zeigen, dass es bei Bluetooth dank des adaptiven Frequency Hoppings kaum eine Kommunikationseinbuße bei einem parallelen Betrieb mit einem komplett ausgelasteten WLAN-Kanal gibt.

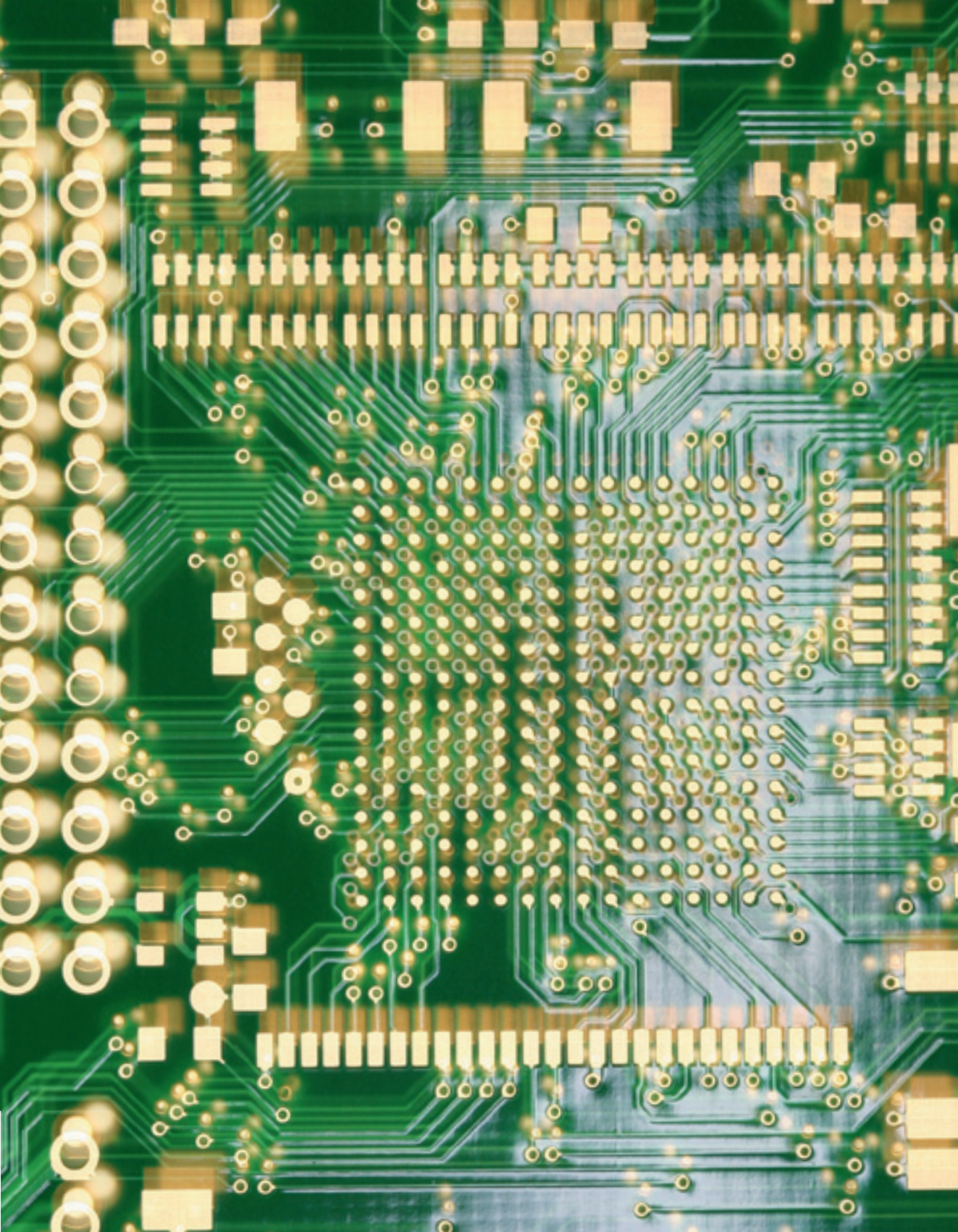
// Koexistenzmanagement

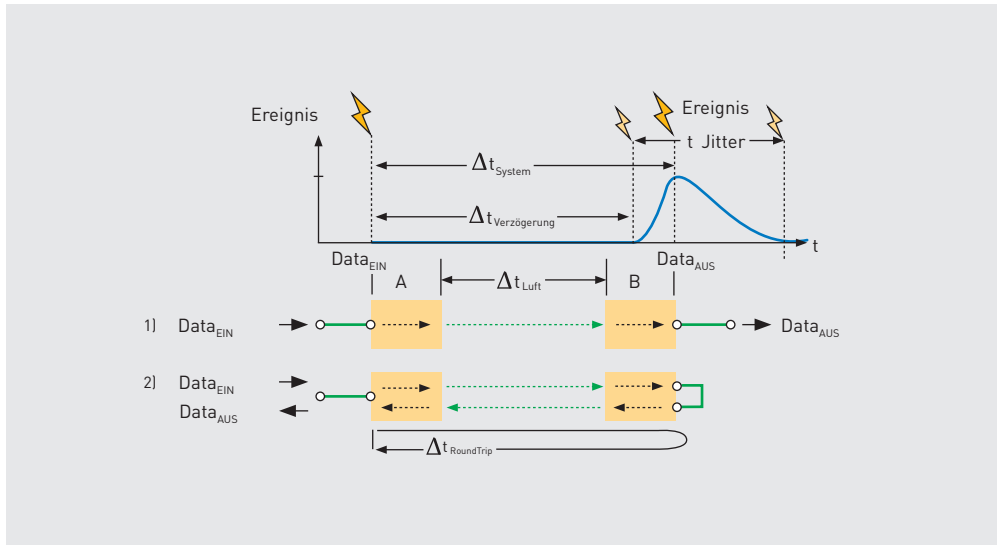
Die vorhergehenden Ausführungen machen deutlich, dass gerade in den freien ISM-Bändern, im Besonderen im 2,4 GHz-Band, ein Management der Frequenzen und der Systeme notwendig ist. Funk darf man nicht sich selbst überlassen. Jeder Accesspunkt und jede Funkstation sollte in einem Anwendungskontext und in seiner Umgebung bekannt sein.

Duty-Cycle als wichtiges Kriterium

Ein weiterer bestimmender Faktor ist die Kanallast. In den vorhergehenden Abschnitten wurde gezeigt, wie stark der Einfluss des Duty-Cycles auf das Übertragungsverhalten von überlappenden und angrenzenden Frequenzbereichen ist. Hierbei kann man generalisierend feststellen, dass eine Kanallast bis zu 10 % als unkritisch anzusehen ist. In der Regel ist ein Einfluss des anderen Kommunikationsteilnehmers dann kaum messbar.

Kritisch wird es ab einem Duty-Cycle von 50 %. Hier ist nahezu immer ein deutlicher Anstieg der Jitterzeiten festzustellen. Dieses ist ein sicherer Hinweis auf Kollisionen, wenn auch die Kommunikation durch Sendewiederholungen geheilt werden kann. Bei einer größeren Kanallast muss auf exklusive Kanalzuteilung und möglichst kommunikationsarme Seitenbänder geachtet werden.





Antwortzeiten in einem zeitvarianten Funkstreckensystem

Die grundlegenden Fragen des Koexistenzmanagements

Die wesentlichen Betrachtungen bei der Funkplanung sind dann die Fragestellungen:

- Welche Funksysteme existieren im Raum?
- Gibt es Funksysteme, die von anderen Abteilungen bzw. Einheiten verwendet werden?
- Sind Consumergeräte mit Funk (Laptop, Mobile, Smartphone, Headset, ...) im Bereich zulässig und wenn ja, welche Dienste und Funktionen werden verwendet?
- Welche Frequenzbereiche werden von den identifizierten Systemen verwendet?
- Gibt es relevante Überschneidungen der unterschiedlichen Frequenzbereiche?
- Welche Daten werden wie häufig über die jeweiligen Kanäle übertragen?
- Kann der Duty-Cycle für die betrachteten Systeme ermittelt werden?
- Gibt es Mindestanforderungen hinsichtlich der Reaktionszeit, Roundtripzeit oder der Datenrate?
- Gibt es Grenzwerte für den Jitter innerhalb des betrachteten Systems?

// Leistungsparameter

Eine ganz wesentliche Rolle bei der Bewertung der Funkstrecken spielen die Leistungsparameter, also die Anforderungen, die an ein System mit Funkübertragungsstrecke gestellt werden. Zwei wesentliche Anwendungsfälle sind hierbei zu unterscheiden: Funkbrücken und bidirektionale Geräte.

Funkbrücken:

Als Funkbrücke bezeichnet man ein System, bei dem ein Knoten A ein beliebiges Ereignis, wie z. B. ein Eingangssignal $Data_{EIN}$ erhält, dieses über die Luftstrecke zu einem Knoten B übertragen wird und dort als Ereignis auf einen Ausgang gelegt wird. In der Regel wird dies wiederum der hoffentlich unveränderte Datenstrom $Data_{AUS}$ sein. Für ein Echtzeitsystem ist es relevant, wann nach einem Ereignis das Ergebnis anliegt. Diese Zeit wird auch als Reaktions- bzw. Systemzeit bezeichnet. Diese setzt sich zusammen aus den Verarbeitungszeiten der Knoten A und B sowie der

Übertragungszeit der Luftschnittstelle. Im besten Fall ist die Übertragung nach einer minimalen Verzögerungszeit abgeschlossen. Wie im vorhergehenden Abschnitt erläutert, wird jedoch bei einem realen System die Systemzeit mit einem Jitter behaftet sein. Dieser wird durch die variable Bearbeitungszeit in den Kommunikationsknoten und durch mögliche Signallaufzeiten und Sendewiederholungen auf der Luftschnittstelle erzeugt. Die zeitlichen Anforderungen an die Funkbrücken werden durch den Prozess bestimmt. Bei Schaltern für die Mensch-Maschine-Kommunikation sind beispielsweise Systemzeiten bis zu 100 Millisekunden akzeptabel; für »Machine-to-Machine«-Anwendungen sind in vielen Fällen Systemzeiten von einigen Sekunden ausreichend.

Bidirektionale Geräte:

Bei bidirektionalen Geräten initiiert ein Knoten A aufgrund eines Ereignisses eine Kommunikation mit einem über die Luftschnittstelle angebundenen Knoten B. Dieser verarbeitet das Ereignis, errechnet ein Ergebnis und transferiert dieses zurück auf den anfragenden Knoten A, der dieses als Antwortereignis zur Verfügung stellt. Die komplette Verarbeitungszeit wird als Round Trip Zeit bezeichnet. Round Trip Zeiten spielen immer dort eine Rolle, wo mit Steuerungen, Sensoren oder Aktoren bidirektional kommuniziert werden muss.

Neben den genannten Größen sind noch weitere Leistungsparameter von Bedeutung:

1. Periode

Als Periode bezeichnet man den Abstand zwischen zwei Kommunikationsereignissen. Handelt es sich um ein Abtastsystem, ist die Periode unbedingt einzuhalten. Liegt ein stochastisches, ereignisgesteuertes System vor, kann keine Periode, sondern höchstens eine Häufigkeit pro Zeiteinheit angegeben werden.

2. Datenmenge

Die Datenmenge beschreibt die Größe eines Telegramms, das bei einem Ereignis übertragen wer-

den muss. Das können bei einem Automatisierungssystem wenige Bits oder Bytes sein. Ebenso sind aber auch große Datenbündel von etlichen 100 bis einige 1000 Bytes möglich.

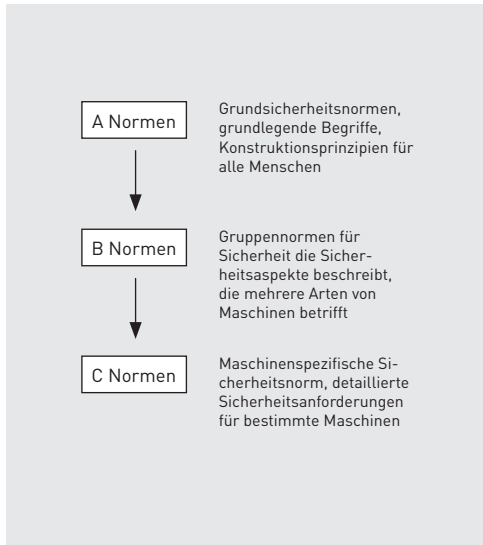
3. Datenrate

Jede Übertragungsstrecke hat eine bestimmte Datenrate. Eine hohe Datenrate sorgt bei kleinen Datenmengen für kurze Übertragungszeiten. Kleine Datenraten ermöglichen große Reichweiten.

Mit den genannten Größen können die Leistungsparameter an einen Kanal hervorragend beschrieben werden. Man erkennt auch sofort das Optimierungspotential. Sind kleine Datenmengen zu übertragen und ist das Frequenzband schon gut belegt, wird es hilfreich sein, eine möglichst schnelle Übertragungstechnik zu verwenden. Hierdurch kann die Übertragungszeit auf der Luftschnittstelle deutlich reduziert und damit der Duty-Cycle klein gehalten werden.

// Koexistenzplanung

Die vorhergehenden Ausführungen machen deutlich, dass man den Einsatz von Funk nicht dem Zufall überlassen sollte. Eine umfassende Kenntnis der Prozesse, der Systemdynamik und auch der Funkinfrastruktur sowie der verwendeten Frequenzbereiche sind dringend notwendig. Ebenso sind die unterschiedlichen Anwendungsfälle zu berücksichtigen. Ein allgemein gültiges Vorgehen zur Erreichung einer uneingeschränkten Koexistenz sämtlicher Systeme ist nicht realistisch. In der Regel muss in der Technologie- und Frequenzwahl ein Kompromiss gefunden werden, der eine akzeptable Lösung beschreibt. Hilfreich ist hierbei eine differenzierte Planung der Maßnahmen anhand der erhobenen Leistungsparameter, Systemanforderungen und Randbedingungen, die auch eine Priorisierung der zu erreichenden Ziele beinhaltet. Einige weitere Aspekte zur Koexistenz sind auch der VDI Richtlinie 2185 / Blatt 2 zu entnehmen.



Sicherheitsnormen sind hierarchisch aufgebaut

// Sicherheit

Die Sicherheit von technischen Systemen ist eine Grundvoraussetzung für deren Betrieb. Allgemein kann man definieren, dass Sicherheit die Abwesenheit von Gefahr ist. Das Gefährdungspotential kann jedoch aus unterschiedlichen Richtungen kommen.

Safety und Security – ein komplexes Thema

Der englische Begriff »Safety« beschreibt die Sicherheit der Person vor der technischen Anlage oder der Maschine. Schützenswert ist hier der Mensch. In der Regel ist in einem Safety-System die Anlage in einen sicheren Zustand zu überführen, so dass keine Gefahr mehr für Leib und Leben besteht. Hierfür hat sich der Begriff der »funktionalen Sicherheit« etabliert.

Ist hingegen die Maschine, ein Gerät oder ein Gebäude schützenswert, spricht man von »Security«. Hier geht es um Maßnahmen, die technische Systeme vor dem Angriff von Dritten schützen.

Häufig geht es um die Datensicherheit: Angreifer von außen sollen keinen Einfluss auf die Daten- oder Steuerungsstrukturen einer Maschine haben.

Sicherheit ist damit ein äußerst komplexes Thema. Regeln und gesetzliche Vorschriften unterschiedlichster Disziplinen sind einzuhalten, um den Nachweis über sichere Systeme zu führen. Sowohl bei Safety als auch bei Security geht es um die Identifikation von Gefahrenpotentialen und Maßnahmen, die getroffen werden, um das System in einem sicheren Zustand zu halten. Man muss sich darüber im Klaren sein, dass maximale Sicherheit nur mit einem maximalen Aufwand zu erreichen ist. Dieses macht eine Differenzierung von Sicherheitsstufen notwendig. In den nachfolgenden Abschnitten werden die Aspekte Safety und Security getrennt diskutiert.

Funktionale Sicherheit – Safety

Programmierbare elektronische Sicherheitssysteme (PES; Sicherheitssteuerungen) sind inzwischen weit verbreitet, nachdem es anfangs nur elektromechanische Lösungen für die Maschinensicherheit gab. Bereits in den 80er Jahren wurden interessante Sicherheitskonzepte auf Software- und Feldbus-Basis entwickelt. Heute findet man eine Vielzahl unterschiedlicher Systemlösungen für den Safety-Bereich. Sie werden neben der Steuerungs- und Automatisierungstechnik u. a. auch in der Antriebstechnik, der Fahrzeugtechnik und der Medizintechnik eingesetzt. Der Trend zu konfigurierbaren Sicherheitssystemen auf elektronischer Basis ist damit offensichtlich.

Maschinenrichtlinie 2006/42/EG

Mit der Einführung der neuen Maschinenrichtlinie (MRL) zum 29.12.2009 ist ein weiterer wichtiger Schritt in Richtung europaweiter Harmonisierung der Sicherheitsrichtlinien erfolgt. Darüber hinaus sind zeitgleich mit der MRL etliche neue Normen für die funktionale Sicherheit in Kraft

EN Norm	Titel
EN ISO 12100-1: 2003/ A1: 2009	Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 1: Grundsätzliche Terminologie, Methodologie
EN ISO 12100- 2: 2003/ A1: 2009	Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 2: Technische Leitsätze
EN ISO 14121- 1: 2007	Sicherheit von Maschinen - Risikobeurteilung - Teil 1: Leitsätze

Sicherheitsgrundnormen

getreten. Dabei steht nicht mehr alleine die deterministische Betrachtung von Fehlerszenarien im Vordergrund, sondern eine umfassende Bewertung der Wahrscheinlichkeit von Fehlerszenarien (Probabilistik).

Die Änderungen gegenüber der Vorgängerversion MRL98/37/EG sind nicht dramatisch, weisen aber in einigen wesentlichen Punkten deutliche Erweiterungen auf. So sind z. B. die Bestimmungen auf Baugruppen und Teilmaschinen ausgeweitet worden, die für sich keine bestimmte Funktion ausführen, sondern nur nach Einbau und Ergänzung von Schutzeinrichtungen vollständig sind.

Die MRL gilt nun auch für Sicherheitsbauteile wie Lichtschranken, Schalmatten, selbsttätig bewegliche Schutzeinrichtungen und auswechselbare Komponenten, die die Funktion einer Maschine verändern (Wechselwerkzeuge, Anbauteile). Für all diese Systeme besteht eine CE-Kennzeichnungspflicht gemäß der Niederspannungsrichtli-

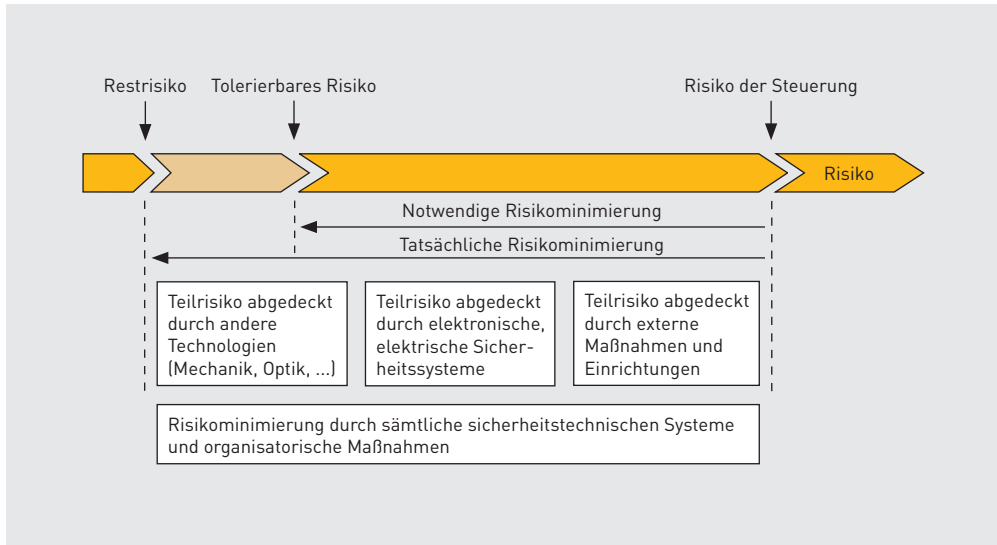
nie (2006/95/EG), die eine Risikobewertung notwendig macht.

Hierarchischer Normenaufbau

Zur Umsetzung der Richtlinien werden im Amtsblatt der Europäischen Union die gültigen harmonisierten Normen veröffentlicht. Diese sind alleine maßgeblich für die Umsetzung. Wird eine Richtlinie abgelöst, so wie es bei der MRL 98/37/EG zum Ende des Jahres 2009 der Fall war, sind auch nur die neuen harmonisierten Normen maßgeblich für die weitere Verwendung. Das heißt: Die mehr als 600 existierenden Normen müssen teilweise revidiert werden. Zudem werden die Normen den internationalen Gegebenheiten angepasst und weltweit vereinheitlicht. Ein gutes Beispiel dafür ist die EN 292 »Sicherheit von Maschinen, Grundbegriffe, allgemeine Gestaltungsleitsätze« die durch die ISO-Norm EN ISO 12100-1 ersetzt wird.

Die Normen sind hierarchisch in A-, B- und C-Normen unterteilt. Die A-Normen, auch als Sicherheitsgrundnormen bezeichnet, behandeln die grundlegenden Begriffe und allgemeinen Leitsätze, Konstruktionsprinzipien und allgemeine Aspekte, die für alle Maschinen gelten. Sie sind bindend und bilden die Basis für alle weiteren Normen.

Unter den B-Normen finden sich die Sicherheitsgruppennormen. Sie beschäftigen sich mit den anwendungsunabhängigen Standards, die auf unterschiedliche Maschinenarten anzuwenden sind und richten sich an die Entwickler und Hersteller von sicherheitsgerichteten Komponenten. Man unterscheidet zwischen B1- und B2-Normen. B1-Normen behandeln besondere Sicherheitsaspekte wie z. B. Sicherheitsabstände, Temperaturbereiche und Geräuschpegel. B2-Normen beschäftigen sich mit sicherheitsbedingten Verfahren und Einrichtungen wie z. B. Stillsetzung, Zweihandschaltungen und Verriegelungseinrichtungen.



Prinzipien der Risikominimierung gemäß IEC 61 508

EN-Normen:

Einige Sicherheitsgruppennormen

GSA 1.2.1 Sicherheit und Zuverlässigkeit von Steuerungen

EN ISO 13849-1: 2008 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze

EN ISO 13849-1: 2008/AC: 2009 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze

EN ISO 13849-2: 2008 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen, Teil 2: Validierung

EN 62061: 2005 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

GSA 1.2.3 Ingangsetzen

EN 1037: 1995 + A1:2008 Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf

GSA 1.2.4.3 Stillsetzen im Notfall

EN ISO 13850: 2008 Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze

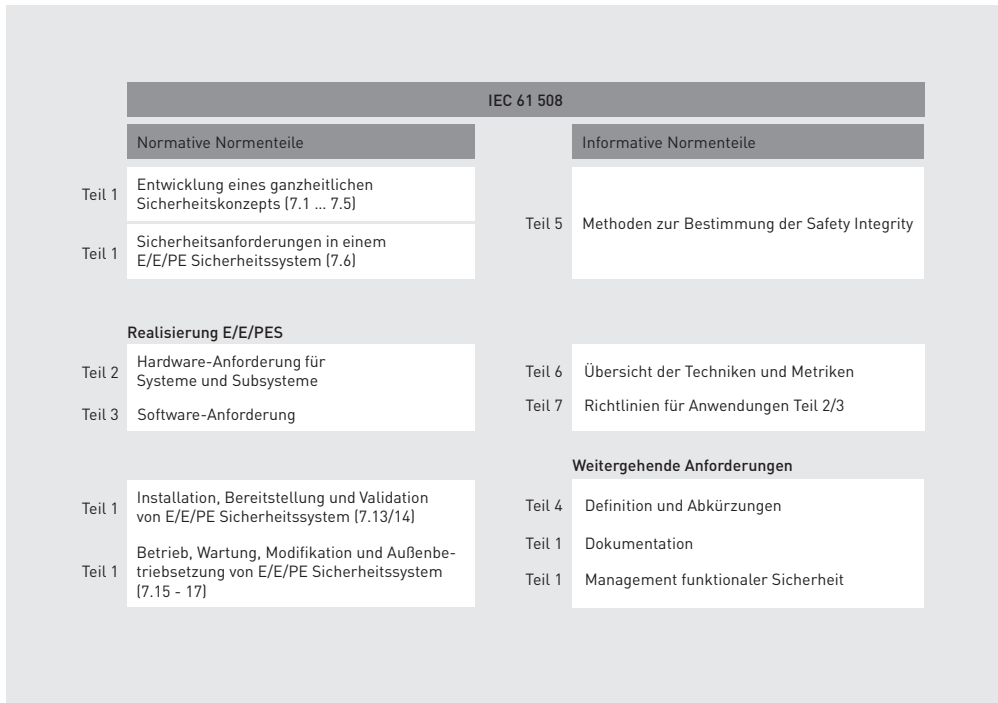
GSA 1.4.2 Besondere Anforderung an trennende Schutzeinrichtungen

EN 953: 1997 + A1: 2009 Sicherheit von Maschinen – Trennende Schutzeinrichtungen – Allgemeine Anforderungen an Gestaltung und Bau von feststehenden und beweglichen trennenden Schutzeinrichtungen

GSA 1.5.1 Elektrische Energieversorgung

EN 60204-1: 2006/A1:2009 Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen

EN 60204-11: 2000 Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 11: Anforderungen an Hochspannungsausrüstung für Spannungen über 1000 V Wechselspannung oder 1 500 V Gleichspannung aber nicht über 36 kV



Inhalt der IEC 61 508

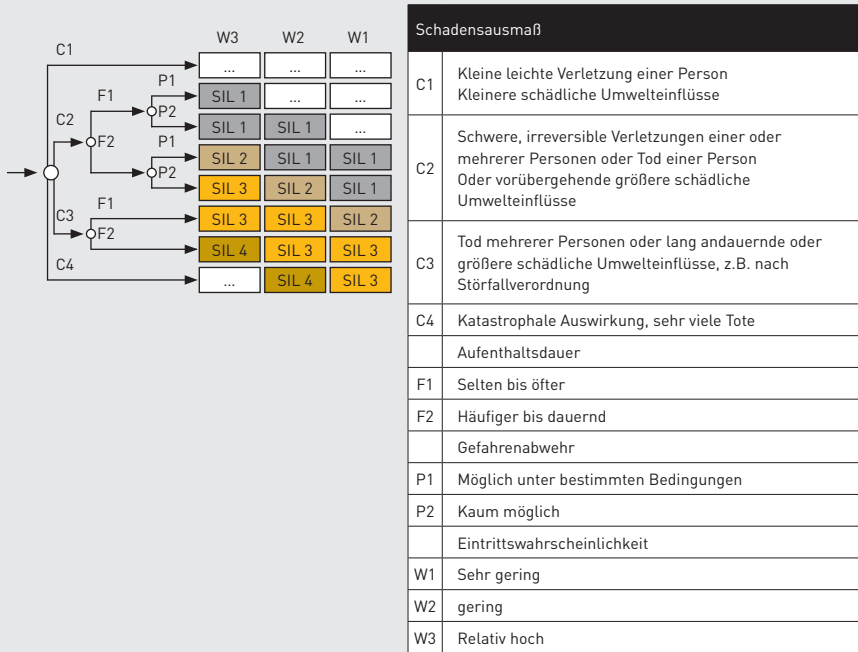
C-Normen sind Sicherheitsfachnormen, die eine Gültigkeit nur in speziellen Anwendungsbereichen bzw. Maschinengattungen haben. Sie werden in so genannte Sachgebiete (ICS) eingeteilt. Die entsprechenden Normen sind nur in dem Sachgebiet gültig und entsprechend hoch spezialisiert. Liegt für eine Maschinengattung keine C-Norm vor, sind die A- und B-Normen zum Nachweis der Übereinstimmung mit der Richtlinie anzuwenden.

Die Stufen der Maschinensicherheit

Mit Einführung der Maschinenrichtlinie dürfen in Europa nur noch Maschinen in den Verkehr gebracht werden, für die eine Risikobeurteilung vorliegt. Eine besondere Rolle spielt dabei für technische Geräte mit Elektronik und Software die IEC 61508 »Funktionale Sicherheit von elektrischen, elektronischen und elektronischen programmier-

baren Geräten«. Diese Norm fordert einen quantitativen Nachweis der Sicherheit.

Personen oder Institutionen, die Maschinen und Anlagen in Verkehr bringen, sind verpflichtet, eine Risikobeurteilung durchzuführen und diesen Nachweis 10 Jahre aufzubewahren. Da es sich mit der Richtlinie um eine Eigenklärung handelt, setzt die EU auf die Eigenverantwortung des Herstellers. Fehlt eine qualifizierte Risikobeurteilung, ist dieses ein Verstoß gegen geltendes Recht. Im Fall eines Unfalls wird untersucht, ob das Sicherheitskonzept dem Stand der Technik entspricht oder ob sich der Unfall aufgrund eines Konstruktionsmangels, fehlender Sicherheitseinrichtungen oder unzureichender Warnhinweise ereignet hat. Kann eine Nachlässigkeit nachgewiesen werden, führt das in der Regel zu einer strafrechtlichen Verfolgung.

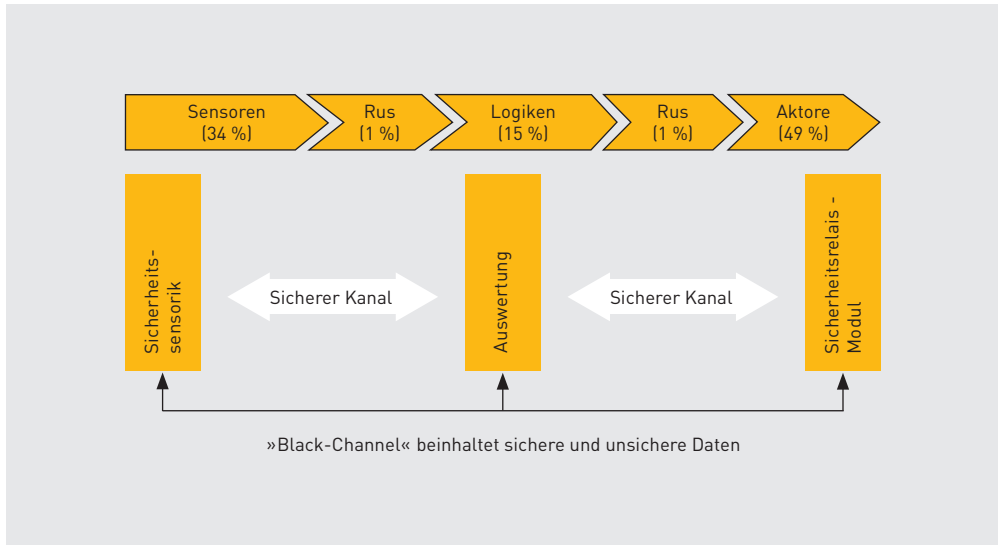


Risikograph nach IEC 61508 zur Bewertung von Safety Levels

Die operativen Schritte, nach der man normenkonform vorzugehen hat, sind: // Funktionale Sicherheit

1. Identifikation des möglichen Gefährdungspotentials der Anlage und Bewertung des potentiellen Risikos. (IEC 61508)
2. Risiko eliminieren und reduzieren durch konstruktive Maßnahmen; Anwendung von Maßnahmen während der Entwicklung / Bau der Maschine EN ISO 12100-2, Artikel 4
3. Risiko reduzieren durch Schutzmaßnahmen gemäß EN ISO 12100-2, Artikel 5
4. Risiko reduzieren durch Unterweisung / Warnhinweise; Beschreibung von Restrisiko durch Unterweisung und Aufbringen von Warnhinweisen gemäß EN ISO 12100-2, Artikel 6.

Die IEC 61508 gilt für alle Anwendungen, in denen elektrische oder elektronische Geräte und Baugruppen zur Ausführung von Sicherheitsfunktionen verwendet werden. Die Norm fordert einen quantitativen Nachweis über das verbleibende Risiko auf der Basis von Versagenswahrscheinlichkeiten. Alle Berechnungen sind für eine komplette Sicherheitskette vom Sensor über die Steuerung bis hin zum Aktor zu bewerten. Die Versagenswahrscheinlichkeit (PFD – Probability of Failure on Demand) ist damit ein Maß zur Bewertung der Sicherheit.



Ein Black-Channel überträgt sichere und unsichere Daten über ein Medium

IEC 61508 ist eine Grundnorm, die direkt angewendet werden kann. In ihr sind alle wesentlichen Aspekte und Ausführungsbestimmungen für die Implementierung und den Betrieb sicherer elektrischer / elektronischer / programmierbarer elektronischer Geräte enthalten. Als »sicher« werden Geräte und Anlagen verstanden, die kein unakzeptables Risiko für die Verletzung von Personen oder Beschädigung der Umwelt hervorrufen. Funktionale Sicherheit bezieht sich auf die Funktion des Sicherheitselements selber und auf die Wahrscheinlichkeit mit der ein Sicherheitselement im Fehlerfall funktioniert. Die Norm beschreibt vier Safety Integrity Levels (SIL 1 bis 4), von denen SIL 4 den höchsten Schutz bietet.

Unter Beachtung des einschlägigen Normenwerks können sichere Systeme erstellt werden. Welche Lösung man hier verwendet, bleibt den Herstellern und Anwendern überlassen. Man geht davon aus, dass zurzeit etwa 10 % aller Sensor- und Aktorkomponenten in der Fertigungstechnik sicherheitsrelevant sind und erwartet

eine deutliche Steigerung in den nächsten Jahren. Die Nutzerorganisationen und führenden Hersteller reagieren entsprechend und bieten für die marktführenden Feldbusse wie Profibus, Interbus, CAN und AS-Interface entsprechende Lösungen an – derzeit allerdings nur für kabelgebundene Systeme.

Der Trend: Integrierte Sicherheitskonzepte

Traditionell wurden Sicherheitslösungen auf der Basis von Standardsteuerungen und elektromechanischen Sicherheitsschaltgeräten realisiert. Diese ermöglichen zwar den Einsatz bewährter Technik und kostengünstiger Komponenten. Sie erfordern aber eine komplizierte Schaltungstechnik und einen fehlerträchtigen hohen Verdrahtungsaufwand. Zusätzlich sind die Not-Aus-Schalter, Signalgeber und Lichtgitter über Meldeleitungen mit dem Steuerungsrechner verbunden, damit auf der Seite der Bedienelemente und Visualisierung eine Rückkopplung zum Benutzer möglich ist.

Performance Level PL	Mittlere Wahrscheinlichkeit gefahrenbringender Ausfälle innerhalb einer Stunde	SIL EN 61 508-A
a	$> 10^{-3} \dots < 10^{-4}$	Keine speziellen Anforderungen
b	$> = 3 \times 10^{-6} \dots 10^{-5}$	SIL 1
c	$> = 10^{-6} \dots 3 \times 10^{-6}$	SIL 1
d	$> = 10^{-7} \dots 10^{-6}$	SIL 2
e	$> = 10^{-8} \dots 10^{-7}$	SIL 3

Die durch IEC 61 508 geforderte funktionale Sicherheit

Aktuelle Maschinenlösungen gehen ganz klar in Richtung integrierter Sicherheitskonzepte. Die Hardwarekomponenten verteuern sich, dem steht aber der Vorteil der perfekten Integration über die Feldbussysteme und die Engineeringwerkzeuge der jeweiligen Hersteller entgegen. Die Sicherheitsverknüpfungen können über entsprechende Werkzeuge geplant und parametrierbar werden; auch eine automatische Validierung ist möglich. Eine integrierte Lösung kann aufgrund der hohen Kommunikationsleistung und vollständigen Vernetzung deutlich schnellere Reaktionszeiten und intelligente Stillsetzungen realisieren als es bei konventionellen Systemen möglich wäre. Integrierte Lösungen ermöglichen damit auch die durch IEC 61508 geforderte funktionale Sicherheit über den gesamten Lebenszyklus einer Maschine bzw. Anlage.

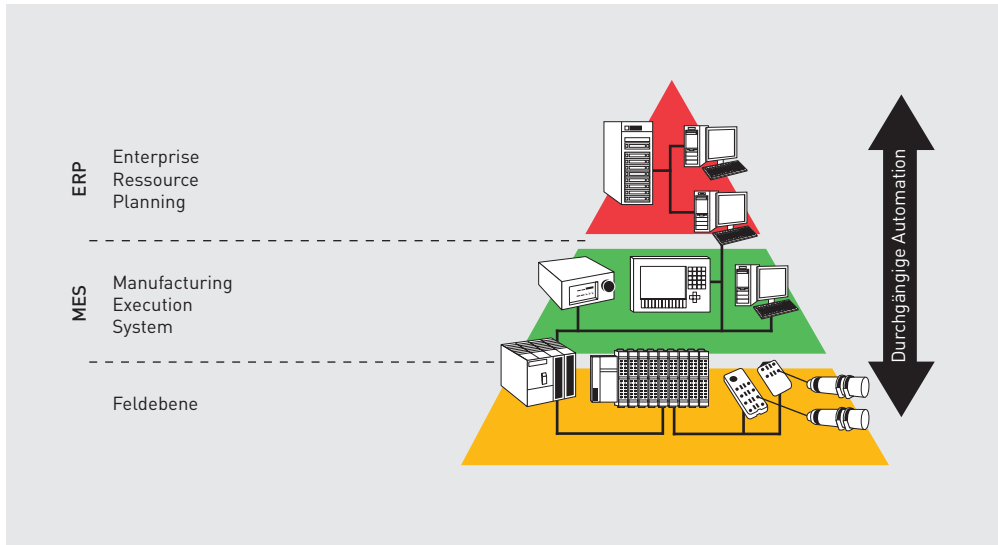
Sichere Kommunikation

Integrierte Sicherheitslösungen fordern Kommunikationssysteme, die eine durchgängige, transparente und fehlerfreie Kommunikation sicherstellen. Anfangs ging man davon aus, dass dies nur mit speziellen Sicherheitsbussen möglich ist. Inzwischen setzt man jedoch die sicherheitsgerichtete Kommunikation auf bewährte Standardbusse auf. Die Verwendung von Sicherheitsprotokollen auf den höheren Anwendungsschichten ermöglicht eine logische Zweikanalig-

keit und die Absicherung der Kommunikation allein durch Softwaremaßnahmen. Ziel ist die Herstellung einer Verfügbarkeit, die den Ansprüchen der jeweiligen Fachnorm genügt. Letztendlich geht es in der Norm um das Sicherstellen, das möglichst alle Fehler erkannt werden. Maßnahmen hierfür können, je nach Bussystem, sein:

- fortlaufende Nummerierung der Sicherheitstelegramme
- Zeiterwartung mit Quittierung des Telegramms
- Kennung für Sender und Empfänger, um die Authentizität des Telegramms sicherzustellen
- zusätzliche Datensicherung (CRC Cyclic Redundancy Check).

Gemäß IEC 61 508 teilt sich der Einfluss der Komponenten für Sicherheitssysteme auf 35 % Sensoren, 15 % Steuerungslogiken und 50 % Aktorik. In diesem Ansatz ist die Kommunikation nicht berücksichtigt. Um auch verteilten Systemen mit Buskommunikation gerecht zu werden, wird dem Bussystem ein Einflussfaktor von einem Prozent zugebilligt. Betrachtet man den Fehlereinfluss entsprechend dem Performance Level eines sicheren Systems, so darf man bei einem Performance Level e maximal $10^{-9}/h$ gefahrbringende Ausfälle innerhalb einer Stunde haben.



Der Wunsch der vertikalen Integration bringt neue Security-Herausforderungen mit sich

Für die Übertragungsstrecke bedeutet dieses eine zulässige Fehlerwahrscheinlichkeit von besser als $10^{-9}/h$ bei SIL3. Das ist gleichbedeutend mit einem Datentransport von mehr als 100.000 Jahren ohne unerkannte Fehler. Damit ist auch die Anforderung an einen sicheren (im Sinne der MRL) Funkstandard definiert.

Voraussetzungen für »Wireless Safety«

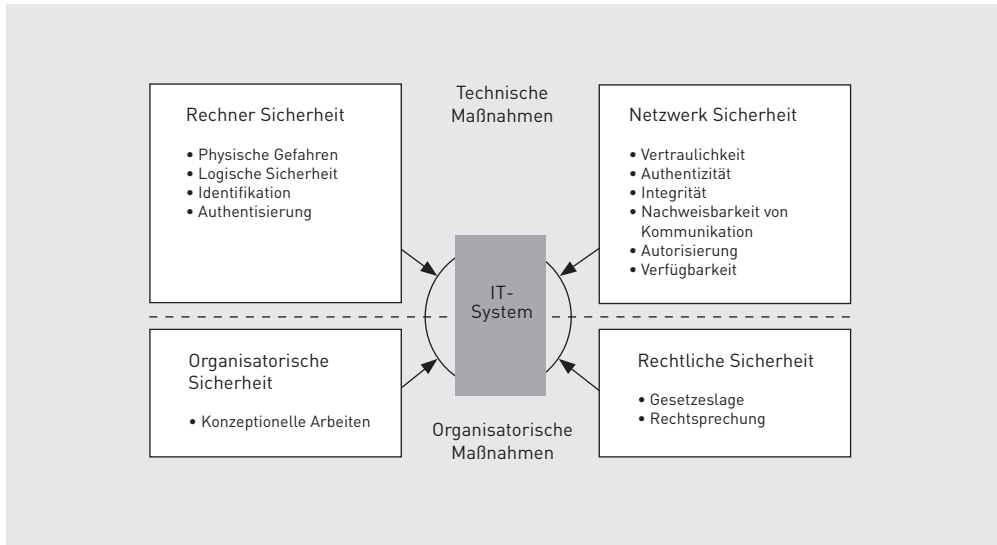
Das Schlüsselwort ist hierbei »unerkannte Fehler«. Sichere Systeme fordern keine fehlerfreie Kommunikation, sondern lediglich Fehlererkennung. Dies eröffnet die Möglichkeit, quasi beliebige Bussysteme als »Black Channel« zu verwenden. Von AS-Interface über Profinet und Profibus bis hin zu Ethercat, Sercos III und Ethernet IP haben heute alle industriellen Bussysteme die Möglichkeit, sichere Telegramme zu übertragen. Auch auf Funkstrecken ist der Sicherheitsaspekt zu übertragen. Da keine spezifischen Anforderungen gestellt werden, ist lediglich die Zuverlässigkeit des Bussystems zu überprüfen. Dies wird in vielen Lösungen umgesetzt, so dass die Übertra-

gung von sicheren Daten über Bluetooth, WLAN oder beliebigen proprietären Funkssysteme ohne weitere Probleme möglich ist.

Hier gibt es erste Ansätze und auch schon reale Einsatzfälle. So haben mehrere Anbieter sicherheitsgerichtete Funkstandards für die funktionale Sicherheit vorgestellt. Ein Feld, in dem sich die sicherheitsgerichtete Funkstrecke schon auf breiter Ebene durchgesetzt hat, ist die Steuerung von Lkw-Ladekränen und von Industriekranen.

EMV-Richtlinie und ATEX-Richtlinie

Weitere sicherheitsrelevante Anforderungen ergeben sich aus der EMV-Richtlinie (2004/108/EG). Ihr Ziel ist die Vermeidung einer elektromagnetischen Störung anderer Betriebsmittel durch ein (neues) Betriebsmittel. Sie gibt vor, in welcher Weise die elektromagnetische Verträglichkeit von elektrisch betriebenen Geräten in den Mitgliedsländern der EU beschaffen sein soll. Dabei ist laut Richtlinie ein »angemessenes Niveau« festzulegen. Details sind bewusst nicht definiert worden.



Informationssicherheit wird durch technische und organisatorische Maßnahmen erreicht

Die Explosionsschutzverordnung (11. GPSGV) setzt in Deutschland die europäische ATEX-Richtlinie 94/9/EG in nationales Recht um. Zweck der Richtlinie ist der Schutz von Personen, die in explosionsgefährdeten Bereichen arbeiten. Sie enthält in Anhang II die grundlegenden Gesundheits- und Sicherheitsanforderungen, die vom Hersteller zu beachten sind. Nähere Hinweise hierzu gibt das Buch »Explosive Themen« von steute.

// Informationssicherheit - Security

Informationssicherheit in der Automatisierungstechnik ist ein recht neues Thema. In autark arbeitenden konventionellen industriellen Feldbussen war ein ungeschützter Datenaustausch bisher vollkommen unproblematisch. Erst durch die vertikale Integration, d. h. den durchgängigen Datenaustausch bis in die Unternehmensebene, machen neue Schutzanforderungen notwendig.

Insgesamt kann man drei Trends erkennen, die schnell die Bedeutung von Informationssicher-

heit auch in industriellen Anlagen aufzeigen.

1. Fernwartung und Fernüberwachung von Anlagen und Geräten stellen neue Anforderungen an die Kommunikation: Mit dem Gewinn der Internetverbindbarkeit sind die Geräte einer vergleichbaren Gefährdung ausgesetzt. Es gelten nahezu die gleichen Anforderungen wie im öffentlichen Internet.
2. Der zweite Treiber ist der Einsatz von Ethernet-technologie in der Automatisierungstechnik, der mit durchgängiger Internettechnologie gleichgesetzt werden kann. Zumindest für die asynchrone Kommunikation wird oberhalb von Ethernet die TCP/IP-Protokollfamilie genutzt, die nicht nur das Finden und Verwalten von Geräten erleichtert, sondern auch eine komfortable Basis für das Parametrieren und Dokumentieren von Geräten bietet. Einfache Webserver, selbst auf Kleinststeuerungen und Embedded-Geräten, sind heute Stand der Technik. Durch das Nutzen der Internettechnologien im innerbetrieblichen Kontext, so genannten Extranets, wird das Schutzproblem in das Unternehmen

hineingetragen. Ist eine Anlage »durchgängig« von der Unternehmensebene bis in die Steuerung, sind auch vergleichbare Sicherheitsanforderungen wie im Internet umzusetzen.

3. Funktechnologie wird vermehrt in industriellen Systemen eingesetzt. Hier galt aus der Sicht der Automatisierer häufig das Motto »was man nicht sieht, ist auch nicht gefährdet«. Dass diese Netze zu schützen sind, zeigen tausende angegriffener WLAN-Netzwerke in den unterschiedlichsten industriellen Bereichen. In der Automatisierungstechnik oder bei technischen Systemen ist der Angriff noch viel tragischer, wenn technische Abläufe oder Funktionen durch fremde Geräte korrumpiert werden. Möglicherweise werden auch über die Luftschnittstelle sensible Daten ausgetauscht, die schützenswürdig sind. Hier gibt es nur eins: Vollschutz nach allen Regeln der Kunst.

Diese drei Trends machen deutlich, dass die IT Einzug in die Automatisierungstechnik gehalten hat. Auch wenn das ein radikales Umdenken erfordert: Informationssicherheit steht ganz oben auf der Agenda beim unternehmensweiten Einsatz von Ethernet-basierten oder funkbasierten Systemen stehen.

Informationen müssen geschützt werden

Unter Informationssicherheit versteht man generell den Schutz von Informationen jeglicher Art und Herkunft. Der Schutz von Daten in Köpfen und auf Papier ist nur organisatorisch zu lösen. Um den Schutz der elektronischen Daten in Rechnersystemen kümmert sich die IT-Informationssicherheit. Rechnersysteme können dabei sehr weit gefasst werden – angefangen von Großrechnern über Desktoprechner bis hin zu Mobiltelefonen, Steuerungsrechnern und intelligenten Sensoren in der Automatisierungstechnik.

Die Grundbedürfnisse: CIA

Die klassischen Grundbedürfnisse der Informationssicherheit werden in der Alliteration CIA zu-

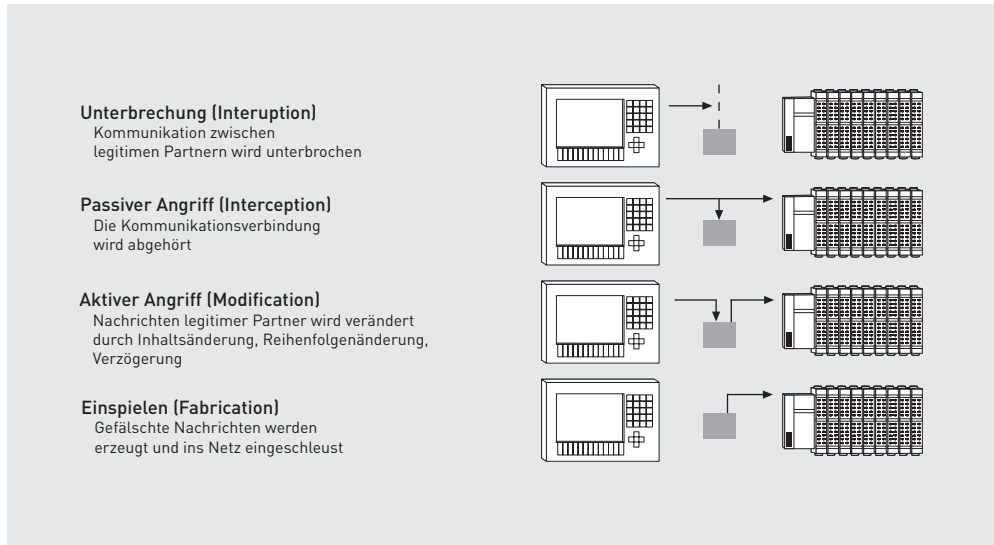
sammen gefasst: Confidentiality (Vertraulichkeit), Integrity (Zuverlässig) und Authenticity (nicht abstreitbar). Daten müssen vertraulich behandelt werden. Sie dürfen nur dem zugehen, der auch wirklich diese Daten verwenden darf. Die Daten müssen zuverlässig sein. Das heißt: Sie müssen exakt so beim Kunden ankommen, wie sie auch versendet worden sind. Eine unerlaubte Modifikation muss auf jeden Fall verhindert oder zumindest aufgespürt werden. Unter Authentizität versteht man, dass der Benutzer der Daten auch wirklich der ist, als der er sich ausgibt.

Hier muss man berücksichtigen, dass es nicht nur vorsätzliche Bedrohungen durch Computerviren, Trojanern, Abhören von Datenleitungen oder Diebstahl von Festplatten oder ganzen Computern gibt. Der Datenbestand ist auch durch höhere Gewalt wie Blitzschlag, Wasser, Strom und Feuer oder durch fehlerhafte Updates und menschliches Versagen bedroht.

Zur Lösung dieser Sicherheitsproblematik sind die unterschiedlichsten Maßnahmen zu ergreifen. Bei Funksystemen spielt die Netzwerksicherheit eine große Rolle. Neben der Vertraulichkeit und Integrität sollte die Kommunikation nachweisbar sein und nur von autorisierten Systemen genutzt werden. Ein weiterer wichtiger Aspekt gerade bei Funksystemen ist die Verfügbarkeit.

In der Regel sind die getroffenen technischen Maßnahmen durch organisatorische Maßnahmen zu unterstützen. Hierzu gehört in erster Linie die organisatorische Sicherheit, die in den Regeln und Richtlinien erarbeitet sind, wie IT-Sicherheit umgesetzt wird, und letztlich gibt es noch die rechtliche Sicherheit. Vergleichbar zu den Safety-Normen sind auch Minimalanforderungen an IT-Systeme in unterschiedlichen Normen definiert worden.

Und schließlich sind auch infrastrukturelle Sicherheitsmaßnahmen zu beachten, die einen



Die vier Grundprinzipien der Angriffe auf IT-Netzwerke

physischen Zugriff Unbefugter auf technisches IT-Gerät mit dem Ziel von Diebstahl oder Manipulation verhindern. Hierzu gehören bauliche Absicherungen und Zugangskontrollen.

Normen und Standards

Wie auch bei den technischen Anforderungen, ist im Bereich der IT-Sicherheit die Normungsarbeit in vollem Gang. Durch das gestiegene Gefährdungspotential wachsen die Normen stetig. Umfassend kann an dieser Stelle kaum auf alle Regeln und Richtlinien hingewiesen werden. Die Normenreihe ISO 27000 ff gibt die entsprechenden Standards für ein Managementsystem der Informationssicherheit an.

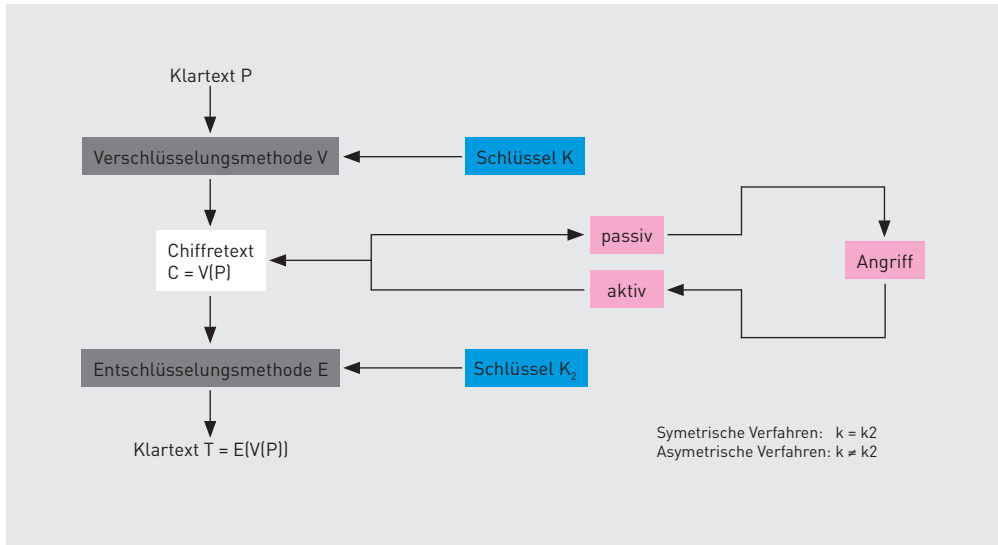
ISO 27 000: Der 27000 Standard gibt einen generellen Überblick über Managementsysteme der Informationssicherheit. Er beschreibt die Zusammenhänge der unterschiedlichen Normen in der 2700x-Familie sowie die grundlegenden Prinzipien, Konzepte und Begriffe für Managementsysteme der Informationssicherheit.

ISO 27 001: Der ISO 27001 Standard »Information technology – Security techniques – Information security management system requirements specification« beschreibt allgemeine Empfehlungen zur Einführung und den Betrieb entsprechender Managementsysteme.

ISO 27 002: Die ISO 27002 »Information technology – Code of practice for information security management« ist ein Rahmenwerk, welches beschreibt, wie ein funktionierendes Sicherheitsmanagement aufzubauen und in der Organisation zu verankern ist. Die Empfehlungen sind mehr für das Management gedacht, als dass es sich um konkrete technische Hinweise handelt.

ISO 27 005: Im ISO 27005 Standard »Information security risk management« sind Rahmenempfehlungen für das Risikomanagement. Diese Richtlinie löst die ISO 13335 -2 ab.

ISO 27 006: Die ISO 27006 »Information technology – Security techniques – requirements for the



Verschiedene Angriffs- und Verschlüsselungsverfahren

accreditation of bodies providing certification of information security management systems« spezifiziert Anforderungen die Akkreditierungs- und Zertifizierungsstellen.

Weitere Standards Die ISO 2700X wächst ständig und wird langfristig verankert werden. Durch die Zertifizierbarkeit wird eine Wahrnehmung wie bei der ISO 9000 zu erwarten sein und damit ein Qualitätsmerkmal für eine Organisation

Im Gegensatz zu den technischen Normen im Bereich Safety ist die Security-Normenlage im Wesentlichen auf die Organisation bezogen. Sicherheit ist damit eine ganzheitliche Herausforderung, die nicht einfach mit einem technischen System hergestellt werden kann.

Angriffsstrategien

Neben den Bedrohungen durch eigene Mitarbeiter (z. B. durch Indiskretionen) spielen die technischen Möglichkeiten eines potentiellen Angriffs eine große Rolle. Hier sind zwei gegenläufige

Trends bemerkenswert. Auf der einen Seite nimmt die Komplexität der Werkzeuge zu, mit denen technische Informationen ausgespäht werden. Auf der anderen Seite benötigt der Angreifer immer weniger technisches Verständnis, da Unmengen an Software und Werkzeugen im Internet bereit stehen. Dies ermöglicht es, einen hocheffektiven Angriff vorzubereiten und durchzuführen, ohne dass der Angreifer über hohes Know-how verfügt. Diese Trends führen zu einem steigenden Gefährdungspotential und einer gewissen Schutzlosigkeit, wenn man sich nicht intensiv mit dem Thema der Informationssicherheit auseinandersetzt.

Prinzipiell unterscheidet man vier Grundtypen des Angriffs auf technische Systeme.

Interruption (Unterbrechung)

Die Kommunikation zwischen zwei oder mehreren legitimen Kommunikationspartnern wird unterbrochen. Bei kabelgebundener Kommunikation kann das beispielsweise durch das Kappen

einer Verbindung realisiert werden, bei Funksystemen reicht häufig eine Störung des Funkkanals beispielsweise durch Störsender (englisch: Jammer) aus.

Interception (passiver Angriff)

Die Leitung wird – oft vom Betreiber unbemerkt – einfach abgehört, der Angreifer interessiert sich für die übertragenen Daten. Bei Funksystemen ist ein passiver Angriff vollkommen unbemerkt zu führen, da es ausreicht, einen Empfänger in Funkreichweite zu positionieren. Ein hinreichender Schutz kann nur bei verschlüsselter Datenübertragung sichergestellt werden.

Modification (Modifikation)

Bei diesem aktiven Angriff wird der Nachrichtinhalt durch einen Angreifer modifiziert, der nicht mit einer eigenen Identität auftritt. Ein typischer Vertreter dieser Gattung ist der »Man in the middle attack«. Eine Absicherung kann nur durch eine gut funktionierende Verschlüsselung und weitere Kommunikations- und telegraphenbezogene Sicherheitsmechanismen erreicht werden.

Fabrication (Einspielen)

Wenn ein Angreifer durch passiven Angriff genügend Informationen über eine Kommunikation erhalten hat, kann er das Zielsystem in einem zweiten Schritt durch Einspielen von Nachrichten mit falschen Informationen versorgen. Der Angreifer spiegelt dann in der Regel die Identität eines legitimen Partners vor. Ein Schutz ist hier nur durch eine authentifizierte und validierte Kommunikationssequenz möglich.

Verschlüsselung – Kryptographie

Die Anforderungen an die Vertraulichkeit lassen sich in einem technischen System nur durch Verschlüsselung realisieren. Unterschiedliche Methoden mit verteilten oder gemeinsamen Schlüsseln sind Stand der Technik. Was eingesetzt wird, hängt von der Schutzbedürftigkeit der Daten ab.

Rein technisch sind die Verfahren prinzipiell vergleichbar. Originaldaten im Klartext P werden mit einer Verschlüsselungsmethode V mit einem Schlüssel k verschlüsselt. Je komplizierter und länger der Schlüssel ist, desto höher ist die Sicherheit, weil ein potentieller Angreifer mehr Rechenleistung in das Knacken der Schlüssel stecken muss. 128-Bit-Schlüssel sind heute Stand der Technik. Der übertragene Chiffretext C ist hoffentlich so gut geschützt, dass der Angreifer die Daten nicht entschlüsseln kann. Der Empfänger hingegen kennt die Entschlüsselungsmethode E , die eine inverse Funktion von V darstellt. Mit der Kenntnis eines Schlüssels kann der ursprüngliche Klartext wieder hergestellt werden.

Die Authentifizierung ist der Prozess, bei dem ein Teilnehmer seine Echtheit beweist, sich also authentisiert, um vor Missbrauch, vor Täuschung, vor Phishing und vor dem Eindringen in sensible Bereiche zu schützen.

Um die Gefahr der Preisgabe der eigenen Identität auszuschließen, werden Verfahren wie Challenge-Response-Authentifizierung und Zero Knowledge verwendet, bei denen das sich authentisierende Subjekt nicht mehr die Identifizierungsdaten selbst übermittelt, sondern nur einen Beweis dafür, dass es diese Identifizierungsdaten zweifelsfrei besitzt. Ansonsten ist es immer empfehlenswert, die Authentifizierung zu verschlüsseln.

Security in der Funkkommunikation

Systeme mit Funkkommunikation bieten von sich aus ein hohes Angriffspotential. Angreifer können mit Störsendern oder so genannten Jammer die Kommunikation unterbrechen oder unauffällig die Luftschnittstelle abhören. Eine sichere Funkkommunikation ist damit ohne geeignete Maßnahmen kaum möglich. Häufig bringen die Technologien jedoch von Haus aus die unterschiedlichsten Techniken mit, die es potentiellen Angreifern schwierig macht.

Welche Technik bei der jeweiligen Funktechnologie eingesetzt wird, hängt häufig vom Anwendungsfall ab. Auch sind Maßnahmen zur IT-Sicherheit in vielen Fällen skalierbar, so dass der Betreiber entscheiden kann, welches Maß an Sicherheit gewählt wird. Dabei muss man bedenken, dass die Prozessoren jeweils Rechenzeit für die gewählten Sicherheitsmechanismen, sprich für die Berechnung der Schlüssel, benötigen. Gerade bei Embedded-Anwendungen ist das ein wesentlicher Gesichtspunkt. Darüber hinaus erfordert eine sichere Frage-Antwort-Kommunikation zusätzliche Eingaben und Mechanismen. Geräte müssen angelernt werden, Schlüssel werden ausgetauscht und auch das Verhalten nach einem Spannungsausfall oder Systemwechsel aufgrund eines Servicefalls muss genau betrachtet werden. Das macht die Anwendung von Sicherheitstechniken manchmal kompliziert.

Um Funk dennoch sicher zu machen, haben sich verschiedene Grundprinzipien bewährt.

1. Frequenzwechselverfahren ermöglichen das Ausblenden von schmalbandigen Störern. Funk-systeme wechseln nach jedem Datenpaket die Frequenz. Der organisatorische Aufwand wird häufig im Linkmanager der jeweiligen Technologie realisiert.
2. Anlernen von Geräten. Auf der Basis der eingesetzten Hardware sollen nur vertrauliche Geräte miteinander kommunizieren. Hierzu ist ein Einbindeprozess notwendig, der Sensoren, Aktoren oder weitere Geräte mit einer Steuerung oder einem Accesspunkt verbinden. Unterschiedliche Mechanismen vom Austausch der MAC-Adressen bis hin zum individuellen geschützten Austausch von Verbindungscodes sind möglich.
3. Verschlüsselung sollte prinzipiell angewendet werden. Nur verschlüsselte Daten sind gegen Abhören geschützt. Der Aufwand zahlt sich mit einer höheren Sicherheit aus. 128-Bit-Schlüssel und AES-Verfahren sind heute Standard und

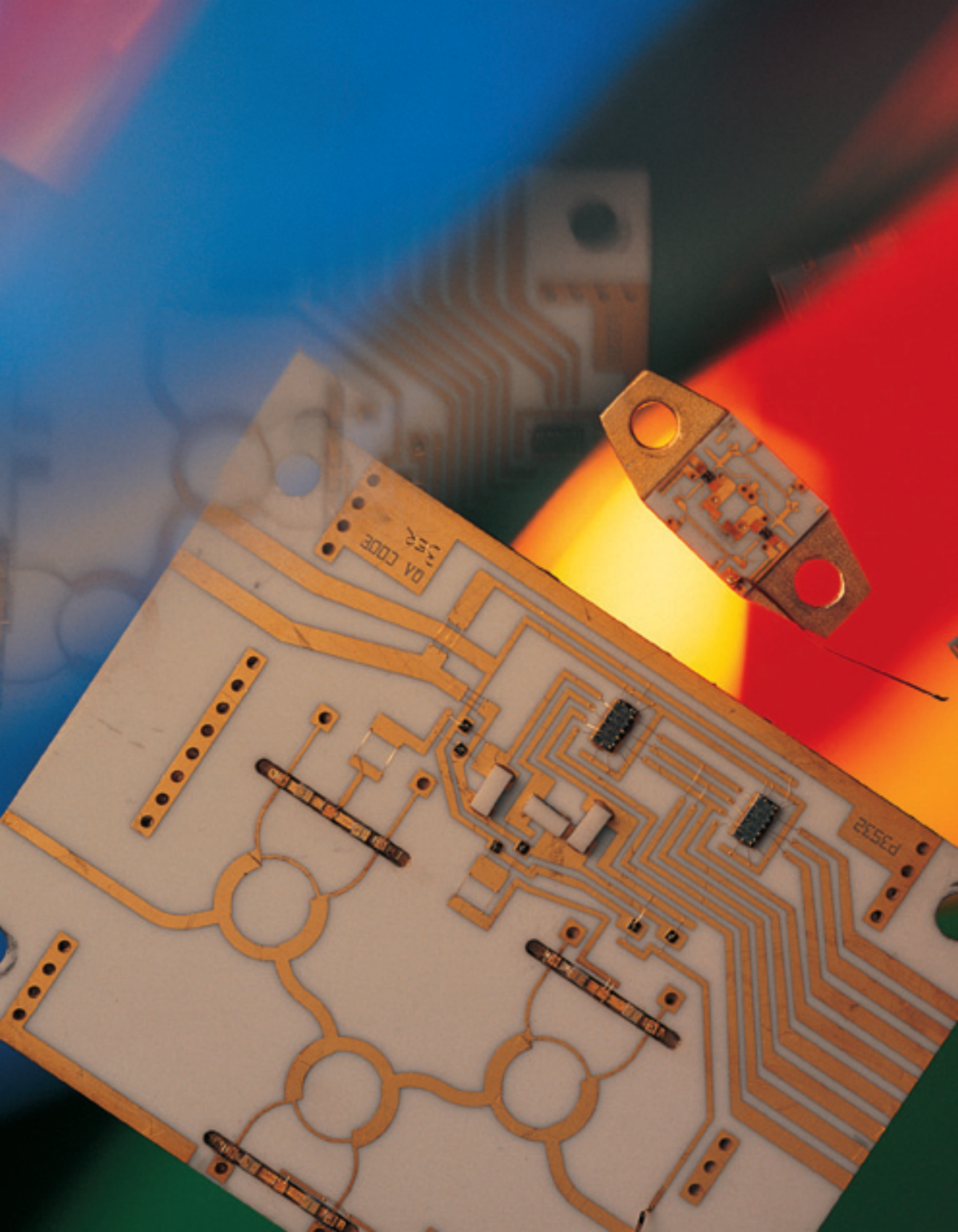
bieten hinreichenden Schutz. Darüber hinaus sind weitere Maßnahmen möglich, die zu einer Steigerung der Sicherheit führen. Abschließend sollen noch einige Charakteristika bewährter Funktechnologien beleuchtet werden.

Bluetooth

bringt von Haus aus alle Mechanismen für eine sichere Datenübertragung mit. Hardwaretechnisch hat jedes Gerät eine einzigartige Bluetooth-MAC-Adresse. Anhand dieser und einem 32-Bit-Zähler wird eine Hopping-Sequenz für das Frequenzsprungverfahren (FHSS Frequency Hopping Spread Spectrum) individuell für jedes Piconetz ausgehandelt. Jedes Piconetz hoppt damit mit seiner eigenen individuellen Frequenz im gesamten zulässigen Frequenzband, so dass schmalbandige Störer sehr gut ausgeblendet werden. Die Authentifizierung erfolgt mit einem Challenge-Response-Verfahren. Der Sender sendet einen 128-Bit-Schlüssel, der vom Empfänger mit einem Link-Key und seiner 48-Bit-Adresse verarbeitet und als Ergebnis zurückgesendet wird. Für die Verschlüsselung wird ein symmetrischer Schlüssel mit 8-128 Bit mit dem AES-Algorithmus verwendet. Hiermit ist Sicherheit nach Stand der Technik in vollem Umfang gegeben – wenn nicht alle Sicherheitsoptionen standardmäßig deaktiviert wären. Der Anwender hat also die Verantwortung für eine ordnungsgemäße Sicherheit zu übernehmen.

WLAN IEEE 802.11

wird in Office-Netzwerken standardmäßig eingesetzt. Auch in Automatisierungsnetzwerken ist WLAN heute Stand der Technik. Hier sind ebenfalls die unterschiedlichsten Sicherheitsmechanismen implementiert, die optional genutzt werden können. WLAN bietet keine Frequenzsprungverfahren, sondern belegt vorher eingestellte Kanäle. Von Haus aus sind jedoch die eingesetzten DSSS- und OFDM-Modulationsverfahren relativ gut gegen schmalbandige Störer geschützt. Bei den Verschlüsselungsverfahren sind unterschied-



lichste Methoden implementiert. Das hat historische Gründe und stellt die Rückwärtskompatibilität bei neueren Geräten sicher – jedoch auf Kosten der Sicherheit. WEP (Wired Equivalent Privacy) lässt sich innerhalb weniger Minuten mit geeigneten Tools aus dem Internet knacken. Eine etwas höhere Sicherheitsstufe bietet WPA (WiFi Protected Access). Zwar wird mit RC4 derselbe Verschlüsselungsalgorithmus wie bei WEP verwendet, jedoch wird der Schlüssel alle 10-kByte-Daten gewechselt. Dieser Schlüsselwechsel wird auch als TKIP (Temporal Key Integrity) bezeichnet.

WPA2 ist heute Stand der Technik bei aktuellen WLAN Produkten. Es verwendet den um ein Vielfaches sicheren AES-Algorithmus. Die AES-Implementierung in WPA2 wird auch als CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) bezeichnet, was nicht unbedingt zu einem besseren Verständnis beiträgt.

IEEE 802.15.4

ist die Basis auf den ISO-OSI-Layern 1 und 2 unterschiedlicher Funknetzwerke wie z. B. ZigBee oder WirelessHART. Proprietäre Lösungen sind ebenfalls mit den am Markt befindlichen Chips möglich. Auch IEEE 802.15.4 bietet Sicherheitsmechanismen auf MAC-Ebene durch einen Message-Integrity-Check und symmetrische Verschlüsselung. Die Schlüssel werden durch die höheren Protokollschichten für jeden Kommunikationspartner separat festgelegt und durch den MAC-Layer verwaltet. Unterschiedliche Verschlüsselungsalgorithmen wie CCM oder AES sind prinzipiell vorgesehen. Welche Verschlüsselung eingesetzt wird, hängt von der Implementierung ab. Teilweise erfolgt in den Chipsätzen eine Hardwareunterstützung, in anderen obliegt die Arbeit dem Hostprozessor.

Insgesamt kann man feststellen, dass mittlerweile alle neueren Funktechnologien eine sichere Übertragung anbieten. In der Regel ist die Security jedoch nicht voreingestellt, sondern optional nutzbar. Es liegt also an der jeweiligen Anwendung bzw. dem Anwender, ob das mögliche Sicherheitsniveau auch erreicht wird oder nicht.

// Antennentechnik

010

Geschichtliches

Sowohl zum Aussenden (Abstrahlen) als auch zum Empfangen von elektromagnetischen Wellen benötigt man Antennen. Eine Sendeantenne wandelt elektromagnetische, leitungsgebundene Wellen in Freiraumwellen um, eine Empfangsantenne wandelt die Freiraumwellen in leitungsgebundene elektrische Wellen zurück. Seit Anbeginn der Funktechnik verwendet man Antennen: Heinrich Hertz benutzte gestreckte Drähte, die später so genannten Hertzschen Dipole.

Der Begriff Antenne leitet sich übrigens vom italienischen Ausdruck für »Zeltstange« bzw. »Segelstange« her, weil ein Pionier der Funktechnik – Guglielmo Marconi – bei seinen ersten Versuchen des Antennenbaus im Jahr 1897 eine hölzerne Zeltstange verwendete. In den Anfängen der Funktechnik nutzte man zuerst einfache Dipole, dann Rahmenantennen als Empfänger. Nach dem Ersten Weltkrieg wurden auch Antennenarrays, Hornstrahler und Parabolantennen eingesetzt.

Wie funktioniert eine Antenne?

Im Prinzip ist eine Antenne nichts anderes als ein offener elektrischer Schwingkreis, in dem beim Einspeisen von Wechselspannung bzw. Wechselstrom Schwingungen erzeugt werden. Anders ausgedrückt: Eine einfache Dipolantenne erzeugt bzw. empfängt sowohl elektrische als auch dazu senkrecht stehende magnetische Felder. Kondensator und Spule bilden einen Schwingkreis, der geschlossene elektrische Feldlinien aussendet, wenn der Kreis in elektrische Schwingungen versetzt wird.

Die senkrecht zum elektrischen Feld verlaufenden Magnetfelder bilden geschlossene Kreise um den Leiter. Im Nahfeld nimmt die Feldstärke proportional zur dritten Potenz der Entfernung r ab. Im Fernfeld verringert sie sich lediglich proportional $1/r$. Die Leistungsdichte der abgestrahlten elektromagnetischen Wellen ist dem Produkt aus elektrischer und magnetischer Feldstärke propor-



Sendeantennen müssen hoch angebracht werden

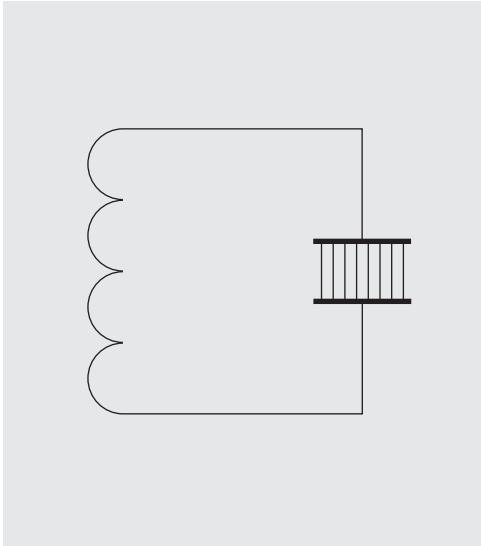
tional und nimmt daher mit $1/r$ ab (Abstandsquadratgesetz).

Wichtiger Faktor: Die Polarisation

Ein wichtiger Faktor bei der Bewertung von Antennen ist die Polarisation. Damit bezeichnet man die Orientierung der abgestrahlten elektrischen Feldlinien gegenüber der Erdoberfläche. Eine lineare horizontale oder lineare vertikale Polarisation liegt vor, wenn die Orientierung des elektrischen Feldes über die Zeit konstant bleibt. Ist die Stärke des elektrischen Feldes zeitlich konstant, die Richtung der Feldlinien jedoch zeitabhängig, spricht man von zirkularer bzw. links- oder rechtsdrehender Polarisation. Wichtig ist diese Unterteilung für die Funktion der Antenne: Wenn Empfangs- und Sendeantenne nicht die gleiche Polarisationsart und -richtung haben, wird die Signalübertragung stark gedämpft.

Resonanz und Resonanzfrequenz

Ein noch wichtigerer Faktor ist die Resonanz. Mit ihr wird die Abstimmung auf die Wellenlänge be-



Eine Dipolantenne ist letztlich nichts anderes als ein offener Schwingkreis.

$$Z_{w0} = \sqrt{\frac{\mu_0}{\epsilon_0}} \approx 120 \pi \, \Omega \approx 376,73 \, \Omega$$

Der Wellenwiderstand des freien Raumes

zeichnet, die die Antennen empfangen oder senden soll. Die Resonanzfrequenz wird durch die Abmessungen der Antenne bestimmt. Durch spezielle konstruktive Maßnahmen kann man erreichen, dass der Fußpunktwiderstand (Impedanz) über einen großen Frequenzbereich weitgehend konstant bleibt und somit ein breites Frequenzband übertragen werden kann. Solche Antennen bezeichnet man als Breitbandantennen.

Weitere Parameter in Kurzdarstellung

Zu den Parametern, die ebenfalls Einfluss auf die Leistungs- und Funktionsfähigkeit einer Antenne haben bzw. die deren Leistungsfähigkeit ausmachen, gehören die Faktoren:

- Absorptionsfläche
- Antennengewinn
- Apertur
- Äquivalente isotrope Strahlungsleistung
- Bandbreite
- Impedanz
- Nebenkeulendämpfung
- Richtfaktor

- Strahlungswiderstand
- Vor-Rück-Verhältnis
- Vor-Seiten-Verhältnis
- Wirkungsgrad.

Absorptionsfläche (Wirkfläche): Wirksame Antennenoberfläche

Antennengewinn: Verhältnis der in Hauptrichtung abgegebenen Strahlstärke in Bezug gesetzt zu einer verlustlosen Antenne gleicher Speiseleistung mit einem Antennengewinn von Null (in dBd und dBi)

Apertur: Freie Öffnung oder deren Durchmesser, durch die Radiowellen ausgesendet oder empfangen werden

Äquivalente isotrope Strahlungsleistung: EIRP; Produkt der in eine Sendeantenne eingespeiste Leistung und des Antennengewinns (bezogen auf einen Isotropstrahler)

Bandbreite: Frequenzbereich, in dem sich die Impedanz nur unwesentlich ändert

Impedanz: Widerstand an den Anschlussklemmen bei der verwendeten Frequenz (Ohm)

Nebenkeulendämpfung: Verhältnis des Gewinns der Hauptkeule in dB zum Pegel der größten Nebenkeule.

Richtfaktor: Richtwirkung einer Antenne mit Vorzugsrichtung; der Wert, der bei der Vorzugsrichtung über den Mittelwert aller Richtungen liegt. Konkret: Verhältnis des Quadrats der maximalen elektrischen Feldstärke (oder der magnetischen Feldstärke) in Hauptstrahlrichtung zum Quadrat der Feldstärke eines angenommenen Isotropstrahlers (dBi) oder einer Hertzschen Dipols (dBd).

Strahlungswiderstand: Zusammenhang zwischen Antennenstrom im Speisepunkt und der im Wellentyp gewandelten Leistung (Ohm).

Vor-Rück-Verhältnis (auch Rückdämpfung): Verhältnis des gemessenen Pegels der Hauptkeule in dB zum Pegel der Rückkeule in 180° .

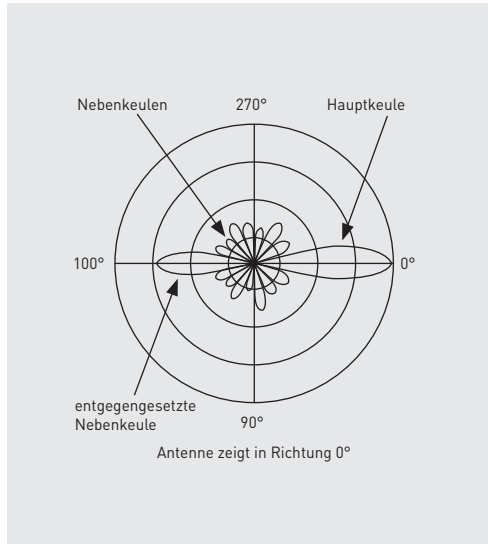
Vor-Seiten-Verhältnis: Verhältnis des gemessenen Pegels der Hauptkeule in dB zum Pegel der Seitenkeule in 90° oder 270° .

Wirkungsgrad: Verhältnis von wirklich abgestrahlter Leistung zu zugeführter Gesamtleistung (in Prozent).

Kürzere Wellen brauchen Sichtverbindung

In den Anfängen des Funkbetriebes mit Lang- und Mittelwellen war die räumliche Lage und geometrische Form der Antennen recht unkritisch. Die Wellen folgten der Erdoberfläche auch weit über den Sichthorizont hinaus. Erst mit dem UKW- Rundfunkdienst wurde die Erfahrung von quasi-optischer Ausbreitung der Funkwellen gewonnen, und die Funkantennen wurden möglichst hoch über der Erde angebracht: die Sendantennen auf exponierten hohen Bergen, die Empfangsantennen auf Hausdächern.

Je höher die verwendeten Frequenzen wurden, und je kürzer die Wellenlängen, um so mehr nähert sich die Funkausbreitung den optischen Bedingungen an. Für eine gute Funkverbindung mussten beide Antennenhöhen möglichst groß sein. Das bedeutet aber auch, dass die Antennen spätestens mit den Dezimeterwellen Sichtverbin-



Durch die Richtwirkung kann man die Reichweite einer Funkverbindung erhöhen

dung miteinander haben müssen. Hier werden in der Praxis sehr häufig die physikalischen Gesetze missachtet bzw. vergessen – auch und gerade in Industrieanwendungen!

Verschiedene Aufgaben – unterschiedlicher Aufbau

Antennen haben die Aufgabe, die erzeugte zugelassene Sendeleistung verlustarm in den Raum abzustrahlen (Sendantennen) oder aus dem Raum möglichst viel Sendeleistung einzufangen (Empfangsantennen). Bereits daraus können sich unterschiedliche Strukturen ergeben, wie ein hoher Sendemast auf der einen und eine einfache Wurfantenne auf der anderen Seite zeigen. Dies gilt vor allem bei einseitigen Funkverbindungen wie dem Rundfunk. Bei zweiseitigen Funkverbindungen sind eher gleiche Antennen die Regel. Eingeschränkt wird diese Reziprozität in der Praxis jedoch durch Faktoren wie die Sendeleistung: Eine Antenne, die für den Empfang konstruiert wurde, ist nicht unbedingt für die hohen elektrischen Leistungen des Sendens geeignet.





Auch der freie Raum hat übrigens einen Wellenwiderstand. Er ist eine Naturkonstante, genauer der Quotient aus zwei Naturkonstanten, und beträgt rund 377 Ohm wie im Bild Seite 171 dargestellt.

Die Antenne passt also den Wellenwiderstand der Speiseleitung (z. B. 75 Ohm) an den des freien Raumes an, damit die Hochfrequenzenergie ohne Reflexionen und damit ohne Verluste durchgeleitet werden kann. Dazu müssen auch Resonanzbedingungen erfüllt werden. Deshalb spricht man von »periodischer« Antennenkopplung. Im Gegensatz dazu ist die »aperiodische« Antennenkopplung zu sehen, bei der ein unabgestimmtes Stück Draht an den abgestimmten Eingangskreis angekoppelt wird, z. B. die Teleskopantenne eines Transistorradios. Der Regelfall sind jedoch die periodischen Antennen.

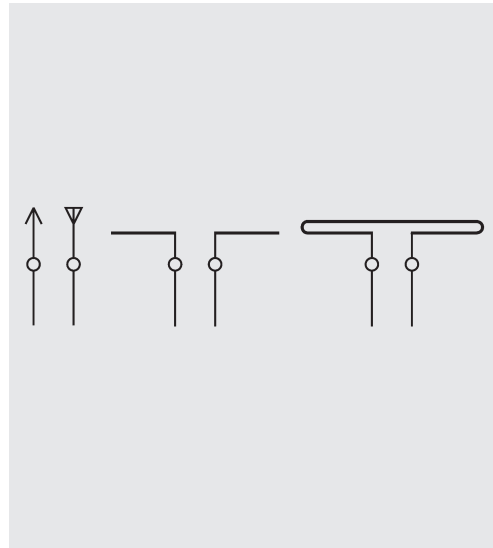
Bauformen der Antennen

Die Vielfalt der jeweiligen Funkdienste und ihre zudem noch unterschiedlichen Aufgabenstellungen führen zu einer entsprechend großen Zahl von Bauformen, von denen hier nur einige typische Bauformen genannt werden sollen. Die bekannteste und verbreitetste Antenne ist der schon von Heinrich Hertz verwendete abgestimmte Dipol, genauer der Dipol von halber Wellenlänge.

Die ideale Antenne:

Der Isotrop- oder Kugelstrahler

Dieser Dipol ist häufig der Bezugsdipol für Antennenvergleiche wie die Angabe von Antennengewinn oder Richtcharakteristik, weil er gleichmäßig in alle Richtungen strahlt. Das gilt streng genommen jedoch nur für die Ebene, auf der dieser Dipol senkrecht steht, seine Äquatorebene. Vertikal dazu hat er in Richtung des Drahtes deutliche Einbrüche an den Polen. Deshalb verwendet man heute als theoretischen Bezug einen gedachten idealen Kugelwellenstrahler (Isotropstrahler), der die HF-Energie in alle Richtungen gleich intensiv abstrahlen würde. Dieser hat per Definition den



Schaltungssymbole: Links einpolige Langdraht- und Stabantenne, rechts zwei Dipolantennen

Antennengewinn 0 dB. Antennengewinne werden auf diese beiden Antennen bezogen und in dBd für den Halbwellendipol und dBi für den Isotropstrahler angegeben. Der Wert für einen Hertzschen Dipol liegt bei 1,8 dBi.

Eine mögliche Unterteilung von Antennen nach ihrer Bauform ist:

- Linearstrahler (lineare Antennen; hierzu gehört der Dipol)
- Gruppenantennen (z. B. Sendeantennen für UKW und TV)
- Flächenstrahler (Flächenantennen) in zwei Bauarten:
 - Aperturstrahler und
 - Reflektorantennen (z. B. Satellitenschüssel und Richtfunkparabole)

Weitere Antennen-Bauformen, die sich nicht unter die vorgenannten Typen einordnen lassen, sind z. B.:

- Wendelantennen (Abstrahlung in Richtung der Achse einer Draht- oder Streifenwendel, zirkuläre Polarisation)

- Vivaldi-Antennen (zweidimensionaler Exponentialtrichter am Ende einer Schlitzleitung)
 - Antennen, die durch Schlitze in Hohlleitern entstehen (Abstrahlrichtung quer oder längs zum Hohlleiter)
 - Spiralantennen, Abstrahlung beidseitig senkrecht zu einer aus Streifenleitungen gebildeten Spirale, zirkular polarisiert
 - Fraktalantenne
 - Topfantenne
 - Patchantennen und PIFA auf Leiterplatten
 - T2FD (Bauform ähnlich einem Faltdipol, durch einen Abschlusswiderstand aber ohne Resonanzeffekte)
- Einige häufig eingesetzte Bauformen werden im Folgenden kurz erläutert.

Lineare Antennen

Lineare Antennen wandeln eine leitungsgeführte stehende Welle in Freiraumwellen um und umkehrt. Zu dieser Kategorie gehören alle Formen von Langdrahtantennen sowie Dipolantennen und Faltdipole. Praxisbeispiele für lineare Antennen sind Rundfunk-Sendemasten für Lang- und Mittelwelle, Drahtantennen für Amateur- und Schiffsfunk, $\lambda/2$ -Dipole als Strahler in Yagi-Antennen und $\lambda/4$ -Dipole in Stabantennen für Funkdienste, Funktelefone, CB-Funk usw.

Verkürzte lineare Antennen

Um die feste Relation von Antennenlänge zu Wellenlänge zu durchbrechen und die Konstruktion von deutlich kleineren Antennen zu ermöglichen, kann man in der Nähe des Speisepunktes eine Induktivität einfügen. Diese wirkt als »elektrische Verlängerung«. So sind Antennen realisierbar, die wesentlich kleiner sind als ein Viertel der Wellenlänge. Gleiche Wirkung erzielt zusätzliche Kapazität am Ende des verkürzten Elementes. Derartige Antennen sind oft gekennzeichnet durch höhere Verluste, kleineren Antennengewinn und kleineren Wirkungsgrad.

Halb- und Viertelwellendipol

Die Länge dieses Dipols entspricht der halben Wellenlänge. Da im Speisepunkt ein Strommaximum und ein Spannungsminimum vorliegt, weist diese Antenne eine niedrige Impedanz von $73,2 \Omega$ auf. Von einem Faltdipol spricht man, wenn der Stromweg eines Halbwellendipols auf zwei Wege aufgeteilt wird. Bei ihm vervierfacht sich die Impedanz des Speisepunktes auf etwa $240 - 300 \Omega$. Er kann geerdet am Antennenträger befestigt und als preiswerte symmetrische Zweidrahtleitung verwendet werden.

Eine Sonderform stellt der Viertelwellendipol dar, bei dem nur der eine Zweig des Halbwellendipols als Antennenstab verwendet wird. Die Funktion der anderen Hälfte übernimmt z. B. eine elektrisch leitfähige Oberfläche. Auch der Körper des Benutzers kann diese Funktion übernehmen, z. B. bei Handfunkgeräten.

Magnetische Antennen

Magnetische Antennen verwenden nicht das elektrische Feld, sondern ein Magnetfeld zur Strahlungserzeugung bzw. sie empfangen primär die magnetische Feldkomponente der elektromagnetischen Strahlung. Sie bestehen aus Spulen (im einfachsten Fall mit nur einer Windung), besitzen eine Richtwirkung (bei stehender Spule eine Achtcharakteristik) und können gegenüber der Wellenlänge sehr klein sein, wenn die Spule aus mehreren Windungen besteht.

Zu den Magnetantennen zählen auch die Rahmenantennen, aus einer drehbaren Spule bestehende Peilantennen und Ferritantennen. Übrigens hat eine magnetische Antenne zur Entdeckung der Funkwellen geführt. Es war die zweite Funkenspule, die bei Heinrich Hertz im selben Laborraum lag und Funken zeigte.

Phased Array- und dielektrische Antennen

Eine weitere Bauform sind die »Phased Array-Antennen« die am ehesten zu den Aperturstrahlern





Typische Antenne für steuerte Wireless-Geräte



Alternativ-Antenne mit Sperrtopf

zählen. Ihre Richtcharakteristik kann elektronisch erzeugt werden, so dass sie in der Lage sind, ihr Richtdiagramm zu verändern und zu schwenken, ohne sich selbst mechanisch bewegen oder verändern zu müssen. Sie bieten zugleich eine Fähigkeit zur Störunterdrückung, indem sie eine Nullstelle ihres Richtdiagrammes auf den Störer legen können und ihn so einfach ausblenden.

Schließlich sind gerade im Bereich von Dezimeter- und Zentimeterwellen mit gutem Erfolg so genannte dielektrische Antennen (z. B. Keramik-Antennen) im Kommen. Ihre Dielektrizitätskonstante ermöglicht kleinere Abmessungen, was ihre praktische Anwendbarkeit fördert, wenn kompakte Baumaße gewünscht sind. Sie sind allerdings verlustbehaftet und vertragen nur geringe Leistungen. Aber das stört z. B. bei SRD-Anwendungen weit weniger als die abstehenden Dipole.

Anschluss von Antennen über Koaxialkabel

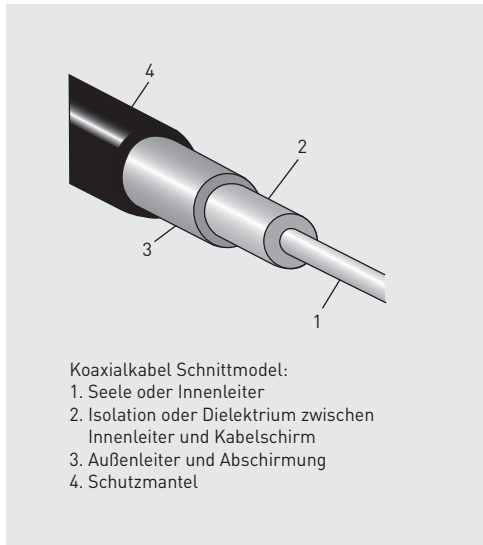
Zum Anschluss von Antennen verwendet man spezielle Kabel, so genannte Koaxialkabel. Hier

handelt es sich um zweipolige Kabel mit konzentrischem Aufbau, die aus Innen- und Außenleiter bestehen. Zwischen ihnen befindet sich ein Isolator, der auch aus Luft bestehen kann. Übliche Koaxialkabel haben einen Außendurchmesser von 2 bis 15 mm, Sonderformen bis 100 mm. Es gibt auch eine koaxiale Bauform von Freileitungen.

Die Innenleiter von flexiblen Koaxialkabeln werden meist aus geflochtenen oder verseilten Kupferdrähten gefertigt. Der Kabelschirm besteht auch aus solchen Kupferdrähten und kann durch eine Folie ergänzt sein. Koaxialkabel besitzen einen definierten Leitungswellenwiderstand. Er beträgt für die Rundfunk- und Fernsehempfangstechnik üblicherweise 75 Ohm, für andere Anwendungen sind 50 Ohm üblich.

Antennensimulation

Bei der Auslegung von Antennen sowie der Bestimmung von Antennenparametern kommt der computergestützten Simulation immer größere Bedeutung neben dem Berechnen bzw. der mess-



Aufbau eines Koaxialkabels

technischen Bestimmung zu. Auf diese Weise kann man die gewünschten Werte unter Berücksichtigung der in der Nähe befindlichen weiteren Einflussfaktoren wie Masten, metallische Abstrahlflächen etc. genau ermitteln. Parameter wie die Richtcharakteristik für jede Polarisationsrichtung sowie die Antennenimpedanz können ebenso berechnet werden wie z. B. die Abstrahlcharakteristik für eine definierte Frequenz sowie die Impedanzwerte über den gesamten oder für einen definierten Frequenzbereich. Zudem geben die Programme häufig auch die Stromverteilung entlang der Antenne an. Diese Information kann als Basis für die Optimierung vorhandener Antennen genutzt werden.

Antennen: Ein zentrales Thema der Funktechnik

Eine umfassende Übersicht über die Antennentechnik und die verschiedenen Antennenbauformen würde den Rahmen dieses Buches sprengen. Umfassendere Informationen findet man bei Wikipedia unter dem Artikel »Antennentechnik«, auf dem Teile dieser Zusammenfassung beruhen.

Darüber hinaus gibt es Fachbücher, die sich speziell mit der Antennentechnik befassen. Deren Lektüre kann man nur empfehlen: Nach Erfahrungen von steute werden hier in der Praxis sehr häufig Fehler gemacht, da viele Konstrukteure sich erst in die Thematik der »Wireless Automation« einarbeiten müssen. Ein besonders extremes Beispiel: Ein steute-Techniker wurde wegen der nicht funktionierenden Funkverbindung eines »Energy Harvesting«-Schalters zum Kunden gerufen. Die Ursache war schnell gefunden: Der Kunde hatte Angst, dass die Antenne Schaden nimmt, und sie sorgfältig in ein Metallrohr »gepackt«.

// Wireless-Technologien und-Produkte von
steute für die Medizintechnik

011

Erste Anwendungen in der Medizintechnik

Seit mehr als zehn Jahren befasst sich die Entwicklungsabteilung von steute mit Wireless-Technologien. Den Anfang machte der damalige Geschäftsbereich Medizintechnik (heute: steute Meditec), der Stalleinrichtungen für medizintechnische Geräte entwickelt und fertigt. In diesem anspruchsvollen Markt verwendet man häufig Fußschalter, um die Geräte zu steuern. Die Hygieneanforderungen sind dabei so hoch, dass sie mit kabelgebundenen Stalleinrichtungen nicht immer zu erreichen sind. Zudem schränken die Kabel die Bewegungsfreiheit und Ergonomie des Personals bzw. des Operators ein.

Start mit Infrarot

Die ersten kabellosen Schaltgeräte, die steute für die Medizintechnik entwickelte, nutzten Infrarot als Übertragungsmedium. Für eine Oralkamera wurde beispielsweise ein Fußschalter entwickelt, der eine kabellose Steuerung der Kamera per IR-Signal ermöglicht. Diesen Verfahren sind jedoch enge Grenzen gesetzt, weil die Übertragung sehr gerichtet erfolgen muss. Die steute-Entwickler haben diesen Nachteil ausgeglichen, indem sie ein sehr energiereiches Signal einsetzen. Auf diese Weise kann man die Reflexionen und Abstrahlungen ausnutzen, die z. B. von den Wänden des OP ausgehen. Zudem senden die Schalter Signale in verschiedenen Frequenzbereichen, um eine hohe Übertragungssicherheit zu erreichen.

Einstieg in die 868 MHz-Technologie

Darauf folgte der Einstieg in die 868 MHz-Technologie – mit einem Fußschaltgerät vom Typ MKF-MED GP23. Allerdings waren diese Schalter nicht weltweit einsetzbar. Zudem handelte es sich hier, was die Randbedingungen angeht, um einen Sonderfall: Die Fußschalter wurden ausschließlich in MRT-Räumen eingesetzt, die hermetisch gegen Strahlung geschirmt sind. Deshalb gab es mit der 868 MHz-Technik in diesem Fall keine Probleme in Bezug auf Koexistenz und Übertragungssicherheit.

Nächster Schritt:

Neuer Standard auf Bluetooth-Basis

Daher als nächster Schritt im Jahr 2003 der Entschluss, den Bluetooth-Standard im lizenzfreien 2,4 GHz-ISM-Frequenzbereich für die Entwicklung einer neuen Generation von Funk-Bediengeräten für die Medizintechnik zu nutzen. Die Entscheidung für Bluetooth fiel aus mehreren Gründen:

- Das Frequenzband ist lizenzfrei und weltweit einheitlich nutzbar.
- Mit einer Reichweite von 10 bis 100 Metern ist der Standard für den Ersatz herkömmlicher Verkabelungen im Medizintechnik- und Industrie-Einsatz sehr gut geeignet.
- Zahlreiche Geräte können parallel betrieben werden.
- Die Signale sind aufgrund von Frequenzspreizverfahren wie dem Frequency-Hopping störfest und eignen sich damit bestens für sicherheits-sensible Einsätze.
- Die Koexistenz zu anderen Funknetzen (z. B. den in Krankenhäusern verwendeten WLAN-Netzen) ist gegeben.

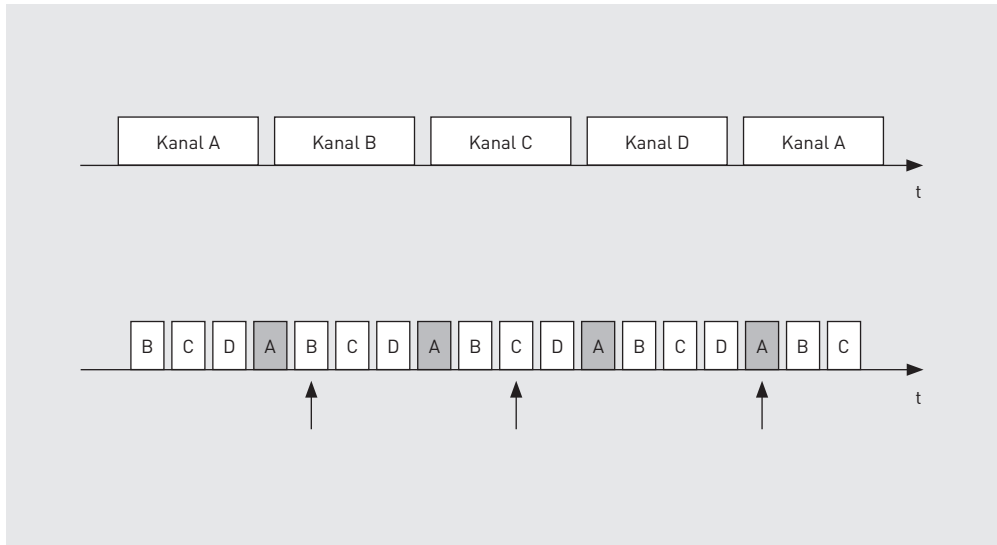
Anpassung an die hohen

Sicherheitsanforderungen

Allerdings musste der Bluetooth-Standard individuell an die hohen Sicherheitsanforderungen der Medizintechnik angepasst werden. Denn zwei »normale« Bluetooth-Geräte können prinzipiell miteinander Daten austauschen – genau das ist ein wesentliches Ziel des Bluetooth-Protokolls. Genau das muss bei den von steute entwickelten Stalleinrichtungen jedoch vermieden werden: Hier muss eine eindeutige Zuordnung von medizintechnischem Gerät und dem dazugehörigen Fußschalter (oder Handbediengerät) gewährleistet sein. Deshalb nutzt das von steute weiterentwickelte bzw. an die Anforderungen angepasste Bluetooth-Protokoll einen individuellen Konfigurationsbereich.



Das universelle RF/BT-Modul mit der Bluetooth-Anbindung kann in unterschiedlichste Stalleinrichtungen integriert werden



Kanal-Hopping während des Verbindungsaufbaus

Individuelle Konfiguration für jedes Bluetooth-Modul

In das Modul können Herkunft und Fähigkeiten des Gerätes eingegeben werden. Neben den Daten zur Klassifikation des Moduls, wie Name des Herstellers, Gerätetyp und Geräteklasse (z. B. Fußschalter), sind hier auch Daten zur Konfiguration des Moduls hinterlegt – z. B. die Anzahl und Funktion der digitalen und analogen Ein- und Ausgänge. Darüber hinaus können auch Betriebs-einstellungen wie Alarm- und Warnzeichen sowie die Übertragungsgeschwindigkeit der seriellen Schnittstelle eingestellt werden. Über diese Konfigurationsdaten können Sender und Empfänger schon während des Verbindungsaufbaus überprüfen, ob sie kompatibel sind und damit ein gefahrloser Betrieb möglich ist.

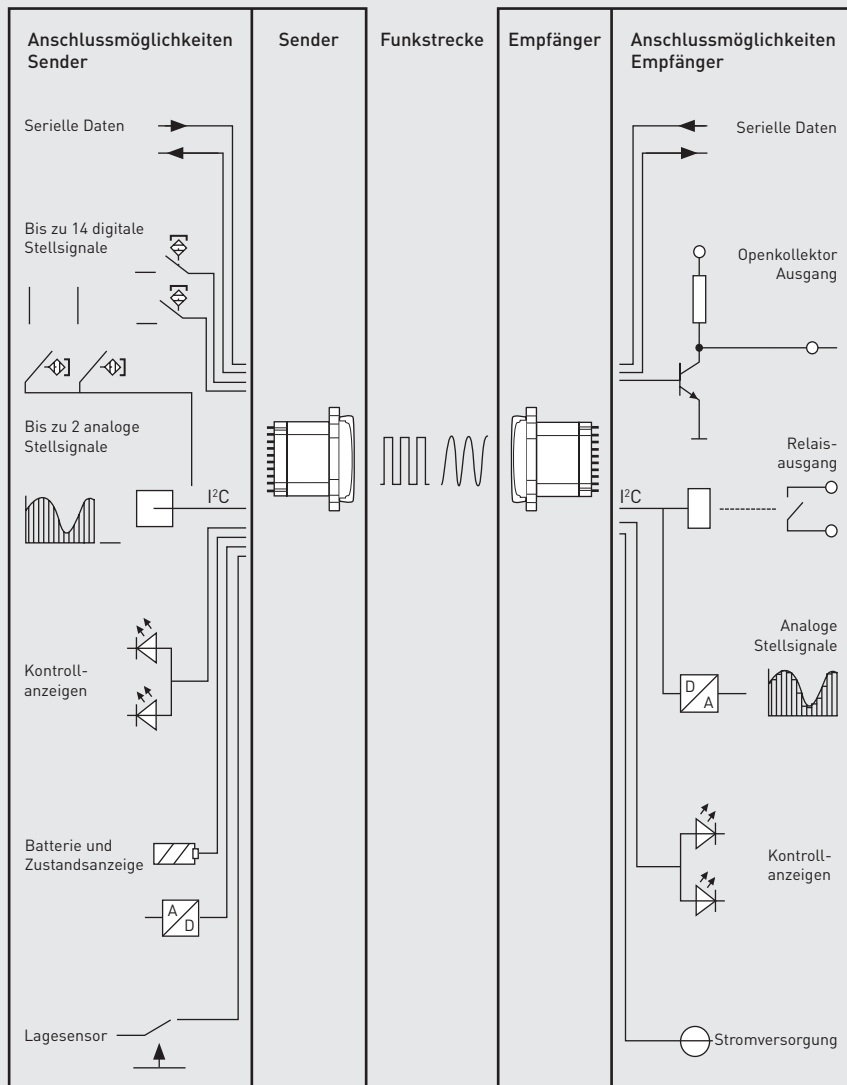
Anmeldeverfahren überprüft Kompatibilität von Schalter und Gerät

Um die Betriebssicherheit noch weiter zu erhöhen und die Kompatibilität von Fußschalter und Gerät sicherzustellen, hat steute eine Reihe wei-

terer innovativer Funktionen integriert. So wurde ein spezielles Anmeldeverfahren entwickelt, über das die Fußschalter einmalig mit dem Gerät »verheiratet« werden. Hierfür hat steute verschiedene Verfahren entwickelt. Zum Beispiel wird über eine Infrarot-Strecke ein zweiter Datenkanal aufgebaut, auf dem Sender und Empfänger Kenn-daten austauschen. Oder man nutzt ein Backup-Kabel als einmalige Kabelverbindung. Alternativ kann das Pairing auch über das Drücken einer Taste am Medizingerät eingeleitet werden. Neben einer individuellen und weltweit nur einmal vergebenen Identifikationsnummer tauschen Sender und Empfänger auch die Hersteller- und Konfigurationsdaten aus.

Sensorik vermeidet Fehlbedienungen

Weil kabellose Fußschalter nicht mehr ortsgelungen sind, muss man besondere Vorsorge treffen, um versehentliche Fehlbedienungen zu vermeiden. Deshalb überwachen Sensoren permanent die Lage des Fußschalters. Wird der Schalter vom Boden abgehoben, werden automatisch alle



Der von steute genutzte Funkstandard bietet vielfältige Anschlussmöglichkeiten auf Sender- und Empfängerseite

Schaltfunktionen gesperrt und ein Warnsignal erzeugt. Wenn der Schalter dann über einen längeren Zeitraum (der im Bereich zwischen 1 und 60 Sekunden konfigurierbar ist) nicht zurückgesetzt wird, unterbricht er automatisch die Funkübertragung.

Universell einsetzbar mit RF/BT-Modul

Zum Erfolg der von steute entwickelten Wireless-Schaltgeräte in der Medizintechnik hat sicherlich die Tatsache beigetragen, dass das Medizintechnik-Programm von steute als Modulsystem konzipiert ist. Der Anwender kann jeweils zwischen einer kabelgebundenen und einer Wireless-Version wählen. Bei den Wireless-Varianten wird das Kabel durch ein kompaktes Modul ersetzt, das die Funkplatine, handelsübliche Akkus und die Antenne enthält.

Alle Ein- und Ausgangssignale des RF/BT-Moduls sind auf den 26-poligen Steckverbinder am Platinenrand geführt. Mit einer minimalen externen Beschaltung lassen sich verschiedene digitale Schaltfunktionen verwirklichen. Auf der Geräte-seite kommt ein kompaktes Empfangsmodul zum Einsatz, das in der Regel in das Kundensystem integriert wird.

Vielseitig: Die Peripherie des RF/BT-Moduls

Zusätzliche Peripherie-Bausteine können über den I²C-Bus an das RF/BT-Modul angeschlossen werden. So lassen sich bis zu vierzehn digitale und zwei analoge Stellsignale übertragen. Die maximale Reaktionszeit beträgt dabei 50 ms. Außerdem ist eine serielle Schnittstelle mit einstellbarer Übertragungsgeschwindigkeit vorgesehen. Abhängig von der externen Beschaltung erlaubt dieses kabellose Interface, asynchrone kabelgebundene Schnittstellen wie RS 232 durch das RF/BT-Modul zu ersetzen.

Spannungsversorgung: Verbesserungsbedarf

Diese von steute entwickelte Technologie etablierte sich in der Medizintechnik. Sie kommt so-

wohl bei relativ einfachen Fußsteuerungen wie ein- bis zweipedaligen Fußschaltern zum Einsatz, aber auch bei sehr komplexen OP-Einrichtungen. In einem sehr wichtigen Punkt sahen sowohl die Entwickler von steute als auch die Anwender noch Verbesserungsbedarf: Der Stromverbrauch der kabellosen Schaltgeräte ist trotz des intelligenten Powermanagements relativ hoch. Da der Verbindungsaufbau bei Bluetooth relativ lange Zeit benötigt, muss die Verbindung dauerhaft aufrecht erhalten bleiben. Das kostet eben Energie und ist häufig nicht akzeptabel. Dies war der Ansatzpunkt für eine neue Entwicklung.

Neue Entwicklung:

Energiesparende 2,4 GHz-Funktechnik

Der »steute wireless«-Standard für die Medizintechnik wurde u. a. mit dem Ziel entwickelt, einen deutlich niedrigeren Energieverbrauch und damit wesentlich längere Batteriestandzeiten zu erzielen als dies bei Bluetooth-Systemen der Fall ist.

Erreicht wird dies durch ein System, das genau wie Bluetooth das weltweit verfügbare, lizenzfreie 2,4 GHz-Band nutzt, jedoch speziell für die Kommunikation von einem oder zwei Fußschaltern (Slave) mit einem Empfänger (Master) entwickelt wurde. Die Initiative zum Verbindungsaufbau geht immer vom Fußschalter aus. Der Empfänger (dessen Energieversorgung unkritisch ist) ist ständig aktiv und wartet auf einen Verbindungsversuch des Fußschalters.

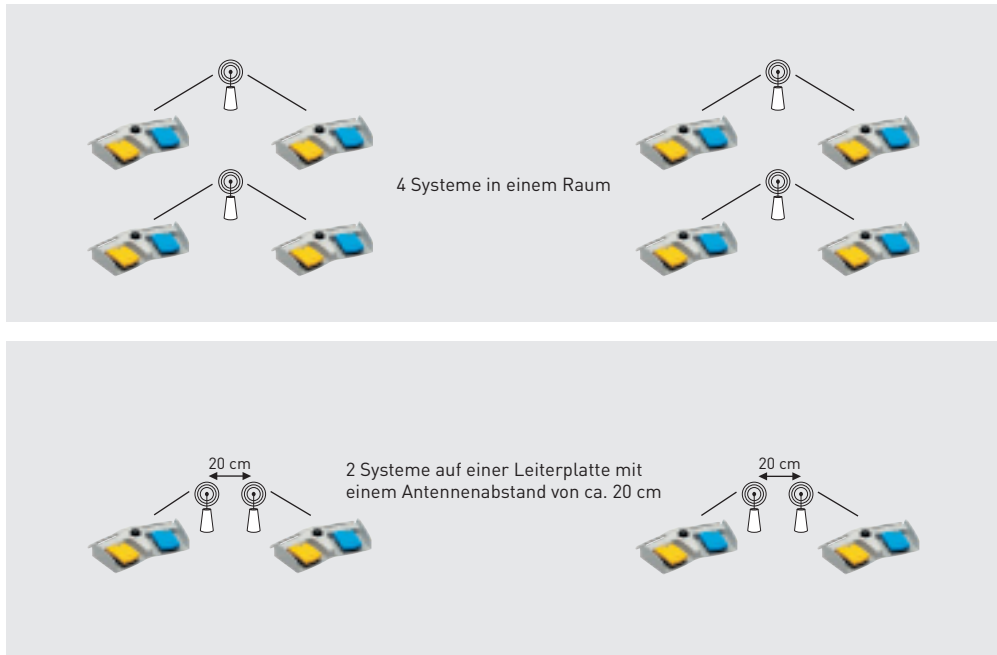
Schnelle Reaktionszeit,

Batterielaufzeiten bis zu einem Jahr

Nach diesem Prinzip erfolgt eine Verbindung mit Kanal B nach 25 ms und eine Verbindung mit Kanal A nach 80 ms. Hinzu kommen jeweils 40 ms für das Senden und Empfangen eines Ersttelegramms. Nach spätestens zwei Durchläufen ist die Verbindung aufgebaut. Hieraus ergibt sich eine Verbindungszeit von 25 ms bis maximal 200 ms. Damit wird die Voraussetzung dafür geschaffen, die Bediengeräte bei Nichtbetätigung in



Die Ophthalmologie ist eine der medizinischen Disziplinen, für die steuerte komplexe kundenspezifische Stelleinrichtungen entwickelt.



Bei steute Wireless können zwei Empfänger in einem Gerät untergebracht und bis zu vier Funkssysteme in einem OP betrieben werden.

einem energiesparenden Sleep-Modus zu betreiben, aus dem sie nach maximal 200 ms »aufgeweckt« werden können.

Durch diese zusätzliche Funktion der »steute Wireless«-Technologie lassen sich kabellose Stilleinrichtungen mit Batterielaufzeiten bis zu einem Jahr betreiben. Es werden Reichweiten von nominal 10 Meter erreicht, und ein fehlerfreies Senden und Empfangen ist selbst beim Betrieb mehrerer WLAN-Netze, die ebenfalls im 2,4 GHz-Netz arbeiten, gewährleistet.

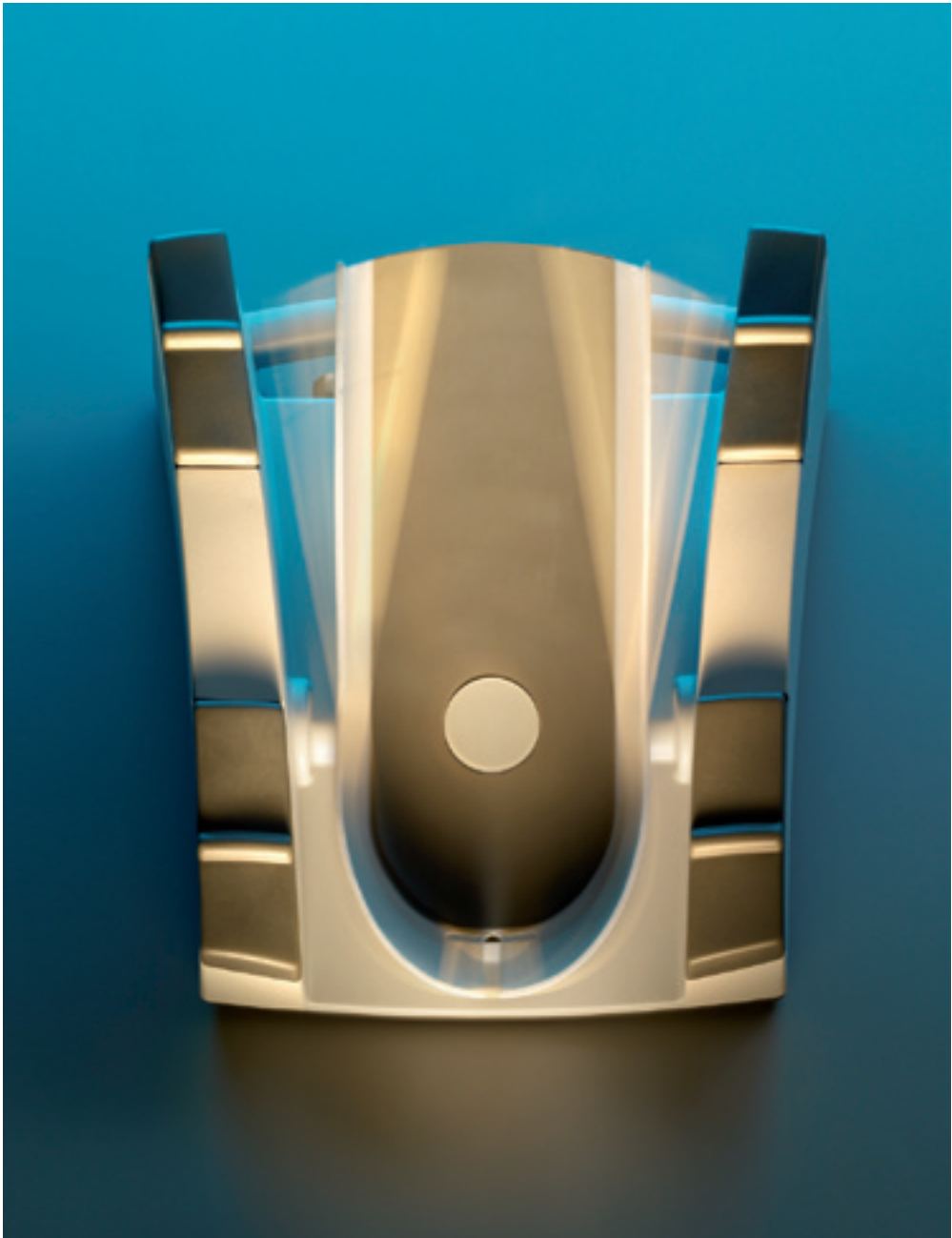
Der Betrieb von mehreren Empfängern in einem medizintechnischen Umfeld ist problemlos möglich, wenn die Antennen der Empfänger einen Mindestabstand von 20 cm einhalten. Auf diese Weise lassen sich bis zu vier Sender-/Empfänger-

Paare in einem OP anordnen, ohne dass sie sich gegenseitig stören (siehe Bild Seite 186). Dieses System befindet sich bereits erfolgreich im Feldeinsatz und ist aus Sicht von steute die Technologie der Wahl für Wireless-Anwendungen in der Medizintechnik. Bluetooth wird weiterhin überall dort seine Daseinsberechtigung behalten, wo große Datenmengen zu übertragen sind.

Beispielhafte Lösung:

Stelleinrichtung für die Phacoemulsifikation

Eine Stelleinrichtung für die Ophthalmologie (Augenheilkunde) verdeutlicht beispielhaft die Funktionen, die steute-Fußschalter in der Medizintechnik übernehmen sowie die Vorteile der Funktechnik. Die weltweit am häufigsten durchgeführte Operation ist die Behandlung des Grauen Stars (Katarakt): Eine Trübung der Augenlinse, die



Diese Stalleinrichtung für die Phacoemulsifikation übermittelt die Signale des Operateurs per Funk an die Steuerung des OP-Gerätes.

zur Erblindung führt und die heute dadurch geheilt werden kann, dass man die getrübte Linse entfernt und durch eine künstliche Linse ersetzt.

Hierfür wurde das OP-Verfahren der Phacoemulsifikation entwickelt: Der Ophthalmologe durchtrennt mit einem nur wenige Millimeter großen Schnitt die Linsenkapsel des Auges und saugt die per Ultraschall emulsifizierte Linse ab. Dann bringt er durch die Öffnung eine eingerollte künstliche Linse ein, die sich anschließend »ausklappt«. Dieser schonende, minimal-invasive Eingriff erfordert höchste Präzision und Konzentration vom Operateur. Da er beide Hände für die Führung der Instrumente benötigt, werden alle wesentlichen Funktionen per Fuß über eine komplexe Steuereinrichtung gesteuert.

Im Zentrum der Bedieneinheit befindet sich ein Pedal, das in vier Freiheitsgraden verstellbar ist. Rechts und links vom Pedal sind vier Wippschalter angebracht, die in jeweils zwei Richtungen betätigt werden können, so dass sie für bis zu acht verschiedene Funktionen genutzt werden können.

Die Bedieneinrichtung ist so in die Steuerung des Phacoemulsifikations-Gerätes eingebunden, dass die einzelnen Schalter bei unterschiedlichen Prozessschritten bzw. Menüs jeweils unterschiedliche Funktionen übernehmen. Auf diese Weise kann man komplexe Abläufe mit einer überschaubaren Anzahl von Bedienelementen steuern. Das schafft die Voraussetzung für ergonomisches, intuitives Arbeiten: Der Operateur kann sich ganz auf den Patienten konzentrieren. Und die Bewegungsmöglichkeiten, die der Fußschalter bietet, werden nicht durch Kabel eingeschränkt.

Hohe Anforderungen – wachsende Verbreitung

Abschließend kann man sagen, dass die Funklösungen, die steute Meditec für die Medizintechnik entwickelt, immer kundenspezifisch an die jeweiligen Anforderungen angepasst sind. Das gilt

für den Funkstandard auf Bluetooth-Basis ebenso wie für das steute Wireless-System.

Unabhängig vom individuell eingesetzten Funkstandard ist immer ein bidirektionaler Signalaustausch gefordert – die Empfangsbestätigung einer Signalübertragung reicht wegen der hohen Anforderungen an die Übertragungssicherheit nicht aus. Deshalb ist die Zweikanaligkeit ein wichtiger Aspekt. Zudem sind hier analoge Systeme gefragt, da die Steuereinrichtungen häufig kontinuierliche Bewegungen ausführen und entsprechende Signale weitergeben.

Nach Einschätzung von steute werden Funktechnologien in der Medizintechnik künftig noch weitere Verbreitung finden: Die Akzeptanz ist hoch und die Vorteile z. B. im Hinblick auf Ergonomie und Hygiene offensichtlich. Die Nutzung von Funkstandards, die speziell für die Medizintechnik entwickelt wurden, und die lange Batterielebensdauer bei den neuesten Funktechnologien wird diese Entwicklung noch beschleunigen.



// Wireless-Technologien und -Produkte
von steute für die Industrie

012

Industrieanwendungen

Explosionsschutz

Industrie-Anwendungen: Untersuchung von Technologien und Marktpotenzial

Parallel zur Entwicklung der ersten Wireless-Fußschalter für den Geschäftsbereich Meditec untersuchte steute den Markt und das Marktpotenzial der Wireless-Technologien in Industrie-Anwendungen. Hier hatten sich bereits Standards etabliert, und steute hatte auf der Basis von Kundenanforderungen bereits erste Produktgenerationen entwickelt, die auf der Basis der 2,4 GHz-Technik arbeiteten.

Diese Lösungen haben sich bewährt, sie werden auch heute noch von Kunden gewünscht und von steute gefertigt. Allerdings entspricht diese Technologie nicht dem selbst gesetzten Anspruch des Unternehmens, Innovationen zu entwickeln und umzusetzen. Außerdem sind die vorherrschenden Wireless-Systeme aus Sicht von steute nur eine halbe Lösung: Die Signalübertragung erfolgt zwar per Funk, aber der Maschinenbauer sowie der Betreiber der Maschine bleiben nach wie vor auf eine kabelgebundene Energieübertragung angewiesen, sofern sie nicht auf wartungsaufwändige Batterietechnik ausweichen möchten.

Alleinstellungsmerkmal: Energieautarke Schaltgeräte für die Industrieautomation

Zudem bot der gut besetzte Markt der konventionellen »Wireless Automation« wenig Möglichkeiten, sich vom Wettbewerb der Schaltgerätehersteller in der Automatisierungstechnik zu unterscheiden. Diese Möglichkeit bot sich 2004, als das neu gegründete Unternehmen EnOcean GmbH die Idee der Energiegewinnung per »Energy Harvesting« für Schaltgeräte nutzbar machte und verschiedene Optionen vorstellte, um Energie aus der Umgebung zu gewinnen. Zu den Innovationen, die EnOcean damals präsentierte und mit denen das Unternehmen den renommierten Hermes Award 2004 gewann, gehörte z. B. ein Solarmodul mit miniaturisiertem Energiespeicher.

Kerntechnologie: Energiearmer Funkstandard

Mit der von EnOcean entwickelten Plattform war die technische Voraussetzung dafür geschaffen, tatsächlich auf Kabel und auch auf eine Batterie zu verzichten. Zu den EnOcean-Kerntechnologien gehören nicht nur die Module, die die Energie aus der Umgebung gewinnen. Mindestens ebenso wichtig ist der vom EnOcean-Gründer Frank Schmidt entwickelte Funkstandard, der mit sehr geringem Energiegehalt auskommt und dennoch eine hohe Übertragungssicherheit gewährleistet.

Rascher Erfolg in der Gebäudetechnik

steute gehörte zu den ersten Unternehmen, die die Bedeutung dieser Technologie erkannten, mit EnOcean einen Vertrag schlossen und mit der Entwicklung kabelloser und energieautarker Schaltgeräte begannen. Andere Unternehmen wie AEG Osram, Funkstuhl, Peha, Thermokon und Warema gingen ebenfalls diesen Weg. Allerdings waren alle anderen EnOcean-Partner in der Gebäudeautomation tätig. Hier bietet das »Energy Harvesting« ganz offenkundige Vorteile: Man kann bei der Elektroinstallation gänzlich auf Kabel zwischen Schaltern und elektrischen Verbrauchern (Licht, Rolladen, Beschattungssysteme, Lüftungsklappen etc.) verzichten und ist damit wesentlich flexibler, wenn Umbauten anstehen, wie sie sowohl in Verwaltungsgebäuden als auch in Industriebauten häufig nötig sind. In diesem Fall kann man z. B. die Lichtschalter einfach an anderer Stelle der Wand platzieren, ohne Kabel zu verlegen oder Kabelschächte zu ziehen.

Nutzung für die Automatisierungstechnik

steute adaptierte diese Technologie für die industrielle Automatisierungs- und Steuerungstechnik und nutzte für die erste Generation der energieautarken Schaltgeräte das EnOcean-Solarmodul, dessen integrierter Speicher einen Funkbetrieb auch während Dunkelperioden von bis zu 48 Stunden zulässt. Zu den Anwendern, die diese Technologie von Beginn an nutzten, gehört z. B. ein namhafter deutscher Hersteller von Bearbei-



Beispiel für die ersten Applikationen des »Energy Harvesting« in der Industrieautomation: Ein Türgriffschalter aus dem TGF-Programm an seitlich verschiebbaren Schutztüren ermöglicht den Verzicht auf verschleißanfällige Kabelschleppereinrichtungen



Die Solarzelle erzeugt die Energie zum Betätigen des Schalters.



Auch Befehlsgeräte gehören zum Programm der energieautarken Schaltgeräte.

tungszentren. Der Arbeitsraum der Maschinen wird durch große seitlich verschiebbare Schutztüren abgesichert. Um die Entriegelungstaste und andere Schaltfunktionen am Türgriff mit Energie zu versorgen, mussten die Konstrukteure eine aufwändige und verschleißanfällige Kabelschleppereinrichtung vorsehen. Ein Türgriffschalter aus dem TGF-Programm ermöglicht den Verzicht auf diese komplexe Art der Kabelzuführung: Die Energie, die die Schalter benötigen, wird durch das Solarmodul generiert, das ebenso in den formschönen Türgriff integriert ist wie mehrere Bedienelemente.

Weitere Innovation:

Der elektrodynamische Energiegenerator

Als weitere Innovation stellte EnOcean einen elektrodynamischen Energiegenerator vor, der die Energie, die zum Übertragen des Funksignals nötig ist, aus der Betätigung des Schalters generiert. Letztlich erzeugt also der Bediener, der den Taster betätigt, die Energie, und aus kinetischer wird elektrische Energie. Dieses Prinzip ist des-

halb besonders elegant, weil die Energie genau in dem Moment erzeugt wird, in dem sie auch benötigt wird. Das macht den Verzicht auf ein Speichermedium möglich, sofern – und das ist die Bedingung – kein Präsenzsinal erforderlich ist.

Umfassendes Programm

Inzwischen steht ein breites Programm an Funk-Schaltgeräten mit EnOcean-Technologie zur Verfügung. Dazu gehören Positionsschalter, Fußschalter, Seilzug- und Zugschalter, verschiedene Baureihen von Befehlsgeräten und die bereits erwähnten Türgriffschalter.

Selbstverständlich gibt es auch für die Empfängerseite verschiedene Lösungen: Neben ein- und mehrkanaligen Funkempfängern für den EnOcean-Standard gehört auch ein Repeater zur Erhöhung der Reichweite ins Programm.

Die Lösung aus dem Koffer

In der Industrie-Automation findet das Prinzip des »Energy Harvesting« immer größere Akzep-



»Plug and play«: Der Funk-Koffer enthält alle Komponenten, die man zum Betrieb eines Funk-Schaltgerätes braucht.

tanz, und steute fördert diese Entwicklung aktiv. Zum Beispiel gehören zum Programm der Funk-Schaltgeräte »Starterpakete« mit allen erforderlichen Komponenten, die im handlichen Koffer angeboten werden und die Zuordnung von Sender und Empfänger per automatisiertes Teach-in in wenigen Schritten erlauben. Diese Koffer stehen mit verschiedenen Arten von Schaltgeräten (z. B. Zugschalter und Positionsschalter) zur Verfügung.

Kreativität der Anwender

In der Praxis zeigt sich, dass die Anwendungen der energieautarken Schaltgeräte nicht nur in der Gebäudetechnik, sondern auch in der Industrieautomation sehr vielfältig sind, denn die Konstrukteure sind sehr kreativ beim Finden neuer Einsatzfelder. Häufig findet man zum Beispiel energieautarke Zugschalter, deren Zugseil zum Öffnen und Schließen von Rolltoren verwendet wird. Hier ist die Montage eines kabelgebundenen Schalters oft sehr aufwändig, weil lange Leitungswege an hohen Hallenwänden und -decken verlegt werden müssen.

Ein weiterer Einsatzbereich sind energieautarke Seilzugschalter an den Montagebändern der Automobilindustrie. Hier wirkt der Schalter als »Reißleine« bei Qualitätsproblemen. Mit ihm wird entweder ein Signal an eine Leitwarte gegeben oder – so entspricht es dem berühmten »Toyota Production System« – das gesamte Band stillgesetzt, um das erkannte Problem sofort zu beheben.

In neueren Anwendungsfällen, die eher der Gebäude- als der Steuerungstechnik zuzurechnen sind, übernehmen Funk-Schaltgeräte mit EnOcean-Technologie Überwachungsfunktionen z. B. bei Solaranlagen und bei Feuerlöschanlagen.

Generell kann man sagen: Im gesamten Maschinen- und Anlagenbau erlauben energieautarke Schaltgeräte flexiblere Konstruktionen an beweglichen oder autarken Anlagenteilen und eine einfachere, kostengünstigere Installation. Dies gilt auch für die Nachrüstung vorhandener Maschinen mit kabellosen und energieautarken Schalt-



Energieautarke Zugschalter werden zum Öffnen und Schließen von Rolltoren verwendet

geräten – auf diese Weise kann man häufig die Produktivität und Ergonomie der Maschine erhöhen, Verschleißteile substituieren und die Verfügbarkeit erhöhen.

Weiterentwicklung für die Anforderungen der Industrieautomation

So innovativ der Einsatz der energieautarken Schaltgeräte in der Industrieautomation auch ist, so muss man doch eine Einschränkung machen: Der von EnOcean entwickelte Energiegenerator ist für Einsätze in der Gebäudetechnik entwickelt worden und deshalb für 50.000 Betätigungen ausgelegt. Das ist in diesem Bereich völlig ausreichend, in industriellen Einsätzen können aber bis zu 5000 Betätigungen pro Tag auftreten. Das war für steute der Anlass einer Neuentwicklung, die dieselbe Platine nutzt, aber eine andere, deutlich langlebigere Mechanik verwendet.

Eigenes System in 868 MHz-Technik

Darüber hinaus gab es von den Anwendern der ersten Stunde zusätzliche Wünsche, die u. a. die

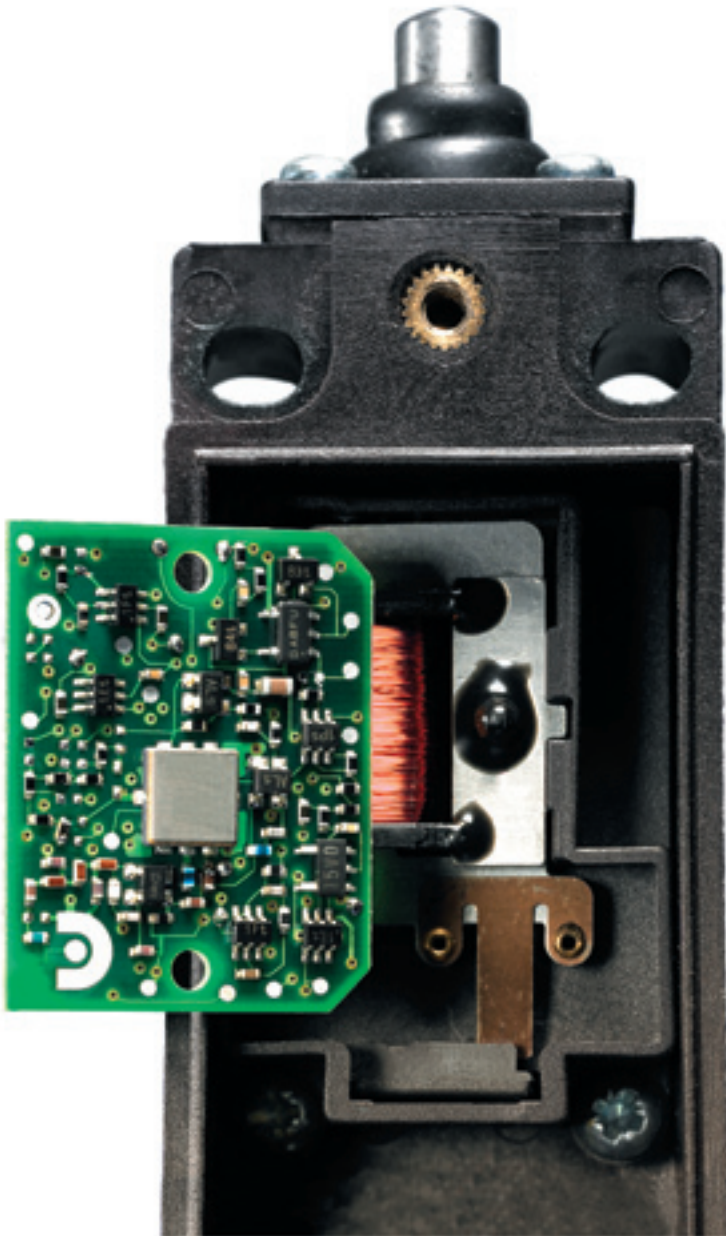
Baugröße des Systems, die Reichweite und die Bidirektionalität der Funk-Kommunikation betreffen. Auch diese Wünsche – so war es erklärtes Ziel von steute – sollten erfüllt werden.

Allerdings ließen sich die Entwicklungsziele nicht auf der Basis der EnOcean-Technologie verwirklichen. Deshalb wurde im Jahr 2010 ein komplett neues Funksystem auf der Basis der 868 MHz-Technik entwickelt. Die Platine dieses Systems wurde gegenüber der EnOcean-Plattform deutlich verkleinert. Zugleich arbeitet der Funkstandard bidirektional, was eine nochmals höhere Übertragungssicherheit gewährleistet, und die Reichweite ist deutlich höher: Im Freifeld werden 700 bis 800 Meter erreicht, während es bei der EnOcean-Technologie nur 300 Meter sind.

Wichtig: Bidirektionalität und hohe Reichweite

Sehr wichtig war vielen Kunden von steute auch die Bidirektionalität, die bis vor Kurzem mit energieautarken Schaltgeräten nicht zu erreichen war. Beim ursprünglichen EnOcean-Standard sendet der Empfänger keine Empfangsbestätigung als Rückmeldung. Zwar gibt es neuerdings mit dem Dolphin-System auch einen bidirektionalen EnOcean-Standard. Das von steute entwickelte energieautarke 868 MHz-System kombiniert den bidirektionalen Datenaustausch jedoch mit höherer Reichweite.

Dabei ist es durchaus anspruchsvoll, bei einem System mit geringer Energiemenge und ohne Speichermedium eine solche Bidirektionalität zu erreichen. Die steute-Entwickler haben diese Herausforderung gemeistert, indem das Signal gesendet und dessen Empfang bestätigt werden, während der elektrodynamische Energiegenerator betätigt wird. Die Rückmeldung wird dann in einem EPROM im Sendergerät gespeichert und bei der nächsten Übertragung mitgesendet. Somit kann man auf ein Speichermedium für Energie verzichten und dennoch das Senden einer Empfangsbestätigung gewährleisten.



Wireless-Positionsschalter mit elektrodynamischem Energiegenerator



Funkschalter in ungewöhnlicher Form: Der Wireless Cube RF 10

Neue Wege auch bei batteriegestützten Funkstandards

Auf den ersten Blick ist es nicht ersichtlich, warum ein Anwender der EnOcean-Technologie ein batteriegestütztes System wünscht. Dafür gibt es jedoch gute Gründe. Entweder soll nach jedem gesendeten Signal eine Empfangsbestätigung gesendet werden, oder man wünscht ein regelmäßiges Statussignal. Da der Energieverbrauch des Systems aufgrund des niedrigen Energiegehaltes des Signals sehr gering ist, kann man sehr langlebige Batterien, in vielen Fällen sogar Lifetime-Batterien, einsetzen.

Ein zentraler Faktor ist dabei auch das Know-how bei der sicheren Beschaltung der Ein- und Ausgänge. Auch deshalb befindet sich das Standardmodul immer auf einem von steute entwickelten Motherboard.

Der »Wireless Cube RF 10«

Ein gutes Beispiel für einen neu entwickelten batteriebetriebenen Funkschalter ist der Wireless Cube RF 10.

Er ist extrem kompakt gebaut und lässt sich auch an unzugänglichen Stellen ganz einfach in die Umgebungsstruktur integrieren. Der EnOcean-Standard erlaubt typische Reichweiten von 300 Meter im Freifeld und 30 Meter in Gebäuden. Die Schalterelektronik wird über eine handelsübliche Batterie mit Energie versorgt, die mit einfachem Werkzeug ausgetauscht werden kann. Als Betätiger des Schaltgerätes dient eine Tastfeder, die auf einen Mikroschalter wirkt. Dabei wird nur ein geringer Betätigungsweg zurückgelegt, und die nötige Betätigungskraft ist ebenfalls gering. Alternativ kann das Gerät auch als Magnetschalteausrückführung mit einem Reed-Kontakt bestückt werden.

Neben der kompakten Bauform und der unkomplizierten Montage zählt die Langlebigkeit zu den besonderen Merkmalen des Funkschalters. Die mechanische Lebensdauer liegt bei über einer Million Schaltspielen, und auch bei sehr hoher Schalthäufigkeit ist das kompakte Gerät in seinem Element: Es kann bis zu 1.800 Schaltspiele pro Stunde ausführen.

Mit diesen Eigenschaften ist der neue Wireless Cube RF 10 das ideale Schaltgerät für schlecht zugängliche und beengte Einbausituationen in Maschinen und Anlagen der industriellen Automation – und eine wirtschaftliche Alternative zu konventionellen kabelgebundenen Positionsschaltern.

// Explosionsschutz

Wireless-Technologien in explosionsgefährdeten Bereichen

Da steute seit jeher eine hohe Kompetenz bei der Entwicklung und Fertigung von Schaltgeräten für explosionsgefährdete Bereiche hat, lag es nahe,



Für explosionsgefährdete Bereiche stehen auch verschiedene Funk-Bediengeräte zur Verfügung

die in der Industrieautomation eingesetzte EnOcean-Technologie auch bei Ex-Schaltgeräten einzusetzen – zumal die Energieautarkie in diesem Anwendungsbereich zusätzliche Vorteile bietet, denn jede kabelgebundene Verbindung ist ein potenzielles Risiko. Und wenn die Schaltgeräte aus den explosionsgefährdeten Zonen »herausfunken«, kann man konventionelle, deutlich kostengünstigere Empfangsgeräte einsetzen.

Aus diesen Gründen hat sich steute frühzeitig mit der Möglichkeit beschäftigt, die EnOcean-Technologie mit elektrodynamischem Energiegenerator auch für Ex-Schaltgeräte zu nutzen. Dazu mussten die Geräte zunächst an die anspruchsvollen Anforderungen des Explosionsschutzes angepasst werden. Dies gilt sowohl für die mechanische als auch für die elektrische Konstruktion.

Bei der Zertifizierung der Geräte nach ATEX-Richtlinie 94/9/EG waren allerdings Hürden zu überwinden, weil zunächst geeignete Prüfstandards entwickelt werden mussten. Dies ist inzwischen geschehen, und steute bietet ein umfassendes Portfolio an »Wireless Ex«-Schaltgeräten, das für den Einsatz in den Gas-Ex-Zonen 1 und 2 sowie den Staub-Ex-Zonen 21 und 22 zertifiziert ist. Das Programm umfasst u. a. Befehlsgeräte, Positionsschalter, Zugschalter und Fußschalter.

Auch bei den energieautarken Ex-Schaltgeräten gibt es bereits interessante Anwendungsbeispiele – z. B. die Stellungsüberwachung von Ventilen an einer Gas-Pumpstation. In diesem Bereich der Station befindet sich keine Stromversorgung. Positionsschalter erfassen die Stellung der Ventile, die manuell über Handräder geöffnet und geschlossen werden und geben die Signale an eine Leitwarte weiter.

Ein anderer Einsatzfall ist die Waggon-Entladung in einem Chemieunternehmen. Hier fährt ein Trolley unter den Waggon, der entladen werden soll, hakt sich dort ein und zieht den Waggon per

Seil in die gewünschte Position. Die Abfrage, ob der Waggon tatsächlich eingehakt ist, erfolgt über einen »Wireless Ex«-Positionsschalter. Diese Schalter kommen u. a. auch in einer Raffinerie zum Einsatz – dort fragen sie die Position von Verladearmen bei der Tankwagenbeladung ab.

Das Wireless-Programm von steute

Für die drei wesentlichen Anwendungsbereiche der Schaltgeräte von steute – Automation, Explosionsschutz und Medizintechnik – steht somit ein umfassendes Portfolio an Funk-Schaltgeräten zur Verfügung. In den Bereichen Automation und Medizintechnik kann der Anwender in Abhängigkeit von den Umgebungs- und Einsatzbedingungen sogar zwischen mehreren Funk-Standards auswählen.

Um diese Vielfalt wirtschaftlich darstellen zu können, nutzt steute ein modular aufgebautes System von Schaltgeräten und Funklösungen. Vielfach werden die Funkstandards auch um kundenspezifische Applikationen erweitert.



Befehlsgerät in Wireless-Ex-Technologie

// Ausblick

013



Energy Harvesting nutzt die Energie aus der Umgebung

Ausblick:

Wachsende Märkte für Funk-Schaltgeräte

Nach Einschätzung von steute werden sich Funk-Lösungen sowohl in der Industrie als auch in der Medizintechnik weiter durchsetzen. Ein wesentlicher Grund dafür ist die höhere Flexibilität von Geräten, die ohne Kabel auskommen.

Die Funktechnologien werden sich hier ähnlich entwickeln wie im Konsumgütermarkt, wo TV-Fernbedienungen, Mobiltelefonie, Wireless-LAN und Keyless Go inzwischen zum Alltag gehören. Dass die altbekannten Funktechniken wie Fernsehen und Radio den umgekehrten Weg gehen und inzwischen häufig kabelgebunden übertragen werden, steht dazu nicht im Widerspruch. Darüber hinaus wird die Funktechnik auch von der Weiterentwicklung der Batterietechnik profitieren, in die zurzeit sehr viel investiert wird: Auf diese Weise werden längere Standzeiten von kabellosen Geräten möglich sein.

Auch das »Energy Harvesting« steht nach Einschätzung von steute erst am Anfang seiner Entwicklung. Die bereits etablierten Verfahren, mit denen man Energie aus der Umgebung generiert wie z. B. Sonne und Bewegung (Stichwort elektrodynamischer Energiegenerator), werden sich weiter durchsetzen. Die Forschung und Entwicklung an Hochschulen und in Unternehmen arbeitet auch an anderen Verfahren, um auf externe Energieversorgung und auf Batterien zu verzichten. Hier stehen zum Beispiel Temperaturunterschiede und Vibrationen im Fokus. Ein praktisches Beispiel für die (nahe) Zukunft könnten Mobiltelefone sein, deren Energiespeicher sich durch die (Geh-)Bewegung des Menschen auflädt.

Kurz gesagt: Es spricht vieles dafür, dass die Funktechnologien in Industrie und Medizintechnik erst am Anfang stehen und noch viel Potenzial bieten. steute wird daran mitwirken, diese Potenziale auszuschöpfen – mit dem Ziel, die Bedienung von Maschinen und Anlagen zu optimieren, ihre Konstruktion zu vereinfachen, die Kosten für Installation und Montage zu senken und eine größere Flexibilität sowohl in der industriellen Produktion als auch bei der apparativen Behandlung von Krankheiten zu erreichen. Hier kann und wird die bewährte Funktechnik auch in Zukunft wichtige Beiträge leisten.

Die dadurch frei werdenden Frequenzen könnten zukünftig z.B. für die rapide wachsenden Funktechnologien im Konsumgütermarkt sowie in der industriellen Anwendungen wieder belegt werden, da sich auf den ISM-Frequenzen ohnehin schon jetzt ein hoher Konkurrenzdruck abzeichnet.

ANS

RING

BUSY

ATND

HOLD

1

2

3

4

MJ

MN

1

ABC
2

// Anhang

Begriff/Erklärung/Seite

	Ad-hoc-Netzwerke	70
	Angriffsstrategien	163
	Antennengewinn	171
	Bitfehlerrate	84
	Bluetooth-Profil	124
	Dämpfung	64
	Digitale Modulationsverfahren	75
	Direktsequenz-Spreizverfahren	63, 141
	Duty-Cycle (Tastgrad)	90, 143
	Energy Harvesting	99, 194
	EnOcean	99, 194
	Fehlersicherungsverfahren	80
	Frequency Hopping	63, 140
	Funkbrücke	150
	Hidden-Station-Problem	130
	Isotropstrahler (Kugelstrahler)	175
	Koaxialkabel	178
	Kanalgewinn	82
	Linkbudget	82
	Maschinenrichtlinie	152
	Medizintechnik	182
	Peer-to-Peer-Netzwerke	70
	Polarisation	170
	Pulsformung	76
	Rauschen	42
	Störschutzverfahren	63
	Strahlungsdichte	40
	»Wireless Ex«	202
	Wireless Safety	158
ARQ	Automated Request/Gebräuchliches Fehlersicherungsverfahren	80
ASK	Amplitude Shift Keying/Digitales Modulationsverfahren	75
BER	Bit Error Rate/Bitfehlerrate	84
BPSK	Binary Phase Shift Keying/Digitales Modulationsverfahren	137
CDMA	Code Division Multiple Access/Multiplexverfahren zur Mehrfachnutzung von Frequenzen	57
CIA	Confidentiality-Integrity-Authenticity	161
CSMA/CA	Zugriffsart im WLAN	129
CTS	Clear to send-Signal	130
DAA	Detect and Avoid/Zugangsregelung für die Frequenznutzung	56
DFWMAC-DCF	Distributed Foundation Wireless MAC	129

DIFS	Distributed Coordination Function Interframe Space/ Zugriffsart im WLAN 130
DMT	Discrete Multitone Transmission/Digitales Modulationsverfahren 75
DSSS	Direct Sequence Spread Spectrum/Direktsequenzspreizverfahren 63
EDGE	Enhanced Data Rates for GSM Evolution/Mehrstufiges digitales Modulationsverfahren 75
EIRP	Effective Isotropic Radiated Power 42
ETSI	Europäisches Institut für Telekommunikationsnormen 54
FDMA	Frequency Division Multiple Access/Multiplexverfahren zur Mehrfachnutzung von Frequenzen 57
FEC	Forward Error Correction/Fehlersicherungsverfahren 80
FFD	Full Function Device 106
FHSS	Frequency Hopping Spread Spectrum/Frequenzsprungverfahren (Störschutzverfahren) 63
FreqBZP	Frequenzbereichszuweisungsplan 50, 51
FreqNP	Frequenznutzungsplan 51, 54
FSK	Frequency Shift Keying/Digitales Modulationsverfahren 75
HART	Highway Addressable Remote Transducer 108
IEEE	Institute of Electrical and Electronics Engineers 126ff
ISM	Industrial Scientific Medical/ Lizenzfreie Frequenzbereiche für Geräte mit geringer Sendeleistung 52
ITU	Internationale Fernmeldeunion 50
LBT	Listen Before Talking/Zugangsregelung für die Frequenznutzung 56
LOS	Line of Sight/Sichtverbindung zwischen Sender und Empfänger 64
MANET	Mobile Ad Hoc Networking/Ad-Hoc-Netzwerke 70
MIMO	Multiple Input Multiple Output 137
MTU	Maximum Transmission Unit 114
NLOS	No Line of Sight/Kommunikation ohne Sichtverbindung zwischen Sender und Empfänger 64
OFDM	Orthogonal Frequency Division Multiplex/Störschutzverfahren 64, 137
PCM	Puls Code Modulation 78
PSK	Phase Shift Keying/Digitales Modulationsverfahren 75
QAM	Quadrature Amplitude Modulation/Digitales Modulationsverfahren 75, 137
QPSK	Quadrature Phase Shift Keying/Mehrstufiges digitales Modulationsverfahren 75, 137
RFD	Reduced Function Device 106
RTS	Ready to send-Signal 130
SAR	Synthetic Aperture Radar 64
SRD	Short Range Devices/Funk-Geräte für das ISM-Band 52, 98
TDMA	Time Division Multiple Access/Multiplexverfahren zur Mehrfachnutzung von Frequenzen 57
WECA	Wireless Ethernet Compatibility Alliance 132
WPA	WiFi Protected Access 167

Seite/Bildquelle

- 25 »Heinrich Hertz«, Quelle: Wikipedia.de
- 25 »Versuchsanordnung zum experimentellen Nachweis elektromagnetischer Wellen« Quelle: Die Entwicklung der Rundfunktechnik. Vom Postlerkonzert 1920 zum digitalen Rundfunk 1993 von Siegfried Hermann (Autor), Wolf Kahle (Autor), Joachim Kniestedt (Autor), R. v. Decker Verlag, Heidelberg
- 27 »Die erste Richtfunkstrecke: Versuchsaufbau von Heinrich Hertz« Quelle: Die deutschen Funknachrichtenanlagen bis 1940 von Fritz Trenkle, Hüthig Verlag, Copyright: Telefunken Systemtechnik GmbH
- 28 »Steckbarer Kristalldetektor mit Pyritkristall und Spitze« Quelle: Wikipedia.de, von PeterFrankfurt, Creative Commons
- 32 »Löschfunktensender von Telefunken« Quelle: Stiftung Deutsches Technikmuseum Berlin, Historisches Archiv
- 33 »Ansicht einer Löschfunkenstrecke mit Teslatransformator«, Quelle: Wikipedia.de
- 34 »Ansicht eines Lichtbogensenders nach Poulsen«, Quelle: Wikipedia.de von Clemens PFEIFFER, Creative Commons
- 35 »Maschinensender nach Alexanderson, links Generator, rechts davon der Vervielfacher«, Quelle: Wikipedia von Gunther Tschuch, Creative Commons
- 36 »Verschiedene Empfangs- und Leistungsröhren« Quelle: Wikipedia von Stefan Riepl (Quark 48), Creative Commons
- 37 »Röhrentyp RE 144 von Telefunken (20er Jahre)« Quelle: Wikipedia.de von Hihiman, Creative Commons



Jörg F. Wollert



Wolfram Gebhardt

Jörg F. Wollert ist Professor an der Hochschule Bochum für Softwaretechnik und Rechnernetze. Nach seinem Studium der Elektrotechnik mit Schwerpunkt Nachrichtentechnik an der RWTH Aachen promovierte er an der Fakultät Maschinenbau über verteilte objektorientierte Systeme in der Automatisierungstechnik. Industrienerfahrung sammelte er als Projektleiter für komplexe Automatisierungssysteme bei einem marktführenden Unternehmen der Logistikbranche. 1999 wurde er an die Hochschule Bochum berufen. Seit 2000 beschäftigt er sich mit verteilten Echtzeitsystemen. Der Schwerpunkt liegt auf Ethernet basierten Feldbussen und kabellosen Systemen. Mit einer Arbeitsgruppe von knapp 10 Personen bearbeitet er in unterschiedlichen F&E-Projekten Systemlösungen im Bereich kabelloser Netzwerke und Konvergenz von kabellosen und kabelgebundenen Echtzeitsystemen.

Wolfram Gebhardt hat seine Vorliebe für Funk bereits am naturwissenschaftlichen Gymnasium entdeckt. Er studierte Luft- und Raumfahrt bei der Luftwaffe mit Schwerpunkt Nachrichtentechnik. Bereits in seiner ersten Truppenverwendung initiierte er die Entwicklung von günstigeren Antennen für den Flugfunk. In einer NATO Kommandobehörde war er für den Aufbau von Richtfunk- und Kurzwellenfunknetzen verantwortlich. Als Dezernent für Funksysteme der Luftwaffe ordnete er die Funknetze und Frequenzuteilungen der Lw und war für alle Aspekte der Funkkoordination zuständig.

Als Leiter der Studiengruppe Kommunikationssysteme der Lw im BMVg war er mit Zukunftstechnologie befasst und begleitete Forschung und Entwicklung neuer Systeme, deren zivile Ausprägungen heute u.a. im Mobilfunk sowie als Bluetooth und als WLAN allgemeine Anwendung finden.

Impressum

Herausgegeben von der
steute Schaltgeräte GmbH & Co. KG, Löhne, Geschäftsbereich Wireless

Für das Verfassen der Kapitel 10, 11 und 12 sowie für die Koordinations- und Redaktionsarbeiten ist das steute-Redaktionsteam verantwortlich:
Andreas Hofmann, Entwicklung; Andreas Schenk, Produktmanagement
Dipl.-Ing. Marc Schmidt, Entwicklung; Dipl.-Ing. Georg Töpler, Leiter Marketing
Dipl.-Ing. Ralf Twellmann, Technischer Leiter

Externe Redaktion: Gerald Scheffels, Wuppertal

Konzeption und Gestaltung: Stephan Degens, Büro Longjaloux GmbH, Wuppertal
Umsetzung der Grafiken: Mark Muchowski, Büro Longjaloux GmbH, Wuppertal

Gesamtherstellung: Westfalia-Druckerei, Löhne

1. Auflage, November 2010, 1000 wd

ISBN 978-3-00-032905-0

steute

Schaltgeräte GmbH & Co. KG

Brückenstraße 91

32584 Löhne, Germany

Telefon + 49 (0) 57 31 7 45-0

Telefax + 49 (0) 57 31 7 45-200

E-mail info@steute.com

www.steute.com