White Paper

Trusted Wireless 2.0 – Grundlagen und praktische Anwendung

Autor:
Dipl.-Ing. Frank Hakemeyer
fhakemeyer@phoenixcontact.com

ION03-17.000.PR5

Inhaltsverzeichnis

Überblick

Der Einsatz von Funktechnologien zur industriellen Automatisierung erfreut sich zunehmender Beliebtheit. Das liegt zum einen daran, dass die drahtlose Vernetzung entfernter Anlagenteile oder mobiler Gewerke immer wichtiger wird. Zum anderen haben industrielle Funktechnologien ihre Vorteile und ihre Zuverlässigkeit in den vergangenen Jahren deutlich bewiesen und bestehende Vorurteile entkräftet.

Das vorliegende Dokument beschäftigt sich speziell mit der industriellen Funktechnologie Trusted Wireless 2.0 und ihrem Einsatz in der Automatisierung. Der Fokus liegt dabei auf der Beschreibung der technologischen Eigenschaften, die für industrielle Einsatzzwecke von besonderem Interesse sind. Dabei werden die Zusammenhänge zwischen Technologie und praktischer Anwendung erläutert und Abgrenzungen zu anderen Funktechnologien vorgenommen.

Dieses White Paper richtet sich in erster Linie an industrielle Anwender im Bereich der Fabrik- und Anlagenautomatisierung sowie der Infrastruktur. Darüber hinaus werden alle Leser mit einem Interesse an den technischen Zusammenhängen industrieller Datenübertragung per Funk angesprochen.

Einsatz von Funktechnologien in der Automatisierungstechnik

Der Einsatz von Funktechnologien in der Automatisierungstechnik wächst von Jahr zu Jahr. Dabei profitieren Anwender von der Mobilität, die durch eine Funklösung erreicht wird, aber auch von der Flexibilität. Häufig ist auch die Kostenersparnis durch den Wegfall der Kabelinstallation der Grund für die Verwendung eines Funksystems.

Die Automatisierungsindustrie setzt dabei überwiegend auf Funktechnologien, die nahezu weltweit verwendbar sind und in lizenzfreien Frequenzbereichen arbeiten. Aufgrund der nationalen Frequenzregulierung gibt es nur wenige Frequenzbänder, die dies erfüllen. Die sogenannten ISM- (Industrial-Scientific-Medical-) Bänder sind zwar lizenzfrei nutzbar, aber lediglich das 2,4-GHz-Band ist nahezu weltweit verbreitet. Daher nutzen die meisten Funktechnologien in der Automatisierungstechnik dieses Band.

Aufgrund der großen Bandbreite von 83 MHz ist ein hoher Datendurchsatz und/oder der Parrallelbetrieb einer Vielzahl von Funksystemen im 2,4 GHz-ISM-Band möglich. Die Bandbreite der niederfrequenten Bänder ist deutlich geringer und liegt zwischen ein paar hundert kHz und 26 MHz. Allerdings sind die Ausbreitungs- und die Eigenschaften der Materialdurchdringung dieser ISM-Bändern deutlich besser (vgl. Abb.1), wodurch höhere Reichweiten und Funkstrecken ohne Sichtverbindung möglich werden.

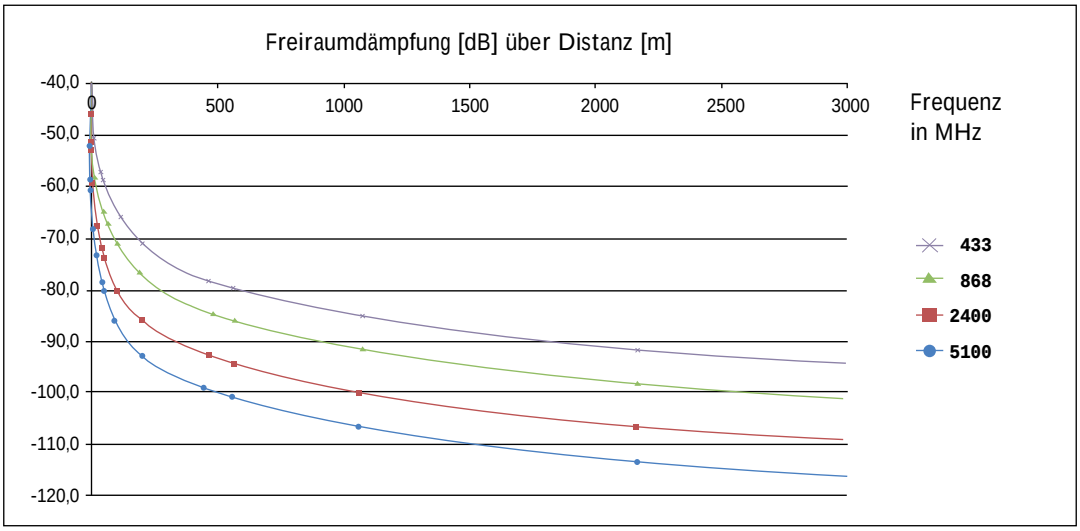


Abbildung 1

Die Freiraumdämpfung nimmt mit steigender Frequenz zu

Daher ist Trusted Wireless 2.0 für die ISM-Bänder 868 MHz (Europa), 900 MHz (Amerika und Australien) und 2,4 GHz (Weltweit) verfügbar. So können auch Anforderungen von Reichweiten über 5 km und ungünstigen Umgebungsbedingungen erfüllt werden. Dabei ist immer entscheidend, die jeweiligen Vorteile aus dem gewählten Funksystem richtig einzusetzen.

Im Folgenden wird sich die Beschreibung der Funktechnologie Trusted Wireless 2.0 häufig an bekannten Funktechnologien aus der Consumer- und IT-Welt orientieren. Da mittlerweile die Bluetooth- und WLAN-Technik ebenfalls im industriellen Umfeld zum Einsatz kommt, sollen in diesem Whitepaper insbesondere die Unterschiede zu diesen Technologien dargestellt werden. Außerdem gibt es bereits eine speziell für die Prozesstechnik entwickelte Funktechnologie WirelessHART, die ebenfalls zum Vergleich genutzt wird.

Da sich Funktechnologien im Sub-GHz-Bereich nicht mit Funktechnologien im 2,4 GHz Bereich vergleichen lassen, werden hier bekannte Low Power WAN Systeme, aus dem Sub-GHz Bereich, zum Vergleich herangezogen.

Anwendungsbereiche von Trusted Wireless 2.0

Trusted Wireless 2.0 ist eine speziell für den industriellen Einsatz entwickelte Funktechnologie, die sich insbesondere bei fehlender Kabelinfrastruktur für Sensor-Aktor-Informationen eignet. Sie wird zur Übertragung geringer bis mittlerer Datenmengen, auch über größere Distanzen von einigen hundert Metern bis zu mehreren Kilometern genutzt.

Die wesentlichen Merkmale von Trusted Wireless 2.0 sind

- Robuste Kommunikation durch FHSS
- Automatische und manuelle Koexistenzmechanismen
- Sichere Kommunikation durch Verschlüsselung (AES 128 Bit) und Integritätsprüfung
- Hohe Reichweite durch hohe Empfängerempfindlichkeit und variable Datenübertragungsraten
- Flexible Netzwerke mit automatischem Verbindungsmanagement
- Dezentrale Netzwerkpflege beschleunigt und erleichtert
- Umfangreiche Diagnoseeigenschaften
- Anpassbarkeit auf die jeweilige Anwendung.

Diese werden nachfolgend genauer erläutert.

Robuste Kommunikation durch FHSS

Jeder Anwender möchte für seine Applikation eine „zuverlässige“ und „robuste“ Kommunikationsverbindung, wobei dies allerdings eher subjektive Kriterien sind. Objektiv werden die Anforderungen durch echte Kenngrößen wie zum Beispiel Verfügbarkeit, Latenz, Determinismus und Datendurchsatz benannt, die je nach Anwendung für den Anwender eine wichtige Rolle spielen.

Es ist aber sehr wichtig, die wirklichen Anforderungen der Anwendung zu kennen und auch einordnen zu können. Die verfügbaren Funktechnologien haben unterschiedliche Schwerpunkte und Leistungsfähigkeiten und müssen anhand der Anforderungen der Applikation ausgewählt werden.

Außerdem ist es wichtig zu wissen, welche Faktoren „die Zuverlässigkeit“ einer Funkstrecke beeinträchtigen und wie die verschiedenen Funktechnologien damit umzugehen versuchen.

Es gibt zwei wesentliche Einflussfaktoren auf eine Funkverbindung. Zum einen die Störung des Funksignals durch andere elektromagnetische Wellen, ausgelöst durch andere Funksysteme oder ungewollte Emissionen anderer Elektro- und Elektronikgeräte (EMV-Störungen). Zum anderen die Störung des Funksignals durch das sogenannte Fading (schwinden, nachlassen), welches durch die Freiraumdämpfung und insbesondere durch Reflexionen verursacht wird.

Störung des Funksignals durch andere Funksysteme oder elektromagnetische Einflüsse

Im 2,4-GHz-Band profitieren Funksysteme von der Tatsache, dass EMV-Störungen durch allgemeine, industrielle Anwendungen nicht bis in diesen hohen Frequenzbereich hineinragen. Die sonst so problematischen Frequenzumrichter, Vorschaltgeräte und andere EMV-Störungen erzeugende Einrichtungen spielen im oberen MHz- und GHz-Bereich keine Rolle mehr. Ihre energiereichen Aussendungen liegen vielmehr im Kilo- und Megahertz-Bereich.

Die Störungen, mit denen sich die Funksysteme auseinandersetzen müssen, sind andere Funksysteme. Hierzu stehen zwei grundsätzlich verschiedene Ansätze zur Verfügung, nämlich, das sogenannte Direktspreizverfahren (Direct Sequence Spread Spectrum, DSSS) und das Frequenzspreizverfahren (Frequency Hopping Spread Spectrum, FHSS).

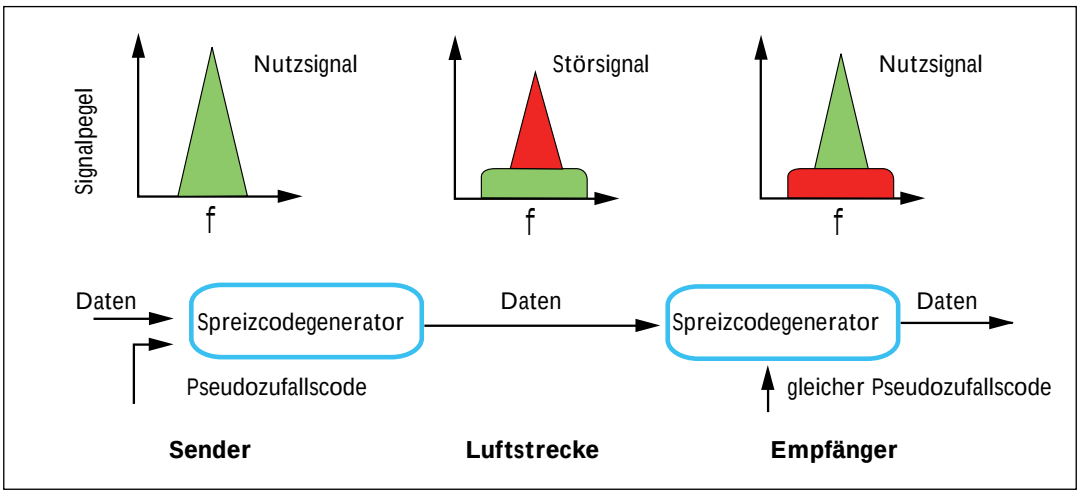


Abbildung 2a
Schematische Darstellung des DSS-Verfahrens

Beim DSSS durchläuft das zu übertragende Nutzsignal einen Spreizcodegenerator, der aus einem schmalbandigen Signal mit hoher Amplitude, ein breitbandiges Signal mit niedriger Amplitude macht (s. Abb. 2a). Das einfallende, schmalbandige Störsignal mit hoher Amplitude durchläuft mit dem Nutzsignal den gleichen Spreizcodegenerator im Empfänger. Dabei wird aus dem breitbandigen Nutzsignal mit geringer Amplitude, wieder ein schmalbandiges Signal mit hoher Amplitude und gleichzeitig wird das Störsignal in ein breitbandiges Rauschen gewandelt. Vorteil dieses Verfahrens ist die mögliche Übertragung mit einer sehr hohen Datenrate. Der Nachteil ist die feste Übertragungsfrequenz, sowie die Tatsache, dass dieses Verfahren nur bis zu einem gewissen Störsignalpegel funktioniert. Ist dieser Pegel überschritten, kann im Empfänger nicht mehr zwischen Nutz- und Störsignal unterschieden werden.

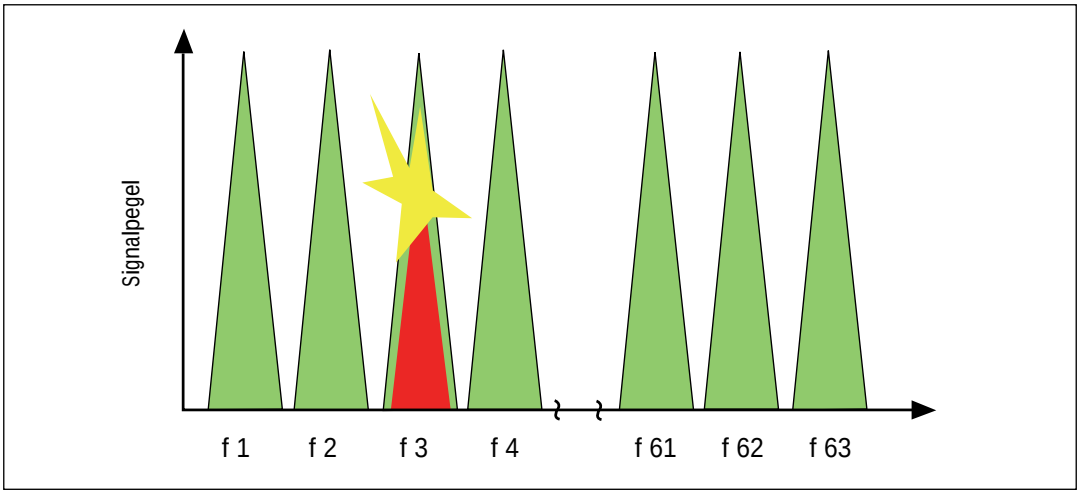


Abbildung 2b

Schematische Darstellung des FHSS-Verfahrens

Beim FHSS werden zur Übertragung des Nutzsignals viele verschiedene Einzelfrequenzen in einem pseudo-zufälligen Muster durchsprungen. Ein auftretendes Störsignal blockiert – egal wie hoch der Pegel ist – somit nur eine oder wenige benachbarte Einzelfrequenzen. Auf den übrigen Frequenzen kann die Übertragung ungehindert stattfinden.

Bei zunehmenden Störungen sinkt bei einem FHSS-System lediglich der Datendurchsatz, während bei einem DSSS-System die Übertragung komplett blockiert werden kann.

Trusted Wireless 2.0 verwendet im 2,4 GHz Band eine Frequenzsprungtechnologie (FHSS) mit bis zu 440 möglichen Einzelfrequenzen, wobei die Geräte hieraus eine Auswahl von maximal 127 Kanälen verwenden. In den Systemen im 868-MHz- und 900-MHz-Frequenzband wird das Verfahren ebenfalls eingesetzt. Aufgrund der geringeren Bandbreiten in den Frequenzbändern ist die Anzahl der verfügbaren Kanäle entsprechend geringer. Die tatsächliche Anzahl genutzter Frequenzen innerhalb des pseudo-zufälligen Sprungmusters hängen von weiteren Einstellungen und Mechanismen ab, wie zum Beispiel dem Aussparen bestimmter Frequenzbereiche (sog. black-listing) für das Koexistenzmanagement oder der Verwendung mehrerer Frequenzgruppen (sog. RF-Bänder) zur Optimierung des Parallelbetriebes.

Störung des Funksignals durch Fading

Beim sogenannten Fading wird das Signal durch verschiedene externe Einflüsse abgeschwächt. Haupteinflussfaktor sind bei der Ausbreitung der Funkwelle auftretende Reflexionen. Durch diese Reflexionen gelangt das Signal auf vielen verschiedenen Wegen vom Sender zum Empfänger (sog. Multipath-Fading). Dabei legen die Signale – abhängig vom Reflexionsweg – unterschiedliche Strecken zurück und benötigen für diese Distanzen eine unterschiedlich lange Zeit. Das hat zur Folge, dass das Signal den Empfänger in einer unterschiedlichen Phasenlage erreicht. Zu jedem Zeitpunkt überlagern sich also viele Einzelsignale in unterschiedlicher Phasenlage.

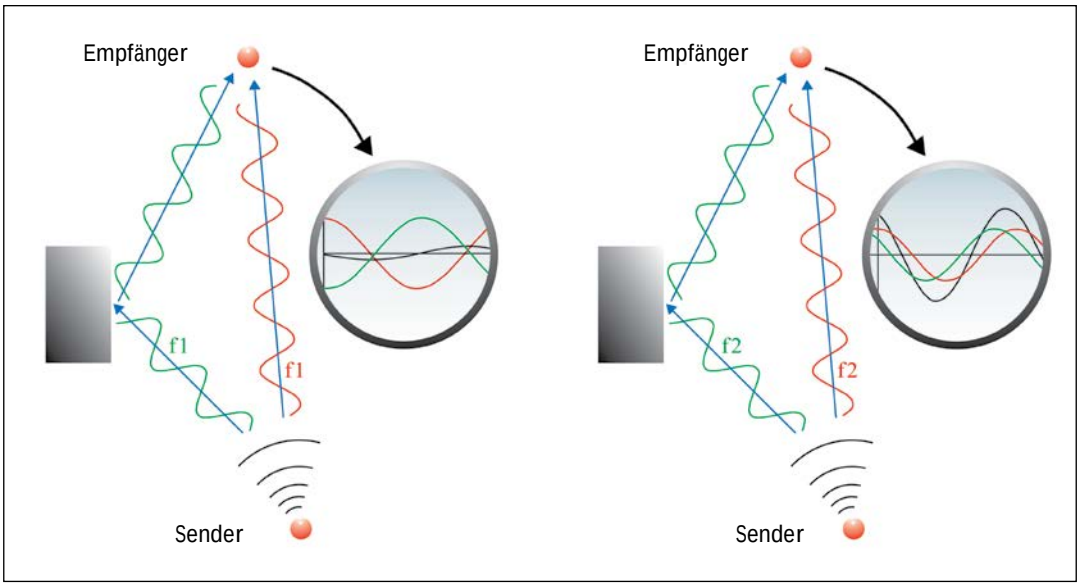


Abbildung 3

Schwächung des Signals auf f1 und Verstärkung des Signals auf f2

Dabei kann es zur Schwächung (destructive interference), oder zur Verstärkung (constructive interference) des Signals kommen (Abb. 3), je nachdem, wie die Konstellation der Phasenlagen am Ort des Empfängers ausfällt.

Wichtig: Verändert sich die Sendefrequenz – und damit die Wellenlänge – bei konstanten Umgebungsbedingungen (Reflexionssituation), so verändern sich die Reflektionssignale und damit die Situation der überlagerten Signale am Empfänger. Ein Funksystem kann also zum Beispiel auf einer Frequenz f1 eine besonders ungünstige Konstellation erfahren und dadurch ein extrem schwaches oder nicht mehr ausreichendes Signal am Empfänger empfangen. Jedoch kann auf einer anderen Frequenz bei gleichen Umgebungsbedingungen sogar eine Verstärkung des Signals erfolgen. Dies ist ein extremer Vorteil eines Frequenzsprungsystems (FHSS), welches ständig die Übertragungsfrequenz wechselt und somit automatisch diese physikalisch bedingte Problemstellung vermeidet.

Die Funktechnologie Trusted Wireless 2.0 benutzt viele einzelne Sendefrequenzen innerhalb des jeweiligen Frequenzbandes (siehe FHSS). Die Abstände zwischen den jeweiligen Frequenzbändern sind so gewählt, dass die Wellenlängenänderung groß genug ist, um einen signifikanten Signalgewinn zu erzielen. So kann eine zuverlässige Übertragung gewährleistet werden, die durch das Signal-Fading kaum merklich beeinflusst wird.

Mit anderen Worten: Ist auf einer Frequenz – bedingt durch das Multipath-Fading keine Übertragung möglich, so ist auf der direkt folgenden Frequenz das Signal so stark, dass es problemlos empfangen werden kann.

Automatische und manuelle Koexistenzmechanismen

Durch die zunehmende Nutzung der ISM-Bänder werden die Koexistenzmechanismen eines Funksystems immer wichtiger für den langfristigen störungsfreien Einsatz.

Als ein möglicher Mechanismus ist hier zum Beispiel das so genannte listen-before-talk (kurz LBT) zu nennen. Beim LBT wird zunächst das einfallende Empfängersignal auf seine Stärke hin gemessen – man ermittelt das so genannte RSSI-Signal (Receive-Signal-Strength-Indicator). Diese Größe liefert – unabhängig von der verwendeten Funktechnologie – ein Maß dafür, ob sich ein anderes Funksystem bereits auf dem Medium befindet. Abhängig von der Stärke des RSSI-Signals kann dann entschieden werden, ob eine Nutzung des Mediums möglich ist.

Dieses Verfahren hat allerdings den Nachteil, dass im Vergleich zu einem festgesetzten Duty Cycle (siehe unten) eine höhere Latenzzeit auftritt. Insbesondere, wenn das 2,4-GHz-Band im Industrieumfeld oder an öffentlichen Plätzen genutzt wird, da hier, zusätzlich zu den installierten WLAN- und Bluetooth-Systemen, alle Privatgeräte ein zu berücksichtigendes Funksystem darstellen können.

Im ungünstigsten Fall kann LBT dazu führen, dass zugunsten anderer Funksysteme oder gar Störern der Funkbetrieb eingestellt wird. Daher nutzt Trusted Wireless 2.0 in allen Frequenzbereichen die in den ISM-Regularien festgeschriebenen Duty-Cycle-Mechanismen.

Je nach ISM Band gibt es verschiedene vorgeschriebene Koexistenzmechanismen, die den Medienzugang legislativ regeln. Dazu zählt zum Beispiel der vorgeschriebene Duty Cycle im 868-MHz-Bereich. Hier wird durch den Gesetzgeber vorgeschrieben, dass ein Funksystem entweder LBT (siehe oben) durchführen muss oder nur 10% der Zeit senden darf. Durch diesen Mechanismus wird ermöglicht, dass ein Funksystem nicht den gesamten Frequenzbereich blockiert und dadurch schwächere Sender, wie z. B. Garagentoröffner oder Babyphones, aussperrt.

Auch ein Frequenzsprungverfahren ist ein wirkungsvoller Koexistenzmechanismus, der es ermöglicht eine Vielzahl von Systemen im gleichen Frequenzbereich zu betreiben. Dadurch, dass die Systeme ständig und pseudo-zufällig ihre Frequenz ändern, entstehen Kollisionen nur gelegentlich und halten nur für einen Kommunikationszyklus an.

Allerdings können Störungen durch koexistierende Systeme mit den genannten Mechanismen nicht ausgeschlossen sondern nur unwahrscheinlicher gemacht werden.

Daher ist es in vielen Automatisierungsanwendungen heute schon gängige Praxis, die eingesetzten Funksysteme in der Anlage zu planen. D.h. es werden für die verschiedenen Anwendungen natürlich unterschiedliche Funkprodukte und damit auch Funktechnologien eingesetzt. Um diesen Produkten einen bestmöglichen Zugang zum Medium zu geben und eine möglichst geringe gegenseitige Beeinflussung zu haben, sollte man das eingesetzte Spektrum entsprechend planen. Besonders trifft dies auf das 2,4-GHz-Band zu, da dort die meisten kommerziellen Funksysteme arbeiten.

Ein WLAN-Kanal nach IEEE 802.11b nutzt zum Beispiel 20 MHz Bandbreite. Werden in einer Anlage mehrere WLAN-Systeme benötigt, so sollten sie unterschiedliche WLAN-Kanäle benutzen. Da die WLAN-Kanäle überlappend angeordnet sind, sollten bei direkter Nachbarschaft der Systeme Kanäle ausgesucht werden, die sich nicht überlappen, zum Beispiel Kanal 1, 6 und 13. Wird dann zusätzlich noch ein Bluetooth oder Trusted-Wireless-System verwendet, so sollten diese Frequenzbereiche der der WLAN-Systeme ausgeblendet (sog. black-listing) werden. In Abb. 4 sieht man das Spektrum des aktiven Frequency Hopping Systems (zum Beispiel Bluetooth) und den drei frei gehaltenen WLAN Kanälen.

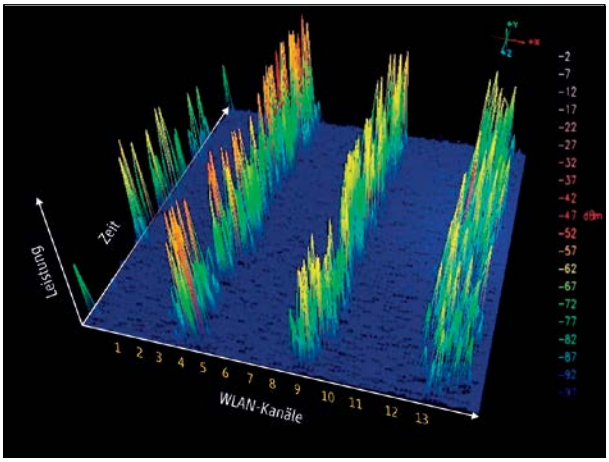


Abbildung 4
Spektrum des aktiven Frequenzsprung-Systems und den drei frei gehaltenen WLAN Kanälen

Es ist also zunehmend wichtig, die Frequenzbandnutzung der verschiedenen Systeme zu planen, und die Technologie muss das black-listing von Frequenzbereichen zulassen. Trusted Wireless 2.0 ist in der Lage, Frequenzbereiche auszusparen (black-listing) und somit die Koexistenz zu anderen Systemen planbar zu machen. Dabei werden die Sprungfrequenzmuster entsprechend den ausgeschlossenen Bereichen neu berechnet.

Bei der Erzeugung der Sprungfrequenzmuster werden bei Trusted Wireless 2.0 mehrere Aspekte berücksichtigt. Zum einen die o.g. Berücksichtigung der black-listing-Bereiche und außerdem die bereits oben erwähnte Mindestsprungdistanz für eine möglichst große Frequenz- bzw. Wellenlängenänderung zur Kompensation des Multipath-Fadings.

Der dritte Aspekt besteht in der Gruppierung von Frequenzen in so genannte RF-Bänder. Ein RF-Band ist eine Gruppe von Frequenzen, die aus einzelnen Frequenzen des gesamten Frequenzbereichs zusammengestellt ist. Dabei nutzen unterschiedliche RF-Bänder komplett verschiedene Frequenzen. Betreibt man also zwei Trusted Wireless Netzwerke in räumlicher Umgebung mit zwei unterschiedlichen RF-Bändern, so wird es niemals eine Kollision zwischen diesen beiden Netzwerken geben können. Trusted Wireless 2.0 verfügt im 2,4-GHz- und 900-MHz-Band über 8 verschiedene RF-Bänder. Im 868-MHz-Band stehen 2 RF-Bänder zur Verfügung.

Außerdem kann durch den gezielten Einsatz von Trusted Wireless in verschiedenen Frequenzbändern ein bereits ausgelastetes Frequenzband umgangen werden.

Sichere Kommunikation durch Verschlüsselung und Integritätsprüfung

Eine große Bedeutung im Bereich der drahtlosen Übertragungstechnik kommt dem Aspekt der Sicherheit zu. Da der Informationstransport in dem ungeschützten Medium Luft erfolgt, müssen Sicherheitsstrategien den unbefugten Zugri verhindern.

Bei den weit verbreiteten Funktechnologien Bluetooth und Wireless LAN stellt sich zudem das Problem, dass die Kommunikationsschnittstelle für jedermann zugänglich ist, d.h. jedes verfügbare Bluetooth oder WLAN-Funkprodukt lässt prinzipiell eine Verbindung mit dem industriell genutzten Netzwerk zu. Das Gefährdungspotenzial ist insbesondere bei der WLAN-Schnittstelle hoch, da sie im PC-Umfeld extrem verbreitet und für Hacker-Angri e sehr attraktiv ist.

Eine industrielle Funkstrecke mit Trusted Wireless 2.0 ist durch die nicht-o ene Technologie prinzipiell wesentlich besser vor möglichen Angri en geschützt. Außerdem erschwert das Frequenzsprungverfahren ein Ausspionieren des Protokolls erheblich.

Doch Trusted Wireless 2.0 verfügt zusätzlich über zwei echte Sicherheitsmechanismen, eine Verschlüsselung aller übertragenen Informationen nach dem so genannten Advanced Encryption

Standard (AES), sowie eine nach RFC3610 beschriebene Integritätsprüfung der Nutzdaten.

Die Verschlüsselung nach AES sorgt dafür, dass theoretisch mitgehörte Datenpakete nicht „verstanden“ werden können, d.h. der Inhalt kann nicht interpretiert werden. Der 128 Bit lange Schlüssel wird aus einem gegeben Passwort (Pre-Shared-Key) berechnet und muss allen Teilnehmern bekannt sein.

Mindestens genauso wichtig ist die Integritätsprüfung von gesendeten Datenpaketen. Die einfachste Form eines Angri□s auf eine Funkstrecke liegt im Mithören und gegebenenfalls Verändern und Wiedereinspeisen einer Nachricht. Es muss also sichergestellt werden, dass die Quelle der Nachricht, also der Sender, nur ein gültiger, beglaubigter Sender ist. Dazu werden die Nachrichten mit einem fortlaufenden Code versehen, der sich nicht wiederholen darf. Dieser fortlaufende Code ist bei Trusted Wireless 2.0 so gewählt, dass ein Angreifer mehr als 1000 Jahre warten müsste, bevor sich dieser Code wiederholt.

Hohe Reichweite durch hohe Empfängerempfindlichkeit und variable Datenübertragungsraten

In industriellen Funkanwendungen spielt die Reichweite insbesondere in den Outdoor-Anwendungen eine wichtige Rolle. Aber auch dort, wo keine großen Reichweiten zu überbrücken sind, liefert eine gute Empfängerempfindlichkeit eine hohe Systemreserve zur Übertragung bei schlechten Bedingungen, zum Beispiel bei NLOS (non-line-of-sight). Die Empfängerempfindlichkeit hängt im Wesentlichen von der Qualität der verwendeten Schaltkreise und der Übertragungsgeschwindigkeit ab. Trusted Wireless 2.0 verwendet hochwertige Bauteile in den Sende- und Empfangsstufen und erreicht durch zusätzliche Vorverstärkung eine gute Empfindlichkeit.

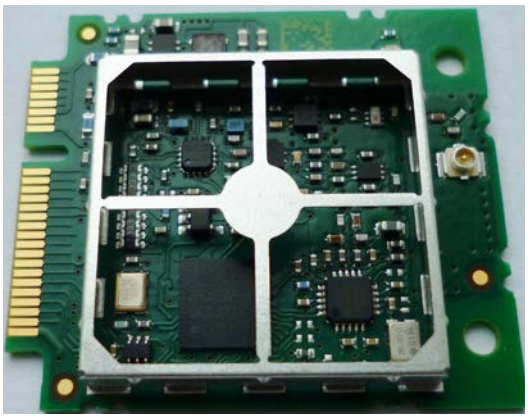


Abbildung 5

Hochwertige Bauteile für besonders gute Empfängerempfindlichkeit

Weitaus größer ist jedoch die zusätzliche Erhöhung der Empfindlichkeit durch variable Datenraten. Wird eine niedrigere Datenrate auf der Luftübertragungsstrecke verwendet, so wird jede einzelne Information (jedes Bit) für eine längere Zeit mit der Sendeleistung P ausgesendet. Die Energie je Bit [EBit = P • tBit] ist also bei einer vierfach höheren Datenrate, um ein Vierfaches niedriger (Abb. 6).

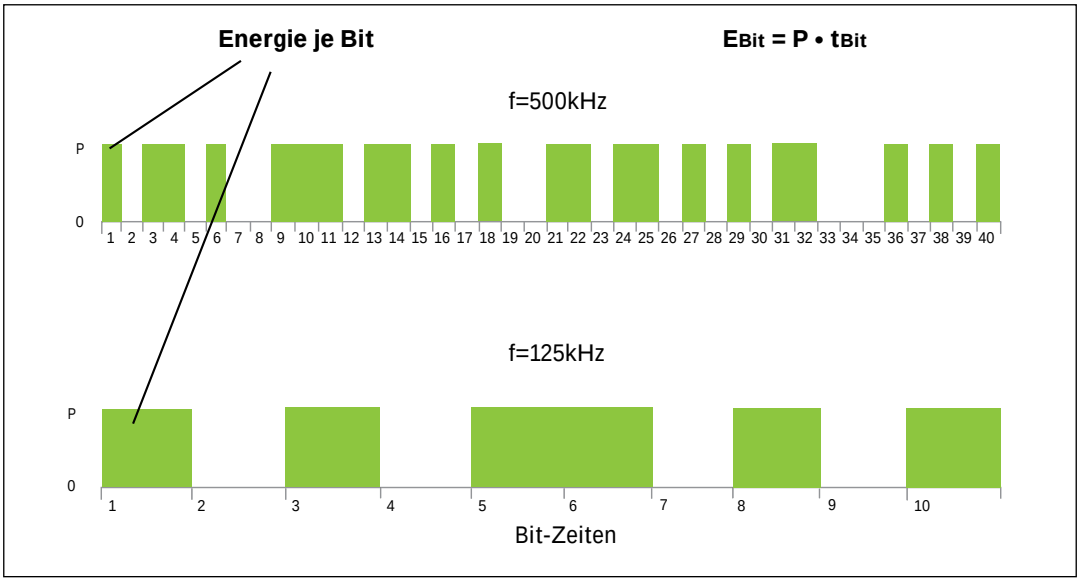


Abbildung 6

Je geringer die Datenrate, desto höher die Energie je Bit

Eine höhere Energie je Bit resultiert in einem höheren Systemgewinn. Ausdruck findet dies in einer höheren Empfängerempfindlichkeit. Eine vierfach niedrigere Datenrate ergibt einen Systemgewinn von etwa 6 dBm. Da sich die Reichweite eines Systems alle 6 dB verdoppelt, ist somit die Reichweite eines 125-kHz-Systems etwa doppelt so groß wie die eines 500-kHz-Systems.

Trusted Wireless 2.0 bietet den Anwendern verschiedene einstellbare Datenraten. Damit kann – abhängig von den Applikationsanforderungen – die Reichweite maximiert werden und übertrifft somit die Reichweiten von gängigen Bluetooth- und WLAN-Systemen um ein Vielfaches.

Folgende Empfängerempfindlichkeiten bietet die Funktechnologie Trusted Wireless 2.0:

OTA Datenrate in kBit/s	Typische Empfänger-empfindlichkeit in dBm	Mögliche, über-windbare Distanz bei LOS und 12 dB Systemreserve	ISM-Band	max. EIRP in dBm
250	-93	1 km	2,4 GHz	20
125	-96	3 km	2,4 GHz	20
16	-106	5 km	2,4 GHz	20
500	-95	8 km	900 MHz	30
250	-102	18 km	900 MHz	30
125	-105	24 km	900 MHz	30
16	-112	32 km	900 MHz	30
120	-103	8 km	868 MHz	27
60	-104	10 km	868 MHz	27
19,2	-111	18 km	868 MHz	27
9,6	-114	20 km	868 MHz	27
1,2	-122	25 km	868 MHz	27

* Die Sendeleistung im 2,4-GHz-Band ist in Europa abhängig von der Datenrate und ist bei Trusted Wireless 2.0 < 19 dBm.

Tabelle 1:

Vergleich der Empfängeremp ndlichkeit und Reichweite in den jeweiligen Systemen.

Um die überwindbare Luftstrecke zu bestimmen muss der Empfängerempfindlichkeit die Sendeleistung hinzugerechnet werden. Um eine echte Berechnung des so genannten Link-Budgets durchzuführen, müssen außerdem die Kabeldämpfungen der Antenneninstallation, sowie ggfs. ein Antennengewinn einberechnet werden. Eine sichere Funkverbindung sollte zudem immer mit einer Systemreserve von ca. 10 – 15 dB betrieben werden.

Für die Funktechnologie Trusted Wireless 2.0 ergeben sich daher realistisch erzielbare Reichweiten im Kilometerbereich – bei Sichtverbindung – abhängig von der jeweils verwendeten Datenrate und der Antenneninstallation.

Flexible Netzwerke mit automatischem Verbindungsmanagement

Funknetzwerke im Industrieumfeld haben – wie oben bereits beschrieben – besondere Anforderungen an die Zuverlässigkeit. Diese kann auch durch die Netzwerkstruktur stark verbessert werden. Bluetooth verwendet nur Punk-zu-Punkt-Verbindungen und ein Master kann davon bis zu sieben Stück gleichzeitig verwalten. Dadurch können an einem Bluetooth-Master bis zu sieben Bluetooth-Slaves arbeiten.

Ein WLAN-Access-Point arbeitet in einer Stern-Struktur mit einer sinnvollen Anzahl von unter 20 Clients. Beide Technologien unterstützen keine Repeater-Funktion. Dadurch sind die Ausdehnungen dieser Netzwerke geringer und es gibt nicht die Möglichkeit alternativer Funkverbindungen. Trusted Wireless 2.0 verfügt über Repeater-Funktionen, und das Netzwerk ist in der Lage, sich bei einem Verbindungsabbruch selbst zu heilen (self-healing network), d.h. einen alternativen Verbindungspfad aufzubauen oder zu finden. Dieses Self-healing geschieht automatisch innerhalb sehr kurzer Zeit (abhängig von der Datenrate im Bereich von Millisekunden bzw. Sekunden).

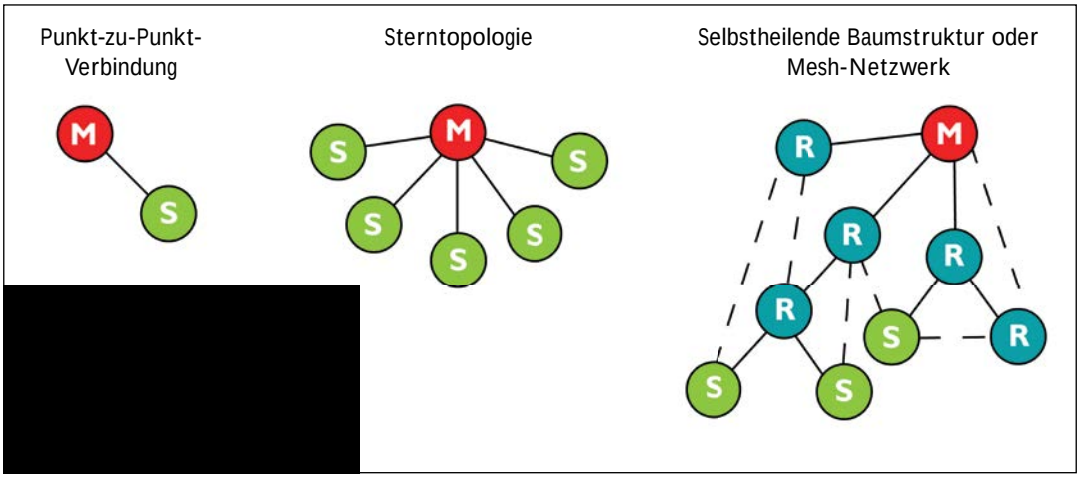


Abbildung 8

Mögliche Netzwerkstrukturen mit Trusted Wireless 2.0

Da aufgrund dieser mehrfachen Kommunikationswege zwischen den Knoten im Netzwerk kleine Maschen entstehen, nennt man diese Art von Funknetzwerk auch Mesh-Network. Damit kann ein Trusted-Wireless-2.0-Funknetzwerk in allen Netzwerkformationen betrieben werden.

In realen Netzwerken kann es aufgrund der hohen Empfängerempfindlichkeit von Trusted Wireless 2.0 vorkommen, dass sich ein Knoten nicht am nächstgelegenen Knoten anbindet, sondern an einem weit entfernten. Daher bietet Trusted Wireless 2.0 die Möglichkeit ein so genanntes parent-black-listing durchzuführen. Hierbei werden gezielt Knoten als mögliche Repeater ausgeschlossen. Jedem Knoten können also andere Knoten als Repeater „verboten“

(parent-black-listing) oder „erlaubt“ (parent-white-listing) werden. In der Grundeinstellung sind alle Repeater als mögliche Knoten erlaubt.

Mit dieser Funktionalität sind Netzwerkoptimierungen durchführbar. Außerdem können so bewusst Netzwerkstrukturen, zum Beispiel eine Kette, aufgebaut werden, wenn dies gewünscht ist. In Abb. 9 könnten Knoten 1, 2 oder 3 gute Verbindungen für Knoten 5 sein. Hingegen sind Knoten 4, 6 und 9 keine guten Repeater und könnten über das parent-black-listing ausgeschlossen werden.

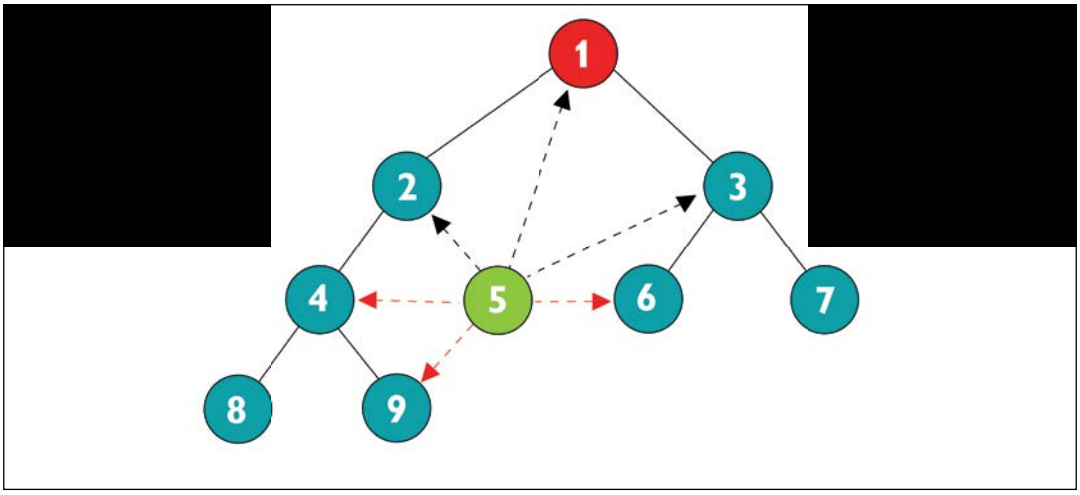


Abbildung 9

Parent-black-listing für Knoten 5 sollte die Knoten 4, 6 und 9 enthalten

Dezentrale Netzwerkpflege beschleunigt und erleichtert

Um ein Funknetzwerk zu betreiben, benötigt es interne Kommunikation zwischen den einzelnen Funkknoten – unabhängig von der zu transportierenden Datenmenge. In diesem Zusammenhang muss zum Beispiel der Prozess zur Aufnahme eines neuen Knotens in das Netzwerk (joining) behandelt werden, oder aber auch die zyklische Pflege bereits eingebundener Knoten.

Funknetzwerke wie Zigbee oder WirelessHART verfolgen dabei einen zentralen Ansatz unter Verwendung einer zentralen Kontrollfunktion, dem sogenannten Manager. Dies führt dazu, dass alle Netzwerkmanagementnachrichten im Manager initiiert werden und durch das Netzwerk bis an den Zielknoten transportiert werden müssen. Auch die Antworten durchlaufen den gesamten Weg. Dieses Prinzip verursacht einen nicht unerheblichen Nachrichtenverkehr im Funknetzwerk.

Trusted Wireless 2.0 hingegen nutzt einen dezentralen Ansatz. Hier wird das gesamte Netzwerkmanagement innerhalb der Parent-Child Zone abgewickelt. D.h. ein Parent kümmert sich um seine Children und bindet auch neue Knoten gegebenenfalls in seine Zone ein. Diese Informationen müssen nicht immer bis zum zentralen Manager hinauf und herunter gegeben werden, was einerseits den Nachrichtenverkehr im Netzwerk reduziert und außerdem den gesamten Vorgang stark beschleunigt.

Dies wirkt sich besonders auf die Netzwerkformierungsgeschwindigkeit aus. Verliert in einem zentral gepflegten Netzwerk der Manager die Versorgungsspannung und damit die Informationen über das Beziehungswissen der Knoten, so dauert eine Neuformierung sehr lange. Bei WirelessHART kann dies – abhängig von der Anzahl der Knoten – etliche Minuten dauern.

Bei Trusted Wireless 2.0 hingegen können diese Vorgänge in den einzelnen Zweigen des Netzwerkbaumes sogar parallel ablaufen (Abb. 10 - P/C-zone 2.1 und 2.2), weil sie innerhalb der Parent-Child-Zone geschehen. Dies beschleunigt eine Neuformation des Funknetzwerkes erheblich.

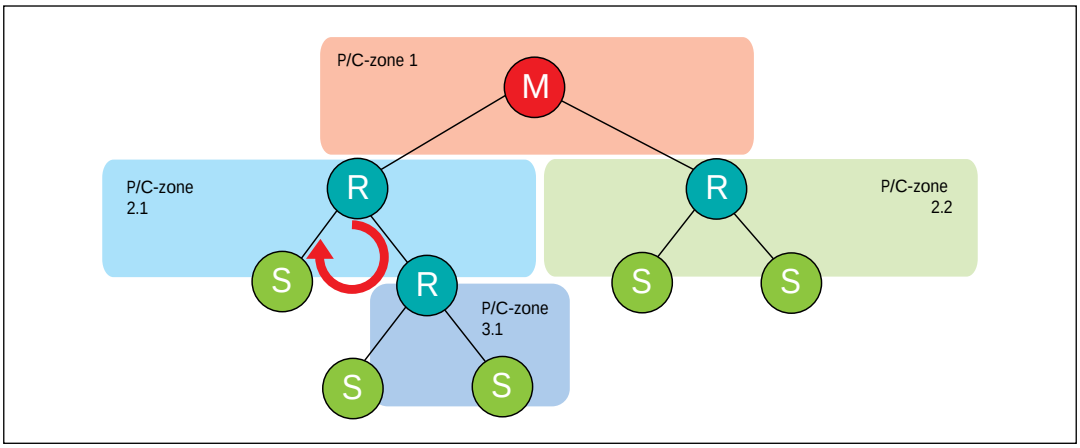


Abbildung 10
Dezentrales Netzwerkmanagment in der Parent-Child-Zone (P/C-zone)

Umfangreiche Diagnoseeigenschaften

Der Betrieb eines industriellen Funknetzwerks unterscheidet sich von Heimanwendungen erheblich. Die Konsequenzen einer Nichtverfügbarkeit bewegen sich auf viel kritischerem Niveau als im privaten Bereich. Daher möchten die Anwender auch viel mehr Informationen über den Zustand ihres Funknetzwerkes erhalten. Das Thema „Diagnose“ wird damit sehr wichtig.

Trusted Wireless 2.0 bietet hier eine sehr große Fülle an Diagnoseinformationen. So sind in jedem Knoten eine so genannte Knotentabelle und eine so genannte Kanaltabelle abgelegt. Die Knotentabelle beinhaltet Informationen über die direkt angeschlossenen Knoten, ihre Eigenschaften (Master, Repeater, Slave), ihre Verbindungsqualität (RSSI-Signal), die jeweilige Netzwerktiefe und die Liste der erlaubten beziehungsweise verbotenen Parents.

In der Kanal-Tabelle werden Informationen über die verwendeten Funkfrequenzen abgelegt, unter anderem der Rauschpegel (aktuell und maximal), die Kanal-Blockierungsrate und die Paketfehlerrate. Alle Diagnoseinformationen lassen sich über das Funknetzwerk fernabfragen und vermitteln dem Betreiber ein exaktes Bild des Netzwerks und seiner Umgebung. Hierdurch lassen sich dann auch gezielte Optimierungsmaßnahmen durchführen.

Anpassbarkeit auf die jeweilige Anwendung

Trusted Wireless 2.0 ist eine speziell für die industrielle Anwendung entwickelte Funktechnologie. Sie orientiert sich an den Bedürfnissen industrieller Infrastrukturanwendungen und schließt die Lücken zwischen speziellen Sensornetzwerken wie zum Beispiel WirelessHART und der Hochgeschwindigkeitstechnik Wireless LAN. Trusted Wireless 2.0 zeichnet sich durch seine besondere Anpassbarkeit auf die jeweilige industrielle Applikation aus und bietet dem Anwender ein hohes Maß an Zuverlässigkeit, Robustheit, Sicherheit und Flexibilität. Das folgende Bild zeigt eine vergleichende Einstufung von Trusted Wireless 2.0 und anderen Funktechnologien im 2,4-GHz-Band.

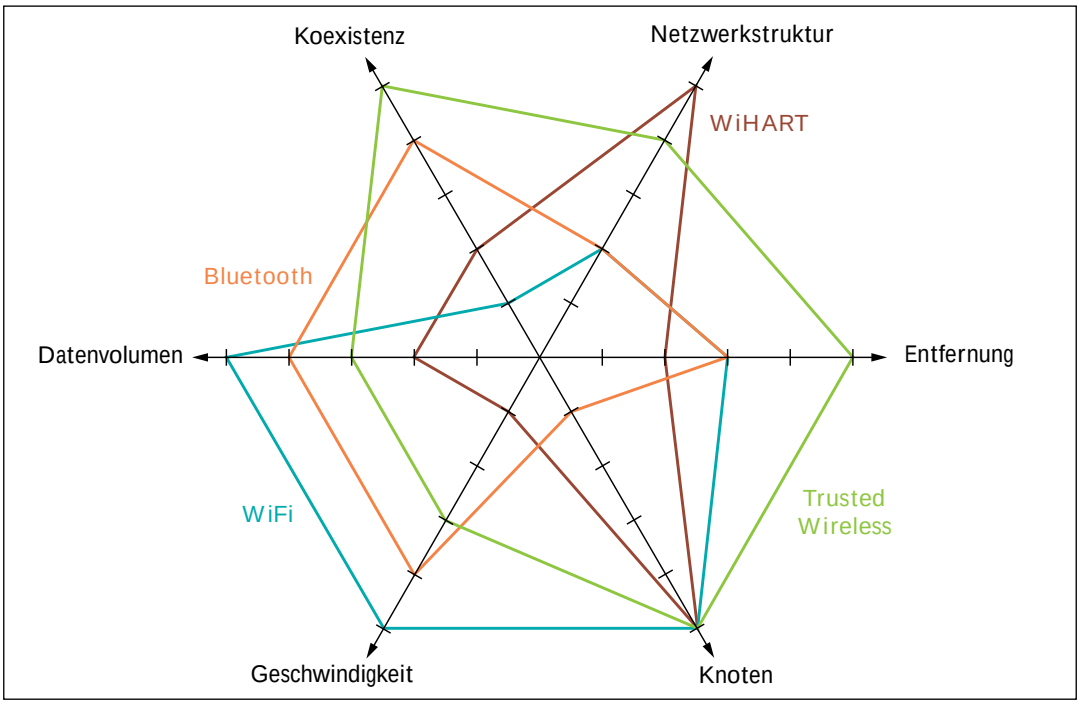


Abbildung 11

Vergleich verschiedener Funktechnologien im 2,4-GHz-Band

Außerdem stellt Trusted Wireless 2.0 im 868- und 900-MHz-ISM-Band eine private Alternative zu den Provider-abhängigen Low-Power-WAN-Netzwerken dar. Im Vergleich zu Sigfox, LoRa und anderen Anbietern in diesem Segment zeichnet sich Trusted Wireless 2.0 durch eine deutlich höhere Datenrate und Flexibilität aus. Durch die einzigartige Diagnosetiefe, die hohe Reichweite und den vollen Zugri auf das eigene Netzwerk, lassen sich große Netzwerke ohne Datenlimitierung aufbauen, deren Verfügbarkeit unabhängig von Netzausbreitung oder Betreibern ist. Das folgende Bild stellt die technologischen Eigenschaften von Trusted Wireless 2.0 mit anderen Funksystemen im 868- und 900-MHz-ISM-Band in Vergleich dar.

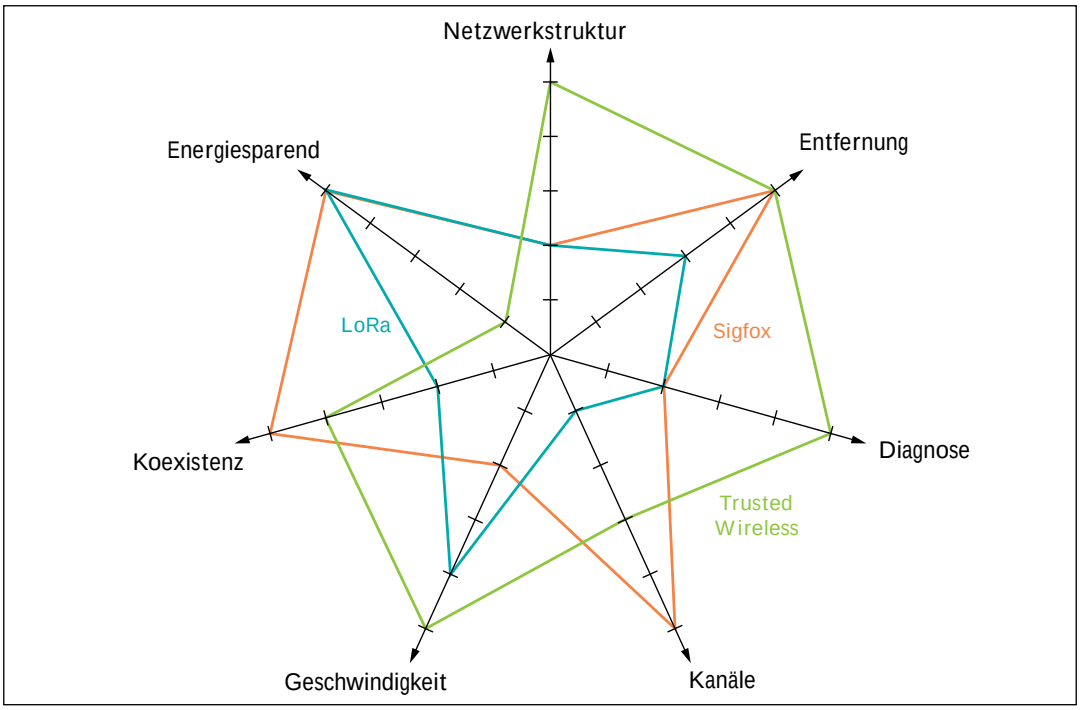


Abbildung 12
Vergleich verschiedener Funktechnologien im 868- und 900-MHz-ISM-Band

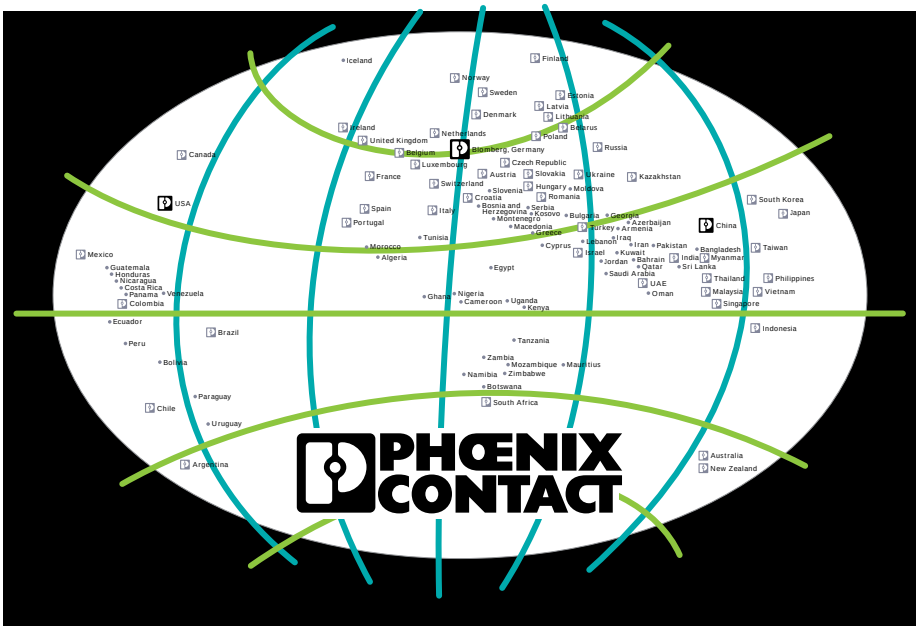
Glossar

AES	Advanced Encryption Standard
DSSS	Direct Sequence Spread Spectrum
EMV	Electromagnetische Verträglichkeit
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
ISM band	Industrial Scientific Medical band
LBT	Listen Before Talk
LOS	Line of sight
NLOS	Non-line-of-sight
OTA	Over-the-Air
P/C Zone	Parent-Child Zone
R & TTE	Radio and Telecommunications Terminal Equipment
RF band	Radio Frequency band
RFC	Request for Comments (Standardisierungsdokument der Internet Research and Development Gruppe, zum Beispiel zur Definition von Protokollen oder Diensten
RSSI	Receive Signal Strength Indicator
WLAN	Wireless Local Area Network

Weltweit im Dialog mit Kunden und Partnern

Phoenix Contact ist ein weltweit agierender Marktführer mit Unternehmenszentrale in Deutschland. Die Unternehmensgruppe steht für zukunftsweisende Komponenten, Systeme und Lösungen in der Elektrotechnik, Elektronik und Automation. Ein globales Netzwerk in mehr als 100 Ländern mit 15.000 Mitarbeitern garantiert die wichtige Nähe zum Kunden.

Mit einem breitgefächerten und innovativen Produktportfolio bieten wir unseren Kunden zukunftsfähige Lösungen für unterschiedliche Applikationen und Industrien. Das gilt besonders für die Bereiche Energie, Infrastruktur, Prozess und Fabrikautomation.



PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Deutschland
Tel.: +49 (0) 52 35 3-00
Fax: +49 (0) 52 35 3-4 12 00
phoenixcontact.net