

# TRUSTED WIRELESS

## Trusted Wireless™ – im Detail

### INTERFACE

Anwenderhinweis  
103146\_00\_de

© PHOENIX CONTACT - 11/2006



### Vorteile von Trusted Wireless™

Die **Trusted Wireless™**-Funktechnologie wurde speziell für industrielle Anwendungen von der kanadischen Firma Omnex Control Systems entwickelt. Die in den lizenzfreien Frequenzbändern 900 MHz und 2,4 GHz arbeitende Technik bietet eine extrem hohe Zuverlässigkeit und Robustheit. Sie zeichnet sich außerdem durch hohe Reichweiten, gute Interferenz- und Koexistenz-Eigenschaften sowie sehr gute Diagnose-Möglichkeiten aus.

Der vorliegende Anwenderhinweis zeigt, wie die Trusted Wireless™-Funktechnologie diese Eigenschaften erreicht und wie sie sich von anderen Techniken unterscheidet.

### Robustheit und Störsicherheit

Die Grundlage der Trusted Wireless™-Funktechnik ist ein sogenanntes Frequenzsprungverfahren (FHSS = **F**requency **H**opping **S**pread **S**pectrum). Das Frequenzsprungverfahren wurde 1942 von Hedy Lamarr und George Antheil erfunden und patentiert. Zum Einsatz kam es im militärischen Bereich zur störsicheren Steuerung von Torpedos. Außerdem wurde es verwendet, um das Abhören von militärischen Funknachrichten zu verhindern.

Bei einem solchen Verfahren werden die Funkübertragungen auf verschiedenen schmalbandigen Funkkanälen durchgeführt. Dabei wechseln Sender und Empfänger kontinuierlich die Übertragungsfrequenz. Die verwendeten Frequenzen und die Reihenfolge, in der sie benutzt werden, bilden das sogenannte Sprungmuster. Dieses Sprung-

muster ist pseudozufällig und nur dem Sender und dem Empfänger bekannt. Dadurch lässt sich die Kommunikation zwischen zwei Geräten von außen nicht verfolgen und ein Abhören der Nachricht ist nicht möglich.

Neben der Abhörsicherheit bietet das Verfahren aber noch weitere Vorteile. Durch den ständigen Wechsel der Funkfrequenz können Störungen sehr gut toleriert werden. Bild 1 zeigt, dass ein schmalbandiges Störsignal nur eine oder einige wenige benachbarte Frequenzen stören kann, wodurch möglicherweise ein Kommunikationszyklus behindert wird. Die Funktechnik wechselt beim nächsten Kommunikationszyklus auf eine andere Funkfrequenz und weicht damit dem Störsignal aus (siehe Bild 1). Dies geschieht – je nach Produkt – im Bereich einiger Millisekunden.

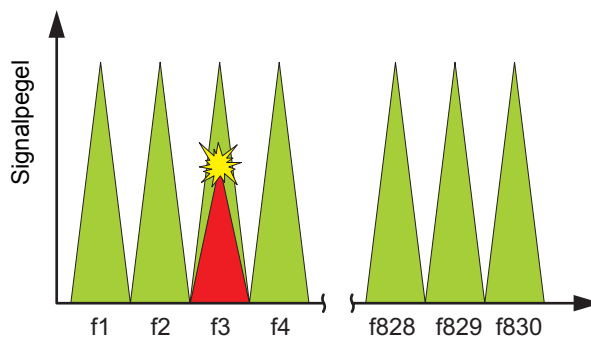


Bild 1 Frequenzwechsel nach einer Störung



Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.  
Diese steht unter der Adresse [www.download.phoenixcontact.de](http://www.download.phoenixcontact.de) zum Download bereit.

Die Trusted Wireless™-Funktechnik kann dabei je nach Anwendung auf bis zu 830 einzelne Funkfrequenzen zurückgreifen, welche pseudozufällig und über das ganze Band verteilt angesprochen werden (siehe Bild 2). Damit erzielt sie ein extrem hohes Maß an Störsicherheit und Robustheit.

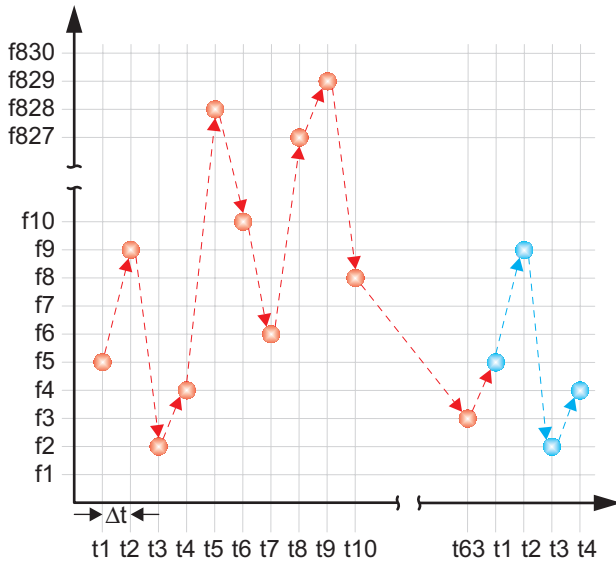


Bild 2 Frequenzsprungverfahren (Hoptime  $\Delta t = 27$  ms)

### Interferenzen

Alle Funksysteme unterliegen Interferenzen, d. h. die Signale am Empfänger überlagern sich. Sie sind eine Mischung aus dem Nutzsignal, seinen Reflexionen und anderen Funksignalen (siehe auch „Koexistenz“ auf Seite 3).

Die Interferenz durch Reflexionen ist ein physikalisches Phänomen. An einem örtlich festen Empfänger kommt das Nutzsignal durch Überlagerung des direkten Pfades und unendlich vieler Reflexionen an. Da die Reflexionen unterschiedlich lange Wegstrecken durchlaufen, sind die Amplituden am Empfänger unterschiedlich (Phasenverschiebung). Die entstehende Überlagerung kann zufälligerweise positiv sein, d. h. die Reflexionen verstärken das Signal. Sie kann aber auch negativ sein, sodass das Signal gedämpft wird. Dies kann bis hin zur kompletten Auslöschung des Funksignals geschehen, wodurch ein sogenanntes Funkloch entsteht.

Ein Funksystem, das auf einer festen Frequenz arbeitet, sieht sich immer mit diesem Problem konfrontiert. Ein Frequenzsprungsystem hingegen erreicht durch die Änderung der Funkfrequenz eine Änderung der Wellenlänge und somit eine Änderung der Reflexionsbedingungen an einem festen Ort. Unter der Voraussetzung, dass die Änderung der Frequenz oder der Wellenlänge genügend groß ist, kann somit auf der Frequenz  $f_1$  eine Auslöschung stattfinden (siehe Bild 3), aber auf der nächsten Frequenz  $f_2$  ist das Signal hinreichend stark (siehe Bild 4). Ein Frequenzsprungsystem bewegt sich also automatisch aus den möglichen Funklöchern heraus.

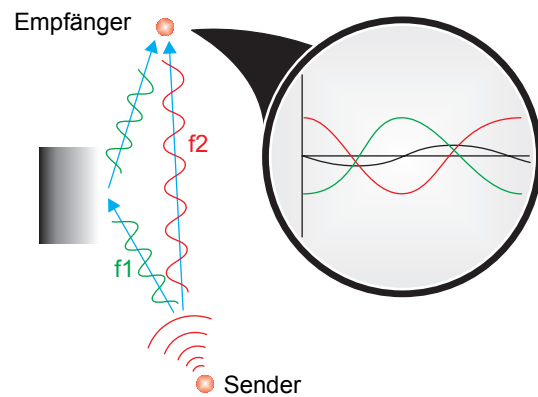


Bild 3 Auslöschung durch Interferenzen

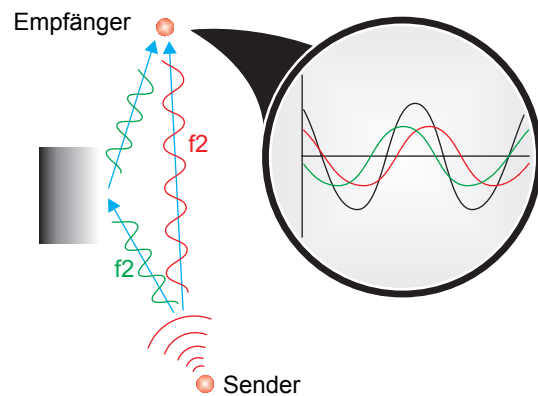


Bild 4 Ausreichendes Signal trotz Interferenzen

## Koexistenz

Die Frage der Koexistenz muss unter zwei Gesichtspunkten gesehen werden: zum einen die Koexistenz mehrerer Trusted Wireless™-Systeme nebeneinander und zum anderen die Koexistenz zu anderen Funktechniken.

Die Koexistenz mehrerer Trusted Wireless™-Systeme nebeneinander ist hervorragend, da die Systeme nicht alle zur Verfügung stehende Frequenzen, sondern nur ein Subset davon verwenden. Außerdem wird die Reihenfolge der benutzten Frequenzen so variiert, dass das Sprungmuster eines Trusted Wireless™-Systems einmalig ist. Somit gibt es keine zwei Trusted Wireless™-Systeme, die das gleiche Sprungmuster verwenden.

Dadurch lassen sich sehr viele Systeme parallel in räumlicher Nähe betreiben, ohne einander signifikant zu stören. Messungen haben ergeben, dass der Datendurchsatz bei einem Betrieb von 400 Systemen in räumlicher Nähe lediglich um durchschnittlich 50 % reduziert wird. Die Interferenz durch Nutzung parallel arbeitender Systeme, d. h. gegenseitige Störung, ist somit extrem gering.

Der zweite Aspekt hinsichtlich der Koexistenz ist das Verhalten zu anderen Funktechniken im gleichen Frequenzband.

Die Trusted Wireless™-Funktechnik verhält sich freundlich zu anderen Funksystemen, da sie zum einen sehr schmalbandige Sendefrequenzen nutzt, so dass andere Frequenzspringer (z. B. Bluetooth) problemlos parallel arbeiten können. Zum anderen können Sendefrequenzen oder Frequenzbereiche von der Nutzung ausgeschlossen werden, so dass sich die Trusted Wireless™-Technik auch problemlos zu WLAN-Systemen betreiben lässt. Bei nicht konfigurierbaren Trusted Wireless™-Produkten ist dies üblicherweise der Kanal 5 von WLAN (2422 MHz bis 2442 MHz). Bei den konfigurierbaren Produkten sind bis zu zwei WLAN-Kanäle auswählbar.

## Zuverlässigkeit und Diagnose

Die Zuverlässigkeit der Trusted Wireless™-Funktechnik wird durch bestimmte Software-Mechanismen im Protokoll weiter gesteigert. Die Kommunikationspakete werden dazu mit Sende- und Zieladressen versehen, die die Verwendung fälschlich empfangener Pakete verhindern. Außerdem wird über das gesamte Telegramm ein 16-Bit-CRC-Check gelegt, der die Korrektheit der Telegramme sicherstellt. Eine Forward Error Correction (FEC) hilft, auf der Übertragungstrecke beschädigte Informationen wiederherzustellen. Dazu werden dem eigentlichen Telegramm zusätzliche Bit-Informationen hinzugefügt, die eine Rekonstruktion nach mathematischen Algorithmen möglich machen.

Die Trusted Wireless™-Funktechnik bietet sehr gute Diagnose-Möglichkeiten, auf die je nach Produkt zugegriffen werden kann. Der Status der Funkverbindung wird über das „RF-LINK“-Signal diagnostiziert.

Die Qualität der Funkstrecke hingegen kann mittels eines analogen RSSI-Signals (**R**eceive **S**ignal **S**trength **I**ndicator) präzise überwacht werden. Dieses Signal kann in einer Anlage dauernd überwacht oder lediglich zur Inbetriebnahme und Ausrichtung der Antennen verwendet werden.

Auf die Paketfehlerrate und andere Parameter kann – je nach Produkt – direkt zugegriffen werden.

## Reichweite

Die Trusted Wireless™-Funktechnik ist für mittlere und große Reichweiten optimiert worden. Erzielbar sind bei Verwendung geeigneter Antennen und unter Einhaltung der jeweils gesetzlichen Richtlinien und Maximalwerte folgende Distanzen:

- Im 900-MHz-Band bei 1 W Sendeleistung typisch 15 Meilen (= 25 Kilometer)
- Im 2,4-GHz-Band bei 10/100 mW typisch 3 Kilometer.

Diese Werte können – je nach Applikation – deutlich unter- oder überschritten werden.

Parameter, die die Reichweite eines Funksystems beeinflussen, sind zum einen die Energie pro Bit, die verwendet wird, um die gewünschten Informationen zu übertragen, und zum anderen die Empfängerempfindlichkeit.

## Energie pro Bit

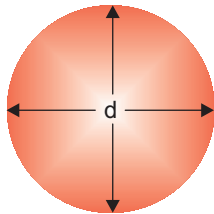
Je höher die Energie pro Bit, umso größer ist die erzielbare Reichweite. Daher ergeben sich theoretisch zwei Ansätze: Entweder die Energie erhöhen oder die Übertragungsrate senken. Die Energie ist gesetzlich limitiert auf 36 dBm im 900-MHz-Band und auf 20 dBm im 2,4-GHz-Band. Beide Werte gelten für die an der Antenne abgestrahlte Leistung EIRP (**E**ffective **I**sotropic **R**adiated **P**ower), d. h. sie beinhalten sowohl die Sendeleistung der HF-Stufe als auch alle Gewinne und Verluste der angeschlossenen Antenne.

Da die Energie also nicht beliebig vergrößerbar ist, kann nur die Übertragungsrate gesenkt werden. Trusted Wireless™ verwendet je nach Anwendung die minimal notwendige Übertragungsrate, sodass ein Maximum an Energie pro Bit erzielt werden kann.

In Bild 5 ist zu sehen, wie die Energie pro Bit eines Trusted Wireless™-Systems trotz der niedrigeren Sendeleistung weitaus höher ist als die eines WLAN-Systems.

$$\frac{10 \text{ mW}}{19200 \text{ bps}} = 520 \text{ nWs/Bit}$$

$$\frac{100 \text{ mW}}{11 \text{ Mbps}} = 9 \text{ nWs/Bit}$$



Trusted Wireless™



WLAN

Bild 5 Energie pro Bit

Bei einem Vergleich zu einem 900-MHz-Trusted Wireless™-System würde die Energie pro Bit aufgrund der Sendeleistung von 1 W sogar noch 100-mal höher sein.

### Empfängerempfindlichkeit

Die Empfängerempfindlichkeit ist ein entscheidender Parameter für die maximale Reichweite.

Allgemein gesehen verdoppelt sich die Reichweite bei einer Erhöhung der Signalstärke bzw. der Empfindlichkeit um +6 dB bzw. -6 dB. Dies kann auf der Senderseite durch eine Erhöhung der Sendeleistung oder den Einsatz einer Antenne mit höherem Gewinn erzielt werden (Achtung: Die abgestrahlte Leistung EIRP ist gesetzlich begrenzt).

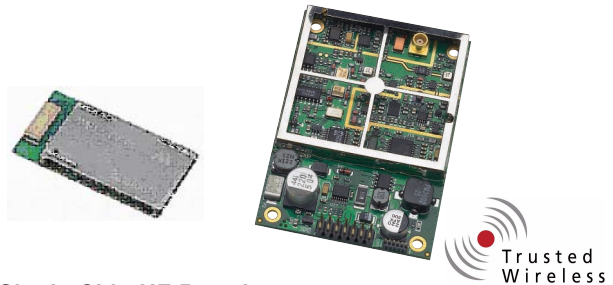
Viel entscheidender wirkt sich aber eine höhere Empfängerempfindlichkeit aus, da diese nicht gesetzlich begrenzt ist und stark von der verwendeten Schaltungstechnik und Qualität und Güte der verwendeten Bauteile abhängt.

In Bild 6 ist ein Standard-Single-Chip-Bluetooth-Board dargestellt. Aufgrund der stark reduzierten Herstellungsprozesse solcher Single-Chip-Lösungen liegt die Empfängerempfindlichkeit typischerweise bei ca. -80 dB. Daneben ist die diskrete Realisierung eines Trusted Wireless™-Funkboards dargestellt. Durch den Einsatz vieler Spezialkomponenten kann – je nach Produkt – eine typische Empfängerempfindlichkeit von bis zu -110 dB bis -115 dB erreicht werden. Das bedeutet einen Unterschied von 30 dB oder einen Faktor von 1000. Das Trusted Wireless™-Board ist also 1000-mal empfindlicher als das Bluetooth-Board (siehe Bild 6).

Wie oben aufgeführt, bewirkt die Verbesserung der Empfindlichkeit um -6 dB eine Reichweitenverdopplung. Daher ergibt sich bei 30 dB Unterschied eine 32-fache Reichweite der Trusted Wireless™-Lösung gegenüber der dargestellten Single-Chip-Bluetooth-Lösung:

$$6 \text{ dB} + 6 \text{ dB} + 6 \text{ dB} + 6 \text{ dB} + 6 \text{ dB} = 30 \text{ dB}$$

$$\rightarrow 2 \times 2 \times 2 \times 2 \times 2 = 2^5 = 32\text{-fach}$$



### Single-Chip-HF-Board

Typische Bluetooth-Empfängerempfindlichkeit:  
**-80 dB**

### Diskretes HF-Board

Typische Trusted Wireless™-Empfängerempfindlichkeit:  
**-110 dB bis -115 dB**

Bild 6 Empfängerempfindlichkeit

© PHOENIX CONTACT 11/2006