

ZigBee - Protokollsoftware und Entwicklungsumgebung

Überblick

Der ZigBee Standard basiert auf zwei voneinander unabhängigen Standards. Das sind der IEEE 802.15.4 Standard für "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)" und dem eigentlichen ZigBee Protokoll der ZigBee Alliance, einer Vereinigung von Firmen, die die Entwicklung und Standardisierung bei ZigBee durchgeführt haben. ZigBee setzt dabei immer auf 802.15.4 auf. Ein anderer Physical Layer ist bei ZigBee nicht definiert. In den PHY und MAC Layer sind aber auch Verfahren (z. B. Beacon Mode) von HomeRF bzw. HomeRF lite eingeflossen.

Im Folgenden wird der ZigBee Protokollstack, die Applikationsschichten und die Vorgehensweise bei einer ZigBee Entwicklung beschrieben. Bezüglich der PHY/MAC Layer, der grundsätzlichen Eigenschaften und Anwendungen wird auf einschlägige Artikel verwiesen.

Bild 1 zeigt die aktuelle (Version 0.9) Architektur des ZigBee Protokollstack. Dabei fällt die stark erhöhte Anzahl (von 32 auf 240) der Application Object's auf.

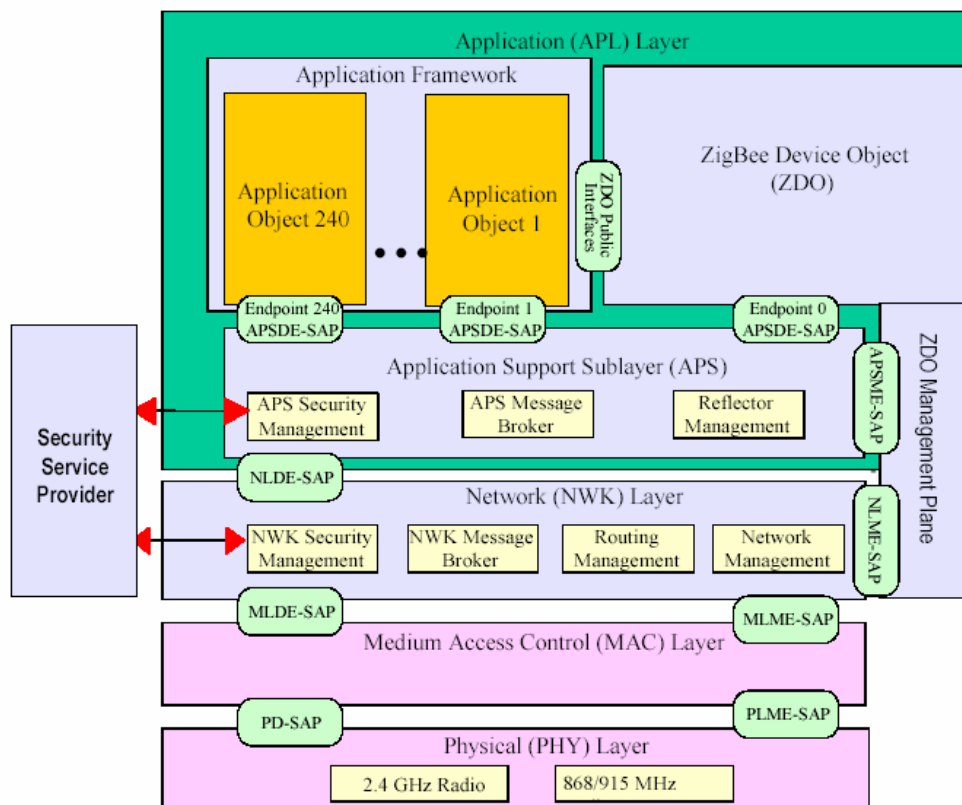


Bild 1 ZigBee Protokollstack nach Version 0.9

Der im Bild gezeigten PHY und MAC Layer entsprechen IEEE 802.15.4. Alle hellblau gezeichneten Blöcke wurden von der ZigBee Alliance definiert. Die in hellbraun gezeichneten Application Object's werden vom Entwickler des jeweiligen Gerätes bestimmt. Er kann dabei den Empfehlungen der ZigBee Alliance folgen, oder aber auch eigene Objects definieren. Dabei besteht eine größtmögliche Freiheit in der Auslegung der Application Object's. Da die Normung bei IEEE und der ZigBee Alliance unabhängig voneinander durchgeführt wurde, ist die Verwendung unterschiedlicher Begriffe unvermeidlich. **Tabelle 1** stellt die Begriffe von IEEE 802.15.4 denen von ZigBee gegenüber. ZigBee definiert den Coordinator, Router und das End Device als ein logisches Device.

IEEE 802.15.4 Spezifikation (physikalische Begriffe)	ZigBee Spezifikation (logische Namen)
Personal Area Network (PAN) Coordinator	ZigBee Coordinator
Full Function Device (FFD)	ZigBee Coordinator, Router oder End Device
Reduced Function Device (RFD)	End Device

Die IEEE Begriffe definieren wesentliche Merkmale eines Devices. Diese sind u. a. die Arbeitsweise in einem Personal Area Network (nicht einem ZigBee Netzwerk!) und die Art wie Geräte gefunden und sich miteinander verbinden.

ZigBee Protokollstack

Der im Bild 1 gezeigte Protokollstack wurde in eine Reihe von Standards definiert. Diese sind:

- Network Specification, Version 0.9
- Der Applikation Layer bestehend aus dem:
 - Application Support Sub-Layer Specification, Version 0.9
 - ZigBee Device Objects, Version 0.9
 - ZigBee Application Framework, Version 0.9
 - ZigBee Device Profile, Version 0.9

Die Standardisierung der ZigBee Alliance umfasst auch die Definition von Profilen. Diese werden gesondert besprochen.

Der Protokollstack ist natürlich nicht unabhängig von der verwendeten Hardware.

Der Network Layer adaptiert die PHY und MAC Layer Funktionen auf die höheren Schichten des ZigBee Stack. Die PHY und MAC Layer Funktionen sind durch IEEE 802.15.4 und durch die Hardware (ZigBee/IEEE 802.15.4 Controller) bestimmt.

Die Übertragung der Daten erfolgt in Frames. Diese bilden die Daten der höheren Schichten auf den MAC bzw. den PHY Layer ab. **Bild 2** zeigt die bei IEEE 802.15.4 und ZigBee verwendete Framestruktur.

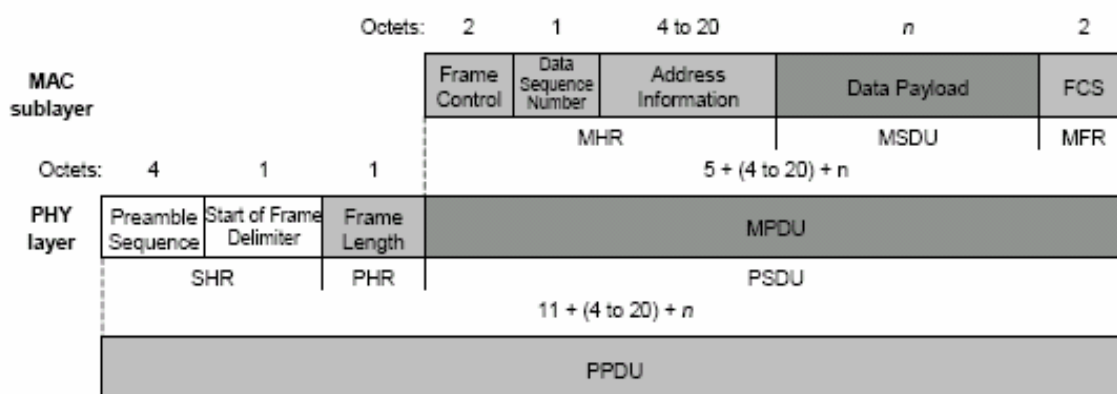


Bild 2 IEEE 802.15.4/ZigBee Framestruktur

Die maximale Größe der ZigBee Nutzdaten beträgt zwischen 102 und 127 Byte. Die genaue Größe hängt von der verwendeten Adressierung ab. Diese Datenmenge sollte für die meisten typischen ZigBee Anwendungen mehr als ausreichend sein.

Im Falle von Sensoren für z.B. verschiedenen Messwerte und Alarmgeber werden sicher nur ein paar Bytes verwendet.

Der **Network Layer** (NWK) ist verantwortlich für die Vergabe von 16 Netzwerkadresse (nur mit dieser werden Pakete im Netz weitergeleitet), den Aufbau des Netzwerkes, die Teilnahme und das Verlassen von Devices in bzw. aus einem Netz, für die Sicherheit des zu übertragenden Frames und das Routing von Frames in einem Mesh oder Tree Netzwerk.

Der ZigBee Network Layer (NWK) unterstützt Star, Tree und Mesh Topologien. In einer Star Topologie wird das Netzwerk vom ZigBee Coordinator kontrolliert. Der Coordinator ist führt den Verbindungsaufbau mit anderen Devices zuständig. Alle anderen Devices kommunizieren mit dem Coordinator. In einer Mesh oder Tree Topologie ist der Coordinator für den Aufbau des Netzes zuständig. Das Netzwerk kann aber durch die Verwendung von Routern vergrößert werden. Dabei wird ein hierarchischer Routing Algorithmus verwendet. Im Tree Netz erfolgt die Weiterleitung der Daten entlang (Auf/Ab) des Tree basierend auf den Netzwerkadressen. Bei Mesh erfolgt die Verwendung eines vereinfachten Ad Hoc On Demand Distance Vector Routing (AODV) Verfahrens. Im NWK wird die Datenlieferung nicht garantiert. Fragmentation und Reassembly wird nicht unterstützt.

Für die Vergabe von garantierter Bandbreite an bestimmte Nodes im Netz, können so genannte Beacons (Zeitschlitz) verwendet werden. Beacons werden im Star und Tree Netzwerk, nicht aber im Mesh Netzwerk über Router hinaus verwendet.

Um diese Funktionalität realisieren zu können, besitzt der NWK ein Interface zum MAC Sub-Layer. Dieses Interface stellt in einem Funktionsblock Services für Daten und das Management zur Verfügung. Dieser Funktionsblöcke (bei ZigBee: Entity) sind die NWK Layer Data Entity (NLDE) für die Datenübertragung und die NWK Layer Management Entity (NLME) für das Management der Verbindungen eines Devices. Die NLME verwaltet auch eine Liste (Network Information Base, NIB) der zu verwalteten Objekte bzw. Devices.

Network Layer Data Entity (NLDE)

Die zu übertragenden Daten werden im NWK als Application Protocol Data Units (APDU) abgebildet und zwischen den beteiligten Devices übertragen. Die beteiligten Devices müssen sich im selben Netzwerk befinden. Die Datenpakete werden mit zusätzlichen Protokoll Headern und Informationen für das Routing versehen. Die Routing Informationen beinhaltet entweder den nächsten Hop (Router) oder das endgültige Ziel.

Network Layer Management Entity (NLME)

Für die Konfiguration eines Devices und den Betrieb innerhalb des Netzwerkes können bestimmte Parameter gesetzt werden. Diese sind:

- Betriebsart als ZigBee Coordinator oder End Device bzw. Router
- Start des Netzwerkes J/N
- die Möglichkeit in ein Netzwerk aufgenommen zu werden bzw. dieses zu verlassen.
- Möglichkeit das Coordinator oder Router ein Device zum verlassen des Netzes auffordern
- Möglichkeit der Adressvergabe durch den Coordinator und Router
- Erkennung der nächsten (One Hop) Nachbarn
- Erkennung des Routing Pfades
- Möglichkeit für ein Device zu erkennen, ob und für wie lange der Empfänger aktiv ist.

Die ZigBee Hardware (IC) wird mit einem angepassten Network Layer gemäß Network Specification geliefert. Eine ZigBee konforme Anpassung ist heute (September 2004) für Chipcon und Motorola Hardware lieferbar. Mit diesen Anpassungen wird dem Entwickler der Einsatz von ICs dieser Hersteller wesentlich erleichtert.

Der **Application Support Sub-Layer** ist für die Verwaltung der Binding Tabelle und der Weiterleitung der Messages zwischen Devices, die über die Binding Tabelle verbunden sind zuständig. Binding ist die Herstellung einer logischen unidirektionalen Verbindung zwischen einem Source Endpoint/Cluster und einem Destination Endpoint, der sich auf einem oder mehreren Devices befindet. Binding kann mit oder ohne Anwendereingriff erfolgen. Binding ermöglicht die Verbindung von Devices basierend auf deren Services und Anforderungen.

Bild 3 zeigt das Binding in einem Beispiel zwischen Lichtschalter und Lampen die alle über einem ZigBee Radio angesteuert werden.

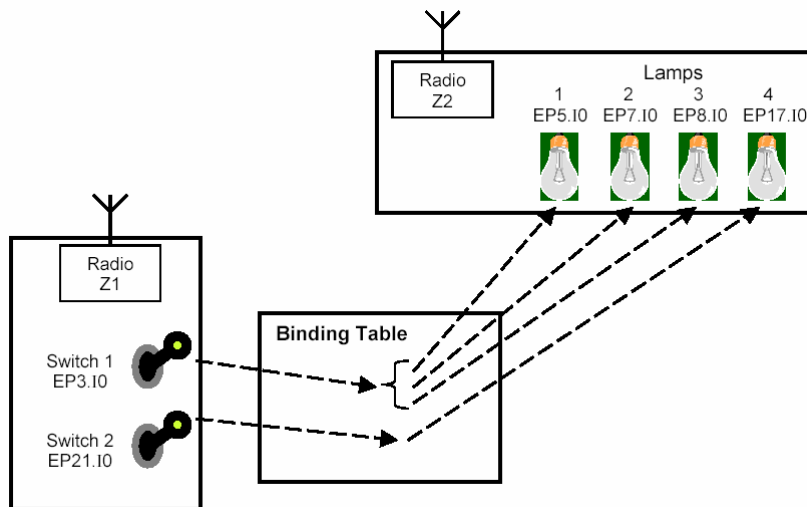


Bild 3 Binding zwischen unterschiedlichen ZigBee Devices.

Der **Application Support Sub-Layer** übernimmt folgende Aufgaben im Netzwerk:

- Definition des logischen Device Typ
- Multiplexing der eingehenden Daten
- Anwendung/Entfernung von Sicherheitsmechanismen auf dem Applikation Layer
- Message Reflection für indirekte Adressierung

Der Application Support Sub-Layer hat ein Datenformat. Im NWK wird die Datenlieferung nicht garantiert. Fragmentation und Reassembly wird nicht unterstützt.

ZigBee Device Objects (ZDO) ist zuständig für die Initialisierung aller ZigBee Layer auf dem Devices außer den Endpoint Anwendungen zuständig. Darunter fallen die Festlegung der Rolle (Coordinator oder End Device) eines Devices im Netzwerk, die Veranlassung und Bearbeitung von Binding Requests und den Aufbau einer sicheren Verbindung. ZDO ist auch für das Suchen (Discovery) von Devices im Netzwerk und die Bestimmung der unterstützten Services zuständig. Im ZDO erfolgt die Festlegung der eigentlichen ZigBee Funktionalität eines Devices. Über den NWK und MAC bzw. PHY Layer erfolgt die Umsetzung der Device Konfiguration auf die Layer, die diese Funktionen letztendlich ausführen müssen.

Beispiele einer solchen Konfiguration sind:

- Festlegung des verwendeten Kanals für Network Scan. Default ist die Verwendung aller Kanäle im ausgewählten Frequenzband (868 MHz, 915 MHz oder 2,4 GHz).
- Auswahl eines Kanals für den Aufbau eines Netzwerks.
- Rejoin eines Netzwerks
- Direktes Join und Join über Proxy

ZDO ist eine wesentliche Komponente eines jeden ZigBee Devices. Im ZDO wird das Verhalten des Devices im Netz bestimmt.

Das **ZigBee Application Framework** ist eine Umgebung in welcher die Applikationsobjekte auf einem ZigBee Device abgelegt werden. Innerhalb dieser Umgebung senden und empfangen die einzelnen Objekte Daten über Service Access Points (SAP). Diese Operationen werden mittels Request, Confirm, Response und Indication durchgeführt.

Es können maximal 240 Endpoints per ZigBee Device (0 ist reserviert für die generischen Merkmale und Funktionen eines Devices, 255 ist reserviert für Broadcast, 241-254 ist reserviert für zukünftige Anwendungen) angelegt werden. Für die Kommunikation mit den Endpoints stehen 2 Services zur Verfügung:

Key Value Pair Service (KVP)

Damit ist es möglich, definierte Attribute im Application Object mit GET, SET, GET RESPONSE und EVENT TRANSACTION zu manipulieren. Acknowledgement (empfohlen) kann optional gesendet werden. Das Format ist ein komprimiertes XML. Das ist sehr gut für kleine Devices mit nur begrenzten Ressourcen geeignet.

Message Service (MSG)

Viele ZigBee Anwendungen werden kundenspezifische Anwendungen einsetzen. Diese lassen sich nicht gut auf den Key Value Pair Service abbilden. Auch ist der Overhead bei KVP für die Abbildung der State Variablen u. U. nicht erwünscht. Dafür wird ein generischer Message Service (MSD) verwendet. Der Transport ist identisch zum KVP. Der Unterschied ist, dass das Datenfeld im APS Frame nicht definiert ist und frei spezifiziert werden kann.

Das **ZigBee Device Profile** beschreibt vollständig ein Device mit allen Merkmalen und Eigenschaften. Dafür werden Parameter für das Device und Service Discovery, End Device Bind Request Processing, Bind/Unbind Command Processing und das Network Management zur Verfügung gestellt. Tabelle 2 beinhaltet alle Parameter für das Device und Service Discovery des Clients beschreibt. Hier wird recht gut ersichtlich, welche Parameter vom Entwickler zu setzen sind.

Device and Service Discovery Client Services	Client Transmission	Server Processing
NWK_addr_req	O	M
IEEE_addr_req	O	M
Node_Desc_req	O	M
Power_Desc_req	O	M
Simple_Desc_req	O	M
Active_EP_req	O	M
Match_Desc_req	O	M
Complex_Desc_req	O	O ¹
User_Desc_req	O	O ¹
Discovery_Register_req	O	O ¹
End_Device_annce	O	O

Tabelle 2 Parameter des Client für Device und Service Discovery.

Mit den Desc_req Kommandos werden Diskriptoren des jeweiligen Devices ausgelesen. Diskriptoren sind abhängig vom Device und seiner Arbeitsweise (z. B. unterschiedliche Power Modes). Die Diskriptoren sind eigentlich Teil der ZigBee Application Profils.

Anwendung und Profile

ZigBee kann für beliebige Anwendungen eingesetzt werden. Auf Grund der gewählten Merkmale des NWK ist ZigBee sehr gute für größere Netze mit hunderten oder gar mehreren Tausend Nodes geeignet. Die integrierten Routing Funktionen bieten auch Sicherheit bei Ausfall einzelner Netzelemente. Ziel von ZigBee ist nicht so sehr eine kundenspezifische Vernetzung Punkt-zu-Punkt Verbindung zwischen 2 Geräten. Es geht primär um die Vernetzung mit vielen Teilnehmern und um die Interoperabilität zwischen Geräten verschiedener Hersteller.

Der Interoperabilität wird bei ZigBee viele Aufmerksamkeit geschenkt. Um diese auf Applikationsebene zu erreichen, wurden die ZigBee Application Profils definiert. Dabei werden Gerätefunktionen für eine bestimmte Anwendung definiert. Das erste ZigBee Anwendungsprofil ist das Home Control Lightning Profil. Dieses profil definiert den Einsatz und die Möglichkeiten von ZigBee für die Steuerung unterschiedlicher Lichtquellen und deren Einsatz.

Das Home Control Lightning Profil besteht aus einer Reihe von Device Beschreibungen für die jeweilige Anwendung. Definiert sind heute:

- Light Sensor Monochromatic
- Switch Remote Control
- Dimmer Remote Control
- Occupancy Sensor
- Switching Load Controller
- Dimming Load Controller

Die im Home Control Lightning Profil und den Beschreibungen eines Device festgelegten Parameter erlauben die Entwicklung von Einsatz von Schaltern und Lichtsteuerungen sowie den Einsatz dieser Geräte von unterschiedlichen Herstellern. Komplexe Lichtsteuerungen lassen sich dann mit Geräten verschiedener Hersteller aufbauen. Beispiel wäre eine Occupancy Sensor des Hersteller A mit einem Lichtschalter und Load Controller von Hersteller B. Die dafür notwendigen Definitionen werden in Clustern abgelegt. Nicht alle Cluster müssen dabei integriert werden. Es gibt dabei mandatory und optionale Cluster. **Bild 4** zeigt die graphische Darstellung eines ZigBee Switching Load Controller. **Tabelle 3** zeigt dessen Cluster (nicht vollständig).

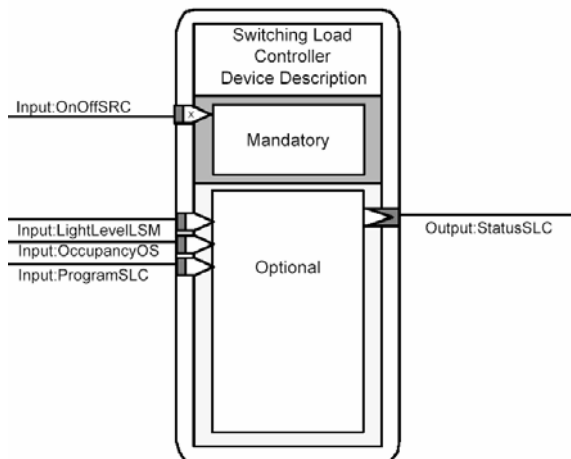


Bild 4 ZigBee Switching Load Controller

Mandatory Clusters		
ClusterName	AttribName	Description
Input:OnOffSRC		ON or OFF commands to external device
	OnOff	Outputs ON and OFF command to external device
Optional Clusters		
ClusterName	AttribName	Description
Input:LightLevelLSM		Current light level reading for Light Sensor Monochromatic
	CurrentLevel	Current light level reading
Input:OccupancyOS		Current occupancy state for Occupancy Sensor
	CurrentState	Current occupancy state of area being monitored (see Table 4-2 for details)
Input:ProgramSLC		Program input to set up key parameters for the Switching Load Controller
	Override	Outputs no longer report data or send control commands until placed in Auto Mode
	Auto	Override is disabled, all Clusters are enabled
	FactoryDefault	Resets all Attributes to factory defaults
	ResetO_LSSLC	Reset Output Load Status to zero
	PresetO_LSSLC	Preset Output Load Status
	BrownOutMinVolt	Minimum voltage level for brown out detection
	ShutDownPKCurrent	Peak Current for shut down
	MeteringPeriod	Length of Metering period in minutes for StatusSLC Attributes
	Output:StatusSLC	
OnOff		Load ON contains data 0xFF, load OFF contains data 0x00
RunTime		Total time load is ON
Watts		Real power consumed by load in watts
TotalPower		Total Real and Reactive Power consumed by load in watts
Energy		Real power * time = Watts * runtime
Vars		Vars (Reactive Power)

Tabelle 3 Cluster des Switching Load Controller

Die Möglichkeit eigene Profile zu definieren ist bei ZigBee gegeben. Was sind die Schritte wenn ein kundenspezifisches Profil integriert werden muss?

- Definition des Devices im Systems
- Abbildung auf ein logisches Devices
- Definition des Profil mittels Partitionierung des Devices
- Definition der Device Descriptions innerhalb des Profils
- Definition der Cluster und Festlegung der Aus- und Eingänge

Um die Kommunikation und die Arbeitsweise der Profile bei ZigBee zu beschreiben, kann wie folgt zusammengefasst werden:

- Devices werden durch Application Objects beschrieben.
- Application Objects kommunizieren durch den Austausch von Clustern und Attributen.
- Jedes Profile Object kann einen oder mehrere Clusters und Attribute enthalten.
- Binding stellt einen Mechanismus für den Austausch von Cluster und Attributen dar.
- Clusters und Attributes werden gesendet zum:
 - Ziel Application Object (Target Device)
 - ZigBee Coordinator, von da evtl. Weiterleitung an ein oder mehrere Targets.
- Generisch ZigBee Device Funktionen werden durch ZDO beschrieben.

Profile sind ein Satz von Clustern und Attributen die eine Anwendung (Home Control Lightning) beschreiben. Ein Endpoint ist eine physikalische Struktur auf einem ZigBee Controller welches mehrere Anwendungen (angesprochen über Endpoint Nummern 1-240) unterstützt. Es gibt maximal 240 Endpoints auf einem Device. Ein Profil pro ein Endpoint.

Entwicklung für ZigBee

Aktuell sind Entwicklungskits von Chipcon und Freescale erhältlich. Diese Kits werden mit angepassten NWK von Figure8Wireless und Entwicklungstools ausgeliefert. Zusätzlich werden auch ZDO, Application Support Sub-Layer und ein Betriebssystemlayer mitgeliefert. Die Entwicklung erfolgt mit den Tools der jeweiligen Basisband CPU. Die Stackkonfiguration ist für die meisten Parameter des NWK, ZDO und Device Profile möglich.

Als Tools stehen Z-Trace für die Ausführung von NWK Systems und Device Description API Aufrufe zur Verfügung.

Für die Anpassung der Devices gibt es den Configurator (**Bild 5**). Damit lassen sich Coordinator/Router (Größe der Routing Tabelle), Kanalliste, Superframe/Beacon Order; im Application Layer Node Descriptor, Power Descriptor, Simple Descriptors für alle Endpoints/Interfaces, Complex Descriptor, User Descriptor, Security Enabled/Disabled, Master Keys, End Device Bind Timeout, Größe der Link Key und Binding Tabelle einstellen.



Bild 5 Configurator

Die Möglichkeit eigene Profile zu definieren ist bei ZigBee gegeben. Dieser Vorgang wird durch den Z-Profile Builder von F8W sehr vereinfacht.

Die Konformität von ZigBee Produkten (inkl. Hardware und Software für die Entwicklung) wird von unabhängigen Testbüros (u. a. Dr. Genz und TÜV Rheinland) sichergestellt. ZigBee Produkte können Plattform oder Profil kompatibel sein.

Installation von ZigBee Netzen

Folgende Punkte sollten bei der Installation größerer ZigBee Netze und der Device Konfiguration berücksichtigt werden:

- Maximale Entfernung zwischen Coordinator und Router ist 25-30 Meter
- Einstellung der Power Save Modes in der ZigBee Hardware
- Batterie- oder Netzbetrieb des Coordinator?
- Wie können Devices im laufenden Netz ersetzt werden?
- Wie können Devices in einem bestehenden Netz hinzugeführt werden?
- Wie werden die Master Keys für Security verwaltet?

Für alle vorgenannten Punkte gibt es in einer ZigBee Implementierung Lösungen. Die Devices müssen nur entsprechend konfiguriert werden.

ZigBee und die Weiterentwicklungen

An ZigBee wird weiter entwickelt. Neue Features sind die Verbindung von 2 und mehr Netzwerken miteinander im laufenden Betrieb, Power Failure Recovery, Multicasting, Profile für Building Automation, Support für Bacnet, LONworks, Modbus und asymmetrische Schlüssel.

September 2004
Rudi Latuske

Informationen

www.zigbee.org

www.ieee802.org/15/pub/TG4.html

www.chipcon.com

www.freescale.com

www.ars2000.com