world of solutions

Offizieller Medienpartner embeddedworld2020

Organ der GMM VDE/VDI-GESELLSCHAFT MIKROELEKTRONIK, MIKROSYSTEM- UND FEINWERKTECHNIK

Elektronik

02 **23. Januar 2020** 8,00 €

DIGITALISIERUNG

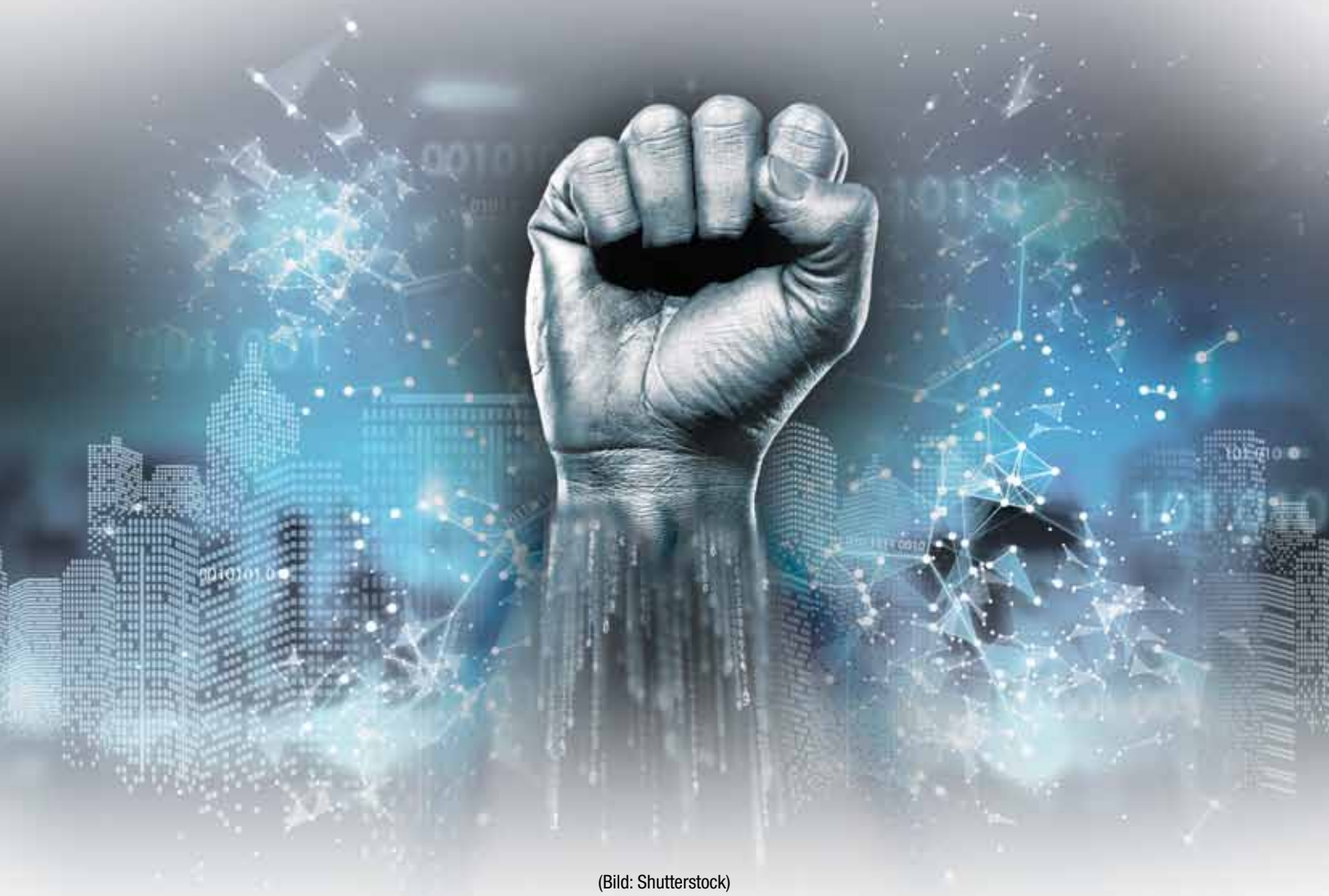
DIE IOT-REVOLUTION FÜR KOMMERZIELLE GEBÄUDE

Netzwerke aus Licht für Industrie und öffentlichen Raum

Datengold schürfen im IIoT mit Edge-Computing

SICHERE UND ZUVERLÄSSIGE FUNKVERNETZUNG

DIE IOT-REVOLUTION FÜR KOMMERZIELLE GEBÄUDE



(Bild: Shutterstock)

Der IoT-Standard für die Funkkommunikation IP500 wurde entwickelt, um die härtesten Ansprüche in kommerziellen Gebäuden adressieren zu können. Mit der EN-Pre-Konformität, bescheinigt vom Verband der Sachversicherer (VdS), positioniert sich der IP500-Standard im Wireless-IoT-Markt als „Hidden Champion“ für kritische Anwendungen.

Von Helmut Adamski und Witali Gisbrecht

Mit den jüngsten Erfolgen der IP500 Alliance [1] hat ein neues Kapitel im IoT-Markt für kommerzielle Gebäude begonnen. Dieses Kapitel haben namhafte Hersteller (Global Player) von Sicherheitsprodukten vor ca. zehn Jahren begonnen zu schreiben.

Zur Erinnerung: Zu der Zeit haben andere Wireless-IoT-Standards im Markt versucht, den IoT-Markt für sich zu gewinnen. Was ja zum Teil für den Smart-Home-Markt gelungen ist und aktuell im Wide-Area-IoT-Markt für Smart-City-Anwendungen versucht wird. Dennoch ist die Distanz (Gap) von bekannten Wireless-IoT-Systemen zum Endanwender und geforderten Normen im kommerziellen Sektor enorm groß. Warum ? – weil technische Herausforderungen im Gesamtbild einer Wireless-IoT-Plattform zusammenspielen müssen. Das heißt, dass unterschiedliche Anforderungen gleichzeitig von einer Wireless-IoT-Plattform unterstützt werden müssen; so als Beispiel eine sehr niedrige zeitliche Verzögerung (Latenz) im IoT-Netzwerk und gleichzeitig eine hohe Datenrate und Reichweite, und das robust und sicher mit einem geringen Energie-Budget der End-Sensoren. Das erscheint auf dem ersten Blick nicht möglich – ist es aber, wenn das gesamte System immer wieder zwischen der Anwendung und der Lösung abgestimmt wird.

Möchte ein Entwickler nur eine bestimmte IoT-Applikation bedienen, so reicht es aus, sich auf wenige oder gar einen technischen Parameter zu konzentrieren z.B. eine hohe Reichweite. Falls jedoch zusätzlich hohe Datenraten und niedrige Latenz gleichzeitig gefordert werden, wird das Angebot geeigneter Funkstandards für diese IoT-Anwendung sehr dünn. Das erfahren Anwender mit anderen Wireless-IoT-Standards; sie sehen sich in einer bestimmten Applikationen „gefangen“, wenn sie neue Funktionen implementieren wollen.

DIE IOT-REVOLUTION KANN BEGINNEN

Das Ziel der IP500 Alliance war von Anfang an: eine Wireless-IoT-Plattform zu etablieren, die alle Smart-Sensor-Applikationen in einem Gebäude in ein und derselben Infrastruktur vernetzen kann. Vergleichbar mit dem WLAN-Standard, der sich für IT-Applikationen als Wireless-Standard durchgesetzt hat (**Bild 1**).

Geht man in Gedanken alle Applikationen in kommerziellen Gebäuden durch, so sind vor allem die Sicherheits-Applikationen in einem IoT-Netzwerk von höchster Bedeutung. Dies erfordert eine Interoperabilität aller IP500-Produkte, egal von welchem Hersteller ein Produkt gefertigt wird.

Diesen Gedanken hat die IP500 Alliance konsequent über die Jahre umgesetzt und hat „Best-In-Class“ Funktechniken in einer geschickten Konstellation

IP500 ALLIANCE

Die IP500 Alliance startete ihre Aktivitäten als Interessensgruppe mit namhaften global agierenden Herstellern, nachdem in 2007 der IEEE-Standard 802.15.4 (2006) ratifiziert wurde. Das gesetzte Ziel war es, aus der Systemsicht des Anwenders, Regularien und Applikationen für das robusteste IoT-System für kommerzielle Gebäude auf Basis des IEEE- und IPv6-Standards zu definieren und mit Partnern zu entwickeln und zu etablieren.

Im Mai 2010 hat sich dann die IP500 Alliance im historischen VDI-Haus in Berlin als eingetragener Verein (e.V.) formiert und ihre Arbeit begonnen.

Die bisherige Arbeit war im Wesentlichen durch drei Phasen geprägt:

➔ **2005–2009:** Mitarbeit an den IEEE-802.15.4- und IPv6-Standards und Formierung der IP500-Spezifikation.

➔ **2010–2013:** Vorstellung der ersten IP500-Funkmodule (CNX100) in Produkten.

➔ **Ab 2014:** Erweiterung des Produkt-Portfolios bis hin zur EN-Pre-Konformität durch den VdS.

Heute hat der IP500-Standard führende Hersteller als Mitglieder mit Voting-Status. Nur sie sind berechtigt – eine Stimme pro Hersteller – die passenden Techniken (Funk, Netzwerk und Infrastruktur) auszuwählen, die den IP500-Standard zum gesteckten Ziel bringen.

Weltweit vertreten wird die IP500 Alliance in Japan, Indien, USA und Kolumbien von Repräsentanten mit lokaler technischer Unterstützung. Der Hauptsitz der IP 500 Alliance ist in Berlin.

Ausgewählte Partner und weltweit tätige Dienstleistungsunternehmen (Serviceanbieter) wurden als „None Voting Member“ aufgenommen und bilden das technische Rückgrat sowie unterstützen die Hersteller in technischen Fragen und der Lieferung der IP500-Funkmodule weltweit.

Um eine Interoperabilität der verschiedenen IP500-vernetzten OEM-Produkte zu garantieren hat die IP500 Alliance einen Zertifizierungsprozess etabliert.

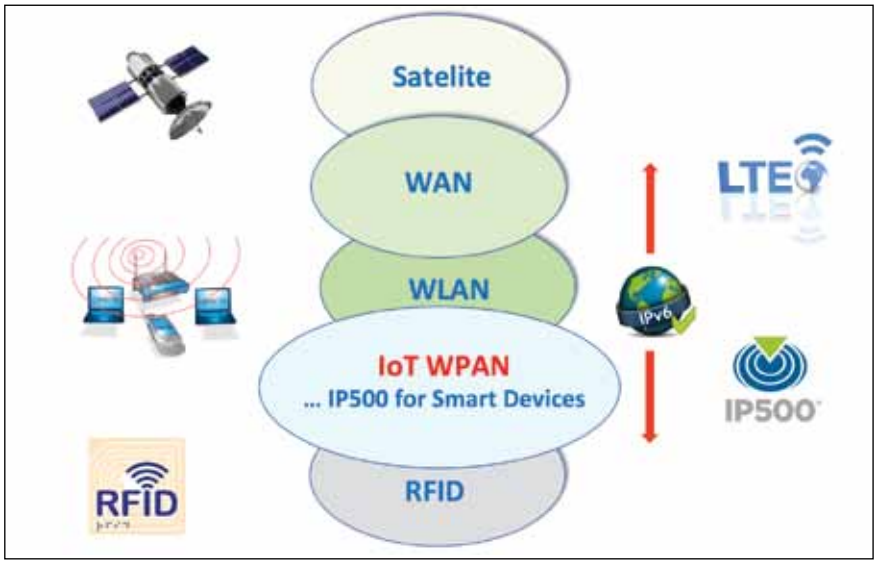


Bild 1. Die IP500 Alliance will den IP500-Standard als dominierende Infrastruktur für Wireless-IoT-Applikationen in kommerziellen Gebäuden etablieren. (Bild: IP500 Alliance)

mit den Netzwerk-Layern und der IoT-Infrastruktur in den Spezifikationen des IP500-Standards festgelegt. Diese Specs wurden dann von Partnern in Produkten umgesetzt, die heute erhältlich sind, z.B. Funkmodule (CNX200, **Bild 2**) und Gateways (GW260).

AUSDAUER UND STARKE PARTNER ZAHLEN SICH AUS

Durch eine enge Zusammenarbeit mit den Zertifizierungshäusern TÜV Rheinland und dem Verband der Sachversicherer (VdS) wurden bei der Entwicklung des IP500-Standards immer wieder die Systemsicht und wichtige Sicherheitsnormen im Fokus behalten. Das Resultat revolutioniert nun die IoT-Welt, mit höchster Robustheit, Skalierbarkeit und technischen Eigenschaften in der Funkkommunikation, in der Netzwerktechnik und in der Infrastruktur.

Unbeeindruckt von den bestehenden Wireless-IoT-Standards, die vor allem durch die Bottom-up-Strategie der IC- und Netzwerkhersteller entwickelt wurden, hat die IP500 Alliance mit Ihren Mitgliedern und Partnern die Wireless-IoT-Plattform IP500 aus Sicht der Systemebene geschaffen. Der IP500-Standard wurde mit den für die Systemebene entscheidenden Sicherheitsnormen in Einklang gebracht und durch die relevanten Zertifizierungshäuser, z.B. den VdS, manifestiert. Dadurch ist heute der IP500-Standard weltweit einzigartig und in der Lage, einen Wireless-IoT-Standard als Plattform zur Verfügung zu stellen, der gleichzeitig höchste Leistungsansprü-

Bild 2. Das IP500-Funkmodul CNX200 enthält einen Mikrocontroller für den IP500-Netzwerk-Stack und auch die Antenne. Es erfüllt alle Anforderungen für die weltweite Zertifizierung – für Europa (RED), Indien, Japan, USA (FCC) etc. (Bild: IP500 Alliance)

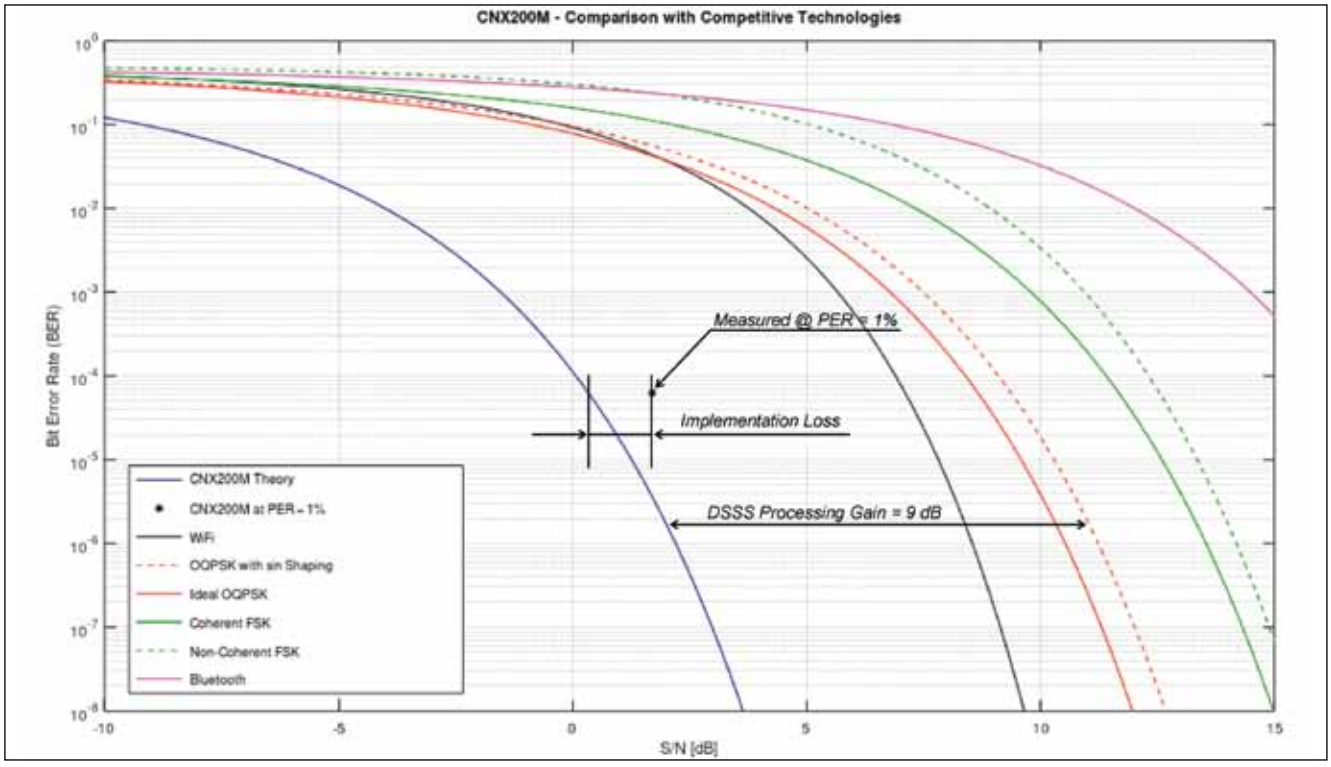


Bild 3. Im Vergleich der verschiedenen Funktechniken zeigt sich, dass IP500 durch den Einsatz von DNSS (Direct Spread Spectrum Sequence) – im 2,4-GHz-Band und bei 250 kbit/s gemessen – einen Prozessgewinn (Processing Gain) von 9 dB realisieren und mit kleinerem Signal-Rauschabstand (SNR) arbeiten kann. (Bild: IP500 Alliance)

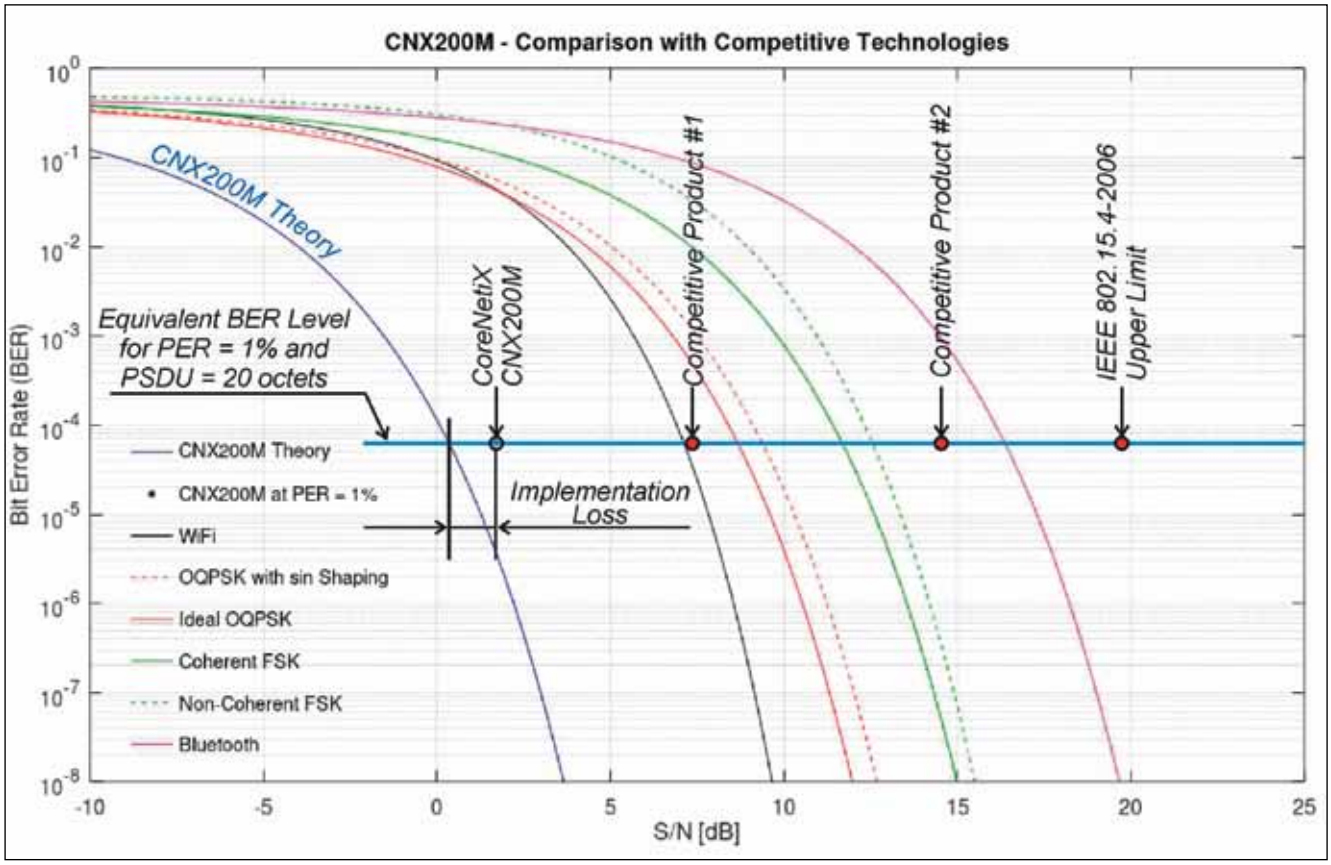


Bild 4. Vergleich der verschiedenen Funktechniken – theoretische Werte und Werte realer Implementierungen. Je weiter links eine Technik oder ein Produkt auf einer Waagerechten platziert werden kann, umso besser ist der Signal-Rauschabstand. (Bild: IP500 Alliance)

che im IoT-Netzwerk erfüllen kann und pre-konform zu europäischen Nomen ist, z.B. zu EN 50131-5-3 [2].

ANSPRÜCHE AN FUNKBASIERTE SICHERHEITS-APPLIKATIONEN

Von Beginn der Entwicklung an wurden im IP500-Standard die Anforderungen und Normen für die kritischen Applikationen in einem kommerziellen Gebäude – Zutrittskontrolle, Brandmelder etc. – in den Vordergrund gestellt. Gleichzeitig wurden die Best-in-Class-IoT-Techniken mit diesen Ansprüchen abgestimmt und in die IP500-Spezifikation eingebettet. Dieser Top-down-Prozess, aus dem Blickwinkel der Systemsicht, hat dazu geführt, dass der IP500-Standard garantiert auch den Ansprüchen der Zielanwendungen gerecht wird. Die Eckpfeiler dieser Anwendungen in kommerziellen Gebäuden sind:

➔ Höchste Robustheit der Funkverbindung im kommerziellen und industriellen Umfeld.
➔ Höchste Sicherheit in der Datenübertragung, inkl. Schlüsselverwaltung.
➔ Kurze Reaktionszeit (Latenz) zwischen Sensoren, Aktoren und der Infrastruktur (Gateways).

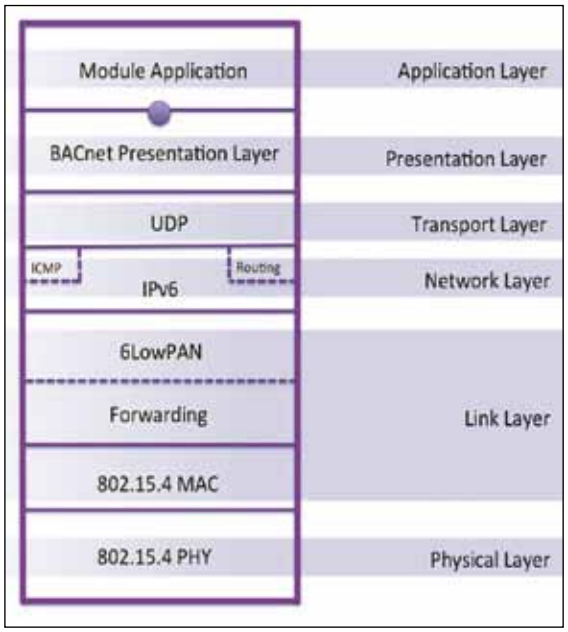


Bild 5. IP500 nutzt eine feinere Unterteilung der Sicherungsschicht (Data Link Layer) als das bekannte OSI-Modell. (Bild: IP500 Alliance)

➔ Hohe Datenrate und gleichzeitig eine hohe Funkreichweite.
➔ Skalierbare und robuste, vermaschte Netzwerkarchitektur (Mesh Topology).
➔ Energie- und Batterie-Management.
➔ Interoperabilität zwischen allen OEM-Produkten.
➔ Redundante Netzwerk-Topologie inklusive Gateways mit Datenbanken.

Die meisten Standardisierungsgremien für Wireless-IoT-Systeme haben aus der Sicht der HF-Transceiver-ICs begonnen, das heißt „Bottom up". Das bedeutet, die IC-Hersteller haben sich nach dem Standard IEEE 802.15.4 (x) gerichtet und die entsprechenden IoT-ICs entwickelt, so auch die Netzwerkhersteller die Softwareentwickler. Allerdings sind die Schichten zur Bit-Übertragung (PHY, Physical) und Sicherung (MAC, Media Access Control) im IEEE-Standard nur grob beschrieben – und sie haben keinerlei Bezug zur Applikation und deren Anforderungen.
Entwickler und Anwender müssen die gesetzlichen Vorgaben hinsichtlich der Frequenznutzung in den jeweiligen Ländern beachten und auch einhalten. Diese Regeln bergen aber enorme Herausforderungen für Wireless-IoT-Systeme. Betrachtet man beispielsweise den 2,4-GHz-Bereich, so ist dieser sehr belegt, vor allem durch Streaming-Applikationen mit WiFi und Bluetooth. Im Vergleich dazu bietet der Sub-GHz-Bereich nur schmale Kanäle und die nutzbaren Frequenzbänder sind von Region zu Region unterschiedlich.
Um diesen Herausforderungen zu begegnen, hat die IP500 Alliance ein Dual-Band-Verfahren spezifiziert, das im 2,4-GHz-Band hohe Datenraten bietet und im Sub-GHz-Bereich eine hohe Reichweite.
Durch das asynchron arbeitende, vermaschte Dual-Band-Netzwerk wurde eine zusätzliche Robustheit und Redundanz für die Übertragung von Sensordaten in einem sehr schwierigen Umfeld eingebaut. Die Datenpakete werden kryptographisch verschlüsselt, sodass der IP500-Standard Leistungsfähigkeit und Sicherheit in einem Wireless-IoT-Netzwerk kombiniert.

PRE-KONFORM NACH EUROPÄISCHEN NORMEN

Das VdS-Zeichen ist ein Gütesiegel und für Sicherheitsverantwortliche der wichtigste Qualitätshinweis bei der Entscheidung, Anschaffung, Integration und Installation von Sicherheitstechnik und Sicherheitsdienstleistungen – vor allem in kommerziellen Gebäuden. Organisiert im Verbund mit anderen europäischen Ländern, ist der Verband der Sachversicherer auch weltweit in seinem Wirkungskreis anerkannt. Durch ein VdS-Zertifikat werden sicherheitsrelevante Systeme zugelassen, nachdem sie auf Ihre Zuverlässigkeit, Ausfallsicherheit und mehr geprüft wurden. Ziel ist es durch den Einsatz der geprüften Techniken das Schadensrisiko zu mindern und letztendlich Schäden vorzeitig abzuwenden.
Die technischen Hürden sind enorm, um ein VdS-Zertifikat auf Produkt- und Systemebene zu erhalten. Ist ein Hersteller interessiert, ein Produkt mit einer Funkverbindung zertifizieren zu lassen, muss dieser Hersteller hohe Investitionen tätigen, um letztendlich seine proprietäre Funktechnik für sicherheitskritische Anwendungen zu entwickeln. Diese Funktechnik muss dann noch die Tests bestehen, was sehr langwierig sein kann. Dabei ist wichtig, dass die Rückwirkungsfreiheit auf die sicherheitstechnischen Anwendungen gegeben ist.
In jahrelanger Zusammenarbeit mit dem VdS ist es der IP500 Alliance gelungen, einen robusten und zuverlässigen Wireless-IoT-Standard in einem ersten Schritt der Pre-Konformität – nach der EN 50131-5-3 [2] – für einige wichtige Anwendungen als IoT-Plattform zu etablieren. Diese Pre-Konformität erlaubt es den Mitgliedern der IP500 Alliance, ihre Produkte, die mit einem IP500-Funkmodul (CNX200) ausgerüstet sind, ohne zusätzlichen Entwicklungsaufwand und sonstigen Pre-Konformitätstest zur VdS-Prüfung zu geben. Dadurch ergibt sich für den

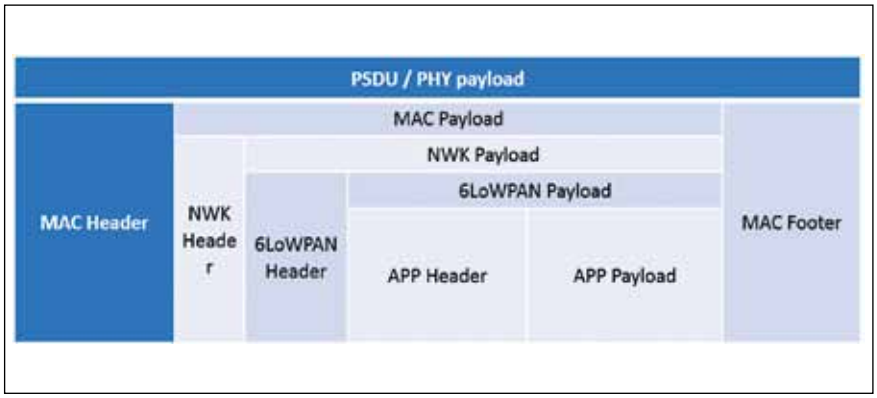


Bild 6. Die Applikationsdaten werden in den höheren Ebenen des IP500-Protokolls mehrfach in Pakete verschachtelt bevor sie per Funk ausgesendet werden. (Bild: IP500 Alliance)

MAC Header					MAC Payload	MAC Footer
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source Address	Nutzdaten	Prüfsumme
2 Byte	1 Byte	2 Byte	2 Byte	2 Byte	variabel	2 Byte

Bild 7. IP500 nutzt den MAC-Frame des IEEE-802.15.4-Standards (2006). (Bild: IP500 Alliance)

NWK Header						
Protocol ID	Header Length	Hop List	Payload Type	Payload Length	Sequence Number	CRC16
1 Byte	1 Byte	12 Byte	1 Byte	1 Byte	4 Byte	2 Byte

Bild 8. Der Kopf des Netzwerkdatenpakets bei IP500 (NWK Header) enthält die Information für das Routing (Hop List). (Bild: IP500 Alliance)

Hop List						
Type	Length	Destination	Source	Hop 1	Hop 2	Hop 3
1 Byte	1 Byte	2 Byte	2 Byte	2 Byte	2 Byte	2 Byte

Bild 9. Die Hop List gibt das Routing eines Funk-Datenpakets durch das IP500-Netzwerk vor. Sie wird vom Quellknoten erzeugt, indem er die kürzeste Verbindung zum Zielknoten berücksichtigt. (Bild: IP500 Alliance)

Hersteller eine erhebliche Ersparnis an Zeit und Kosten.

FUNKTECHNIK FÜR HÖCHSTE ANSPRÜCHE

Um allen Anforderungen gleichzeitig gerecht zu werden, sodass eine Konformität und Interoperabilität erreicht wird, haben die Mitglieder und Partner der IP500 Alliance das gesamte IP500-System auf allen drei Ebenen (Layer) aufeinander abgestimmt und entwickelt. Die drei Ebenen sind in dem Fall:
➔ Funkübertragung (PHY/MAC).
➔ Netzwerk-Stack und Applikation.
➔ Protokoll, Infrastruktur, Gateway und Datenbank.

Die beiden ersten Ebenen – Funkübertragung und Netzwerk-Stack – sind eng aufeinander abgestimmt und bilden eigentlich eine Einheit, wie das Beispiel der True-Dual-Band-Technik mit Mesh-Topologie zeigt. In dem Fall stellt die PHY-Ebene beide Frequenzen gleichzeitig bereit und die Netzwerk-Stack-Ebene routet die Datenpakete abhängig von der Interferenz in einem der Bänder automatisch im Mesh-Verfahren zum Zielknoten – ein Gateway oder ein Endgerät.

VORTEILE DES IP500-STANDARDS AUF DER FUNK-EBENE

Aufgrund der Anforderungen aus der Systemebene ist die Wahl auf die Modulation (OQPSK – Offset Quadrature Phase-Shift Keying) gefallen. Die Basis hierfür ist der IEEE-Standard 802.15.4 (2006), der OQSPK für höhere Datenraten im 2,4-GHz-Band vorsieht. Durch die Systemanforderungen der Sicherheitsapplikationen wurde dann die gleichzeitige Nutzung beider Bänder – Sub-GHz und 2,4 GHz – im IP500-Standard festgelegt. Damit entstand eine sehr hohe Robustheit gegen Interferenzen.
Kombiniert mit dem asynchronen Meshing-Verfahren des Netzwerk-Stacks können der IP500-PHY und -Netzwerk-Stack unterschiedlichen Interferenzen ausweichen – sowohl bei Störungen auf der Frequenzebene als auch bei Störungen auf dem Routing-Pfad.
Die Messergebnisse in **Bild 3 und 4**, in realem Umfeld mit hoher Interferenz gemessen, wie sie typisch für Gebäude, Tunnel oder metallische Umgebungen (Flugzeuge und Schiffe) sind, geben einen Einblick in die Robustheit des IP500-Standards gegenüber anderen Funk-Standards die weltweit eingesetzt werden.
Kleinere Zahlen beim Signal-Rauschabstand (Position des Produkts weiter links in Bild 4) sind aus mehreren Gründen vorteilhaft:
➔ Höhere Leistungsübertragungsbilanz (link budget).
➔ Bei gegebenem Signal-Rauschabstand (SNR) verringert sich die Anzahl von fehlerhaft empfangenen Bits. Zum Beispiel: für SNR = 4 dB sind die empfangenen Nachrichten des IP500-Funkmoduls CNX200M in der Praxis fehlerfrei. Eine Bitfehlerrate BER = 10^{-6} bedeutet ein fehlerhaftes Bit pro eine Million empfangener Bits. Im Vergleich dazu, für das gleiche SNR = 4 dB, beträgt die BER für WiFi = 0,01 – ein fehlerhaftes Bit pro 100 empfangene Bits. Unter solchen Bedingungen (SNR = 4 dB) sind Funkstandards wie WiFi, Bluetooth oder LoRa nicht praktisch zu nutzen.
➔ Reduzieren des Energiebedarfs – eine zuverlässige Übertragung benötigt bei kleinem SNR weniger HF-Sendeleistung.

Beim genauen Blick auf die Test-Resultate fällt auf, dass die bekannten Funk-Standards im kommerziellen oder industriellen Umfeld nicht umfänglich als Wireless-IoT-Plattform verwendbar sind, weil fehlende Leistung, Robustheit oder Sicherheit die IoT-Geschäftsprozesse empfindlich stören können.

DIE NETZWERK-EBENE DES IP500-STANDARDS

Die Ebene des IP500-Netzwerk-Stacks ist verantwortlich für die Topologie des Netzwerks, die Skalierbarkeit, die Latenz und die Verschlüsselung der Daten – und somit für die Robustheit und Sicherheit im gesamten IP500-Netzwerk.
Den IP500-Aufbau nach dem bekannten OSI-Modell zeigt **Bild 5**. Entsprechend dem IEEE-802.15.4-Standard wurde das asynchrone Übertragungsverfahren gewählt. In **Bild 6** ist der Aufbau ei-

nes vollständigen IP500-Funk-Datenpakets dargestellt. Das MAC-Datenpaket entspricht den Vorgaben des IEEE-802.15.4-Standards (**Bild 7**). **Bild 8** zeigt, wie sich bei IP500 der Kopf des Netzwerk-Datenpakets zusammensetzt. Die Hauptfunktionen des Netzwerks sind:

➔ Aufbau der Datenpakete (Frames) und Dateiköpfe (Header).

➔ Weiterleitung der Pakete durch das asynchron arbeitende vermaschte Netzwerk mithilfe der Routing-Tabelle.

➔ Sicherung und Verschlüsselung der Datenpakete.

ROUTING PER HOP LIST

Im NWK Header (Bild 8) definiert die „Hop List“, eine vorgegebene Route durch das Netzwerk (**Bild 9**). Die Nachricht von der Applikation wird organisiert in das Paket geschrieben und entsprechend der Hop List durch das Netzwerk geleitet – im Dual-Band und über die Vermittlungsknoten des vermaschten Netzwerkes. Die Hop List liefert den nächsten Hop durch das asynchron arbeitende vermaschte Netzwerk mit minimalem Rechenaufwand – eine wichtige Fähigkeit, die für geringe Latenz und einen niedrigen Energiebedarf der einzelnen Netzwerkknoten (Sensoren) sorgt. Der eine Nachricht aussendende Knoten bestimmt die Hop List für das Datenpaket aus seiner Routing-Tabelle, indem er die kürzeste Route bildet. Dieses Verfahren bieten dem Endanwender ein selbstheilendes, sich selbst konfigurierendes vermaschtes Netzwerk mit geringster Latenz.

Alle Nachrichten der IP500-Applikationsschicht werden in beiden Richtungen zwischen den Knoten und dem Gateway gesendet, deshalb kennt jeder Knoten und das Gateway die Route ohne Rechenaufwand, und die zuletzt eingetroffenen Nachrichten werden zudem im Gateway gespeichert. Die Verwendung von alternativen Routen im vermaschten Netzwerk sichert somit gemeinsam mit der Redundanz auf der Frequenzebene hohe Zuverlässigkeit und geringe Latenzzeiten beim Auftreten von Interferenzen, was als Grundlage für die Pre-Konformität zu den Europäischen Normen [2] durch den VdS bestätigt wurde **(Bild 10)**.

SICHERHEIT UND VERSCHLÜSSELUNG IM IP500-NETZWERK

Die Berechnung des AES128-Schlüssels zum symmetrischen Ver- und Entschlüsseln der Nachricht basiert auf der Sequenznummer der Nachricht und einem Master-Schlüssel, der durch ein asymmetrisches ECDH-Verfahren (Elliptic-Curve Diffie–Hellman) zwischen jedem einzelnen Knoten und dem Gateway abhörsicher berechnet wird. Durch eine Ende-zu-Ende-Verschlüsselung ist sichergestellt, dass die Nachrichten durch weiterleitende Knoten nicht abgehört oder gefälscht werden können. Eine einmalige Verwendung des AES128-Schlüssels für eine einzige Nachricht erhöht sie Sicherheit des IP500-Netzwerks. HS

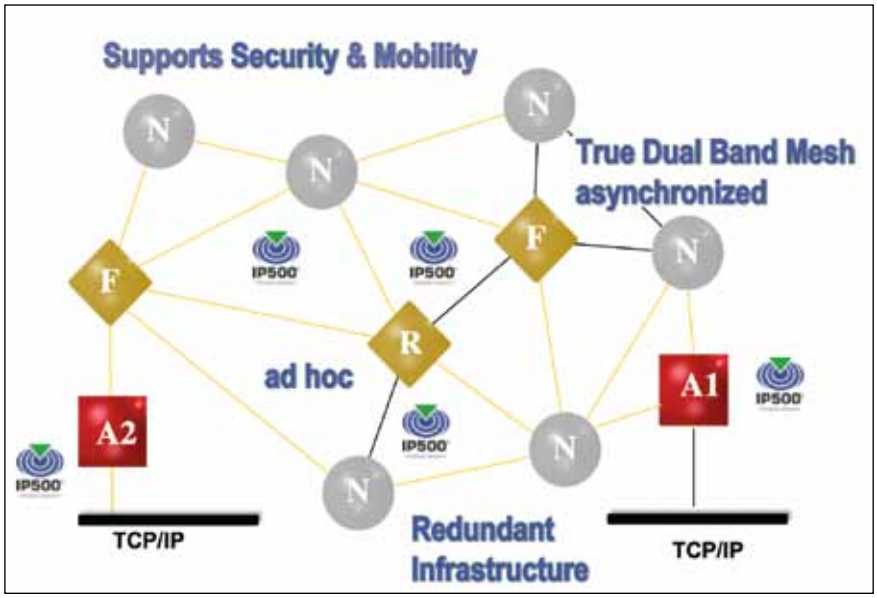


Bild 10. Das IP500-Netzwerk bietet Sicherheit, Zuverlässigkeit und Robustheit durch Redundanz – mit zwei Gateways und dem Betrieb in zwei unabhängigen Frequenzbändern. (Bild: IP500 Alliance)

Literatur

[1] IP500 Alliance, www.ip500alliance.org

[2] DIN EN 50131-5-3:2017-09; VDE 0830-2-5-3:2017-09: Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 5-3: Anforderungen an Übertragungsgeräte, die Funkfrequenz-Techniken verwenden; Deutsche Fassung EN 50131-5-3:2017.

HELMUT ADAMSKI

ist ein IoT-Pionier und führt derzeit als CEO und Vorsitzender die IP500 Alliance e.V. Er verfügt über mehr als 25 Jahre Erfahrung in der High-Tech-Industrie, mit Schwerpunkt auf IoT- und IT-Netzwerkanwendungen, Funk-ICs sowie Sicherheitsanwendungen für Gebäude und Betriebsstätten.

Adamski hat einen Ingenieurabschluss in Elektronik und besuchte Executive-/MBA-Programme am Institute of Excellence, San Diego, und der Stanford University, Kalifornien, USA.

helmut.adamski@ip500alliance.org

WITALI GISBRECHT

Ist Spezialist für die Entwicklung von Embedded Software für Netzwerk-Stacks, Sicherheit-Methoden und Gateway-Architekturen. Er schloss sein Informatik-Studium an der Universität Paderborn 2007 mit dem Abschluss Bachelor of Science ab.