Abschlussbericht: AETERNITAS

Einzelvorhaben: Vereinigung von energieefizienten Hauptknoten und sicherem Wakeup-System zu hochintegrierten Sensorknoten

Zuwendungsempfänger: IHP GmbH

Förderkennzeichen: 16 BN 1110

Laufzeit: 1.10.2011 - 31.3.2015

Inhalt

1 Kurze Darstellung ... 2
1.1 Aufgabenstellung ... 2
1.2 Voraussetzungen für das Projekt ... 2
1.3 Planung und Ablauf ... 3
1.4 Wissenschaftlich/technischer Stand zu Projektbeginn ... 4
1.5 Zusammenarbeit mit anderen Stellen ... 4
2 Eingehende Darstellung ... 5
2.1 Untersuchung innovativer Wakeup-Verfahren ... 5
2.1.1 Systemkonzept, integrierte Filter, analoge Kernschaltungen ... 5
2.1.2 Optimierung von SiGe Komponenten ... 13
2.1.3 RF- und IF-Filter ... 16
2.1.4 Innovative Wakeup-Verfahren auf Basis von SAW Resonatoren ... 18
2.2 Sicherer Wake-Up Receiver für drahtlose Sensorknoten ... 21
2.2.1 Hardware-Plattform für die Entwicklung eines sicheren WakeUp-Empfängers ... 21
2.2.2 Authentifizierungsverfahren für einen WakeUp-Empfänger ... 25
2.2.3 Evaluierung des sicheren Wake-Up Receivers als Software-Lösung ... 30
2.2.4 Integration des sicheren Wake-Up Receivers in den IHPstack als Demonstrator ... 35
2.3 Zusammenfassung und Anschlussfähigkeit der Resultate ... 38
2.4 Aus dem Projekt hervorgegangene Publikationen und Patente ... 40
2.5 Referenzen ... 40

1 Kurze Darstellung

1.1 Aufgabenstellung

Das Ziel von AETERNITAS war, aufbauend auf bisherigen Lösungen für Wakeup-Radios die noch offenen Herausforderungen zu bearbeiten, welche einer weiten Verbreitung dieser Technologie im Wege stehen. Insbesondere basiert das Projekt auf dem zu Projektbeginn verfügbaren Wakeup-Empfänger des Fraunhofer IIS in Erlangen. Als spezielle Ziele für das Gesamtprojekt wurden festgelegt: eine Reichweite von 500m, eine 6-Bit Adressierung um Knoten selektiv aufzuwecken, und einen Energieverbrauch von maximal 10 µW. Die Arbeitsteilung innerhalb des Projektes sah vor, dass das Fraunhofer IIS und die Technische Universität Dresden die Weiterentwicklung des zu Projektbeginn vorliegenden IIS-Systems im Fokus haben. Das IHP untersuchte alternative und innovative Technologien für Wakeup-Empfänger, welche von einem Einsatz weiter entfernt sind, aber das Potential für leistungstärkere und energiesparsame Wakeup(WU)-Systeme haben. Als weitere Hauptaufgabe sollte das IHP eine Absicherung von Wakeup-Systemen entwickeln und implementieren. Die Anforderungen für diesen „secure wakeup“ wurden vom Projektpartner EADS/Airbus formuliert. Sie ergeben sich daraus, dass im Flugverkehr alle Systeme aus gutem Grund gegen unerlaubte externe Eingriffe geschütz weden müssen. Als dritten Aufgabenbereich sollte das im Projekt enstandene Wakeup-System in eine Sensorplatform des IHP, dem TANDEM Stapel, integriert werden und in einem Multi-Hop-Sensornetz demonstriet werden. Viertens hat das IHP die Projektkoordinerung übernommen und die Partner bei der Herstellung der Testchips im IHP Reinraum unterstützt.

Zusammengefasst hatte das IHP folgende Aufgaben im Projekt:

1. Die Untersuchungen innovativen Maßnahmen für Wakeup-Empfänger
2. Die Entwicklung und Implementierung eines secure Wakeup
3. Integration des WU-Systems im TANDEM Stapel mit dem Ziel Multi-Hop Netzwerk
4. Die Projektkoordinierung und Unterstützung der Partner bei der Chipherstellung.

1.2 Voraussetzungen für das Projekt

Zu Beginn des Projektes lag bereits ein funktionierendes WU-System von Fraunhofer IIS vor, welches von IIS und TU Dresden weiter entwickelt wurde. Wichtige Voraussetzung hierfür war die IHP-eigenen Prozesslinie mit 0,25/0,13-µm-SiGe-BiCMOS-Technologien. Insbesondere war dies die Voraussetzung für die Forschungen an der TU Dresden, den Vorteil von SiGe Transistoren im WU-Empfängers zu untersuchen. Das IHP verfügte bereits zu Projektbeginn über ausführliche Erfahrungen in verschiedenen Bereichen, welche als Voraussetzung für das Teilprojekt von Bedeutung waren:

- Die Arbeitsgruppe „Ultra-Low Power“ arbeitet an energieeffizienten Sende- und Empfangsschaltungen für drahtlose Sensornetzwerke. Hier wurden z.B. spezielle UWB Impulsradio Chipsätze entwickelt.
- Im Zusammenhang mit dem Vorläuferprojekt „Nanett“ wurden Technologien für energieeffiziente Sensorknoten erarbeitet, insbesondere zum „Energy Harvesting“, zur Energiespeicherung, zu MEMS-basierter WakeUp-Empfänger und zu Netzwerktopologien.

- Das IHP verfügt über eine eigene Plattform zur Entwicklung und Erprobung von Sensorknoten, dem TANDEM Stapel. Diese hat sich in diversen früheren Projekten bewährt. Die modulare TANDEM-Architektur als Stapel von kompakten Einzelplatinen macht es möglich, Neuentwicklungen in ein bestehendes System effizient einzubauen.
- In der Systemabteilung verfügt das IHP über ein erhebliches Know-How zur Sicherheit in Drahtlosen Sensornetzen. Unter anderem wurden Crypto-Blöcke zu SHA1, AES, und ECC in Hardware entwickelt und in Projektanwendungen erfolgreich eingesetzt.

1.3 Planung und Ablauf

Der Ablauf des Teilprojektes am IHP entsprach im Wesentlichen der Projektplanung. Es gab einige Verschiebungen, welche sich im Lauf der Arbeiten als notwendig oder wünschenswert ergaben.

Erstens gab es eine Verzögerung auf Grund einer Havarie im Reinraum (Ausfall eines Gerätes mit längerer Reparaturzeit) welche die Auslieferung einer Chipserie um einige Wochen verschob. Dadurch konnte der ursprüngliche AETERNITAS-Projektplan nicht eingehalten werden und es wurde eine kostenneutrale Verlängerung um 6 Monate beantragt. Die betroffenen Chips waren Prototypen für das weiterentwickelte IIS System, also Aufträge vom IIS und der TU Dresden. Das IHP war isofern betroffen, als diese Chips in den Demonstrator des Multi-Hop Sensornetzes eingebaut wurden. Die engültigen Chips lagen trotz Projektverlängerung erst recht kurz vor Projektende vor und die Demonstration des Sensornetzes konnte nicht im geplanten Umfang erreicht werden.

Ein Fokus des IHP war die Untersuchung von innovativer alternativer Wakeup-Technologien. Es ergaben sich einige Bereiche, welche weniger erfolgreich waren und andere, welche hinzu gekommen sind. Der angedachte Einsatz nicht-gestresster SiGe-HBTs zur Erzielung höherer Verstärkungsfaktoren in LNAs war nicht erfolgreich. Ebenfalls wurde die Idee nicht weiter verfolgt, in die Si Technologie integrierte SAW Komponenen einzusetzen, da die technischen Parameter unzureichend waren. Als neue und innovative Lösung für Wakeup-Empfängern kam hinzu, einen externen SAW Resonator als Akkumulator für die Energie der eingehenden Radiowelle und damit als passiven Verstärker einzusetzen. Dieses führte zu zwei Patenten wahrend des Projektes.

In der Projektbeantragung wurde davon ausgegangen, dass das IHP die Integration des WU-Systems in den IHP-eigenen Sensorknoten mittels einem ASIC durchführen würde. In der ersten Phase des Projektes wuchs die Entwicklung des secure wakeup zu einem unerwartet wichtigen Schwerpunkt an. Dies lag zum Teil an der erfolgreichen Zusammenarbeit mit Airbus, wodurch konkrete Vorstellungen für ein abgesichertes WU-System frühzeitig verfügbar wurden. Die Analyse der einsetzbaren Sicherheitsmechanismen ergab, dass eine Implementierung im ASIC ungünstig war, da die Algorithmen kompliziert sind und eine Erprobung auf einem FPGA die bessere Lösung ist. Insbesondere können verschiedene algorithmische Varianten verglichen werden und das Risiko einer fehlerhafter oder nicht-optimaler Hardeware wird weitgehend vermieden. Daher wurde statt eines ASICs eine neue FPGA-Ebene für den TANDEM Stapel entwickelt und in Betrieb genommen. Auf diesem System wurde der secure wakeup erfolgreich implementiert und dessen Funktion verifiziert.

1.4 Wissenschaftlich/technischer Stand zu Projektbeginn

Der zu Projektanfang vorliegende WU-Empfänger des Fraunhofer IIS, welcher Basis von AETERNITAS war, hatte eine Empfindlichkeit von -60 dBm, womit eine Reichweite von etwa 30 m möglich ist. Dieser Entfernung reicht für die meisten praktischen Anwendungen nicht aus. Der Energieverbrauch bewegte sich zwischen etwa 10 µW und 300 µW, je nach benötigter Datenrate. Dadurch ergibt sich auch die Latenz, welche bei der sparsamsten Konfiguration etwa 0.5 Sekunden beträgt. Die Situation war also, dass Latenz und Energieverbrauch bereits plausible Werte hatten, dass die Reichweite (also die Empfindlichkeit) erheblich verbessert werden sollte. Dabei ist das Hauptproblem nicht die höhere Empfindlichkeit an sich, sondern dass der Energieverbrauch bei dieser Verbesserung nicht wesentlich ansteigen darf. Die Suche nach alternativen Lösungen für WU-Empfänger ergab eine muntere Landschaft, da viele Forschungsgruppen an der Frage arbeiten. Dabei sind manche der angebotenen System schwer vergleichbar, falls sie beispielsweise eine höhere Datenrate bei höherem Energieverbrauch anstreben. Als Endresultat war die Situation, dass kein verfügbares System die im Projektantrag formulierten Zielparameter erfüllt, und dass das IIS System bei Erhöhung der Reichweite ein starker Kandidat für den praktischen Einsatz ist.

Für die Untersuchungen am IHP waren diese Angaben vor allem als Benchmark signifikant. Ein alternatives WU-System unter Verwendung innovativer Komponenten ist nur dann von Bedeutung, wenn die Eckwerte des IIS Empfängers verbessert werden können. Die Forschungen ergaben, dass Lösungen auf Basis eines Superregenerativempfängers sowie auf Basis der SAW-Resonatoren als passive Verstärker dieses Potential haben. Desweiteren legen die Werte die Anforderungen an das Sicherheitssystem (secure wakeup) fest. Bei den Arbeiten am IHP wurde das secure wakeup System gezielt so entwickelt, dass es mit dem IIS Wakeup-Empfänger kompatibel ist. Dieses bezieht sich auf die Datenrate, auf die Schnitstelle zum WU-Radio, und vor allem auf den Energieverbrauch. Mit einer geeigneten Hardware/Software Partitionierung konnte erreicht werden, dass die Sicherheitskomponenten die Anforderungen von Airbus erfüllen bei nur minimalem zusätzlichem Energieverbrauch gegenüber dem WU-Empfänger selbst.

1.5 Zusammenarbeit mit anderen Stellen

Die Zusammenarbeit des IHP innerhalb des Projektes ist wie folgt zu charakterisieren:

- IIS: Unterstützung seitens des IHP bei der Herstellung Chip-Prototypen, Hilfestellung des IIS bei den Untersuchungen alternativer Lösungen
- TUD: Unterstützung bei der Herstellung von Chips und Zusammenarbeit im SiGe Bereich
- Advico: Spezifikation des WU-Systems, Arbeiten am 868 MHz Radio
- Lesswire: Zusammenarbeit bei der Entwicklung der Demonstratoren
- Airbus: Spezifikation und Anforderungsanalyse für secure wakeup, gemeinsame Bewertung der resultierenden Komponenten

Dazu kam die fortlaufende Zusammenarbeit im Rahmen der Projektkoordinierung.

Zusätzlich wurde das Paul-Drude Institut in Berlin als Unterauftragsnehmer hinzu gezogen. Das Institut hat Protoytypen für innovative SAW Komponenten entworfen, herstellen lassen, und expeimentell bewertet.

2 Eingehende Darstellung

In diesem Teil des Berichtes werden die wissenschaftlich-technischen Egebnisse des Projektes ausführlicher dargestellt.

2.1 Untersuchung innovativer Wake-Up-Verfahren

2.1.1 Systemkonzept, integrierte Filter, analoge Kernschaltungen

Im Rahmen von UAP 3.2 wurden in der Projektlaufzeit analoge Kernschaltungen von Wake-up-Receivern (WuRx) entworfen und untersucht. Insbesondere stand die Minimierung der Leistungsaufnahme im Dauerbetrieb im Designfokus. Um Aussagen zum Einfluß des Technologieniveaus auf die Leistungsparameter zu gewinnen, wurden diese Schaltungen sowohl in der IHP-BiCMOS-Technologie SGB25V (0,25 µm) als auch in SG13S (0,13 µm) realisiert. Insbesondere rauscharme Vorverstärker (LNA) und Hüllkurvendetektoren (Envelopdetektor) standen im Mittelpunkt der Arbeiten. Einen weiteren Schwerpunkt stellt die Integration von Induktivitäten dar. Aus diesem Grund wurden die LNAs für die beiden Frequenzbänder bei 868 MHz und 2,4 GHz jeweils in beiden Technologien hergestellt. Die Bilder 1 und 2 zeigen die Layouts dieser Schaltungen.

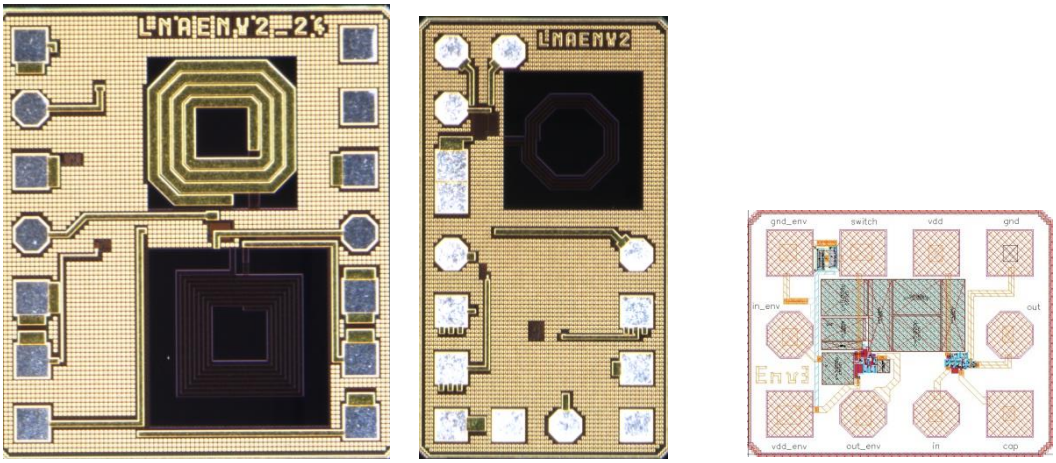


Bild 1: LNA und Envelopdetektoren für 868 MHz und 2,4 GHz in SGB25V

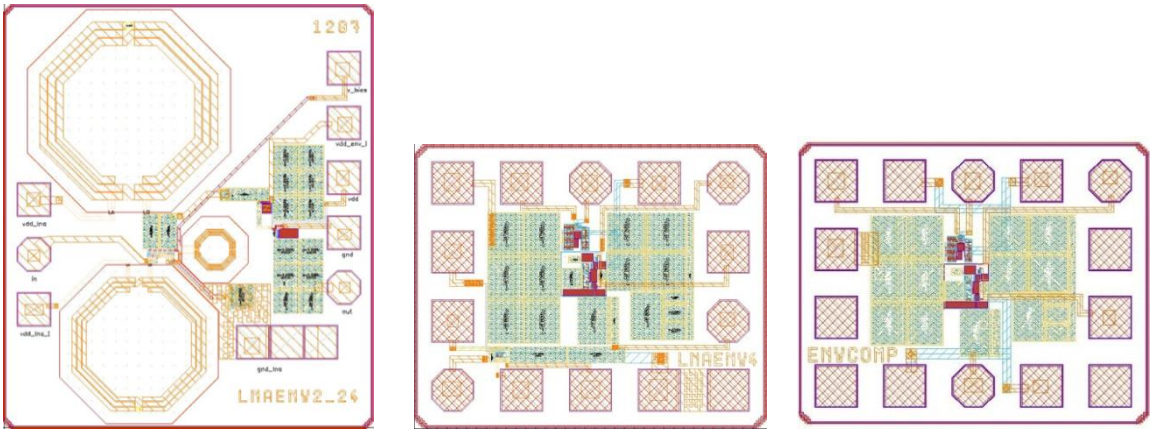
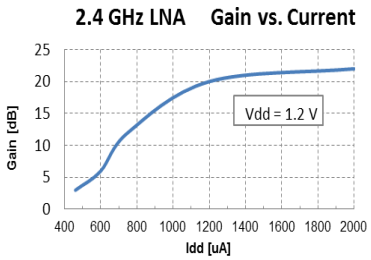
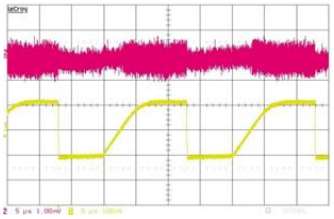


Bild 2: Schaltungsversionen in SG13S

In Bild 3 sind wesentliche Messergebnisse des 2,4-GHz-LNAs in der 0,25 µm IHP-Technologie dargestellt.





	V_{dd} = 1.2 V
I_{dd} [µA] LNA	700
Gain [dB]	10
Center frequency [GHz]	2,28
I_{dd} [µA] ENV	7
I_{dd} [µA] Driver	9
Sensitivity [dBm]	< - 50

Bild 3: Messergebnisse des 2,4-GHz-LNA

Parallel zu den Schaltungsentwürfen wurde der Stand der Technik zu Wake-up-Receivern ermittelt und analysiert. Bild 4 zeigt eine Übersicht international realisierter WuRx-Schaltungen (Stand Sept. 2012). Es stellt den Zusammenhang zwischen Empfängerempfindlichkeit und dem dafür aufzuwendendem Leistungsverbrauch dar. Die durchgezogene Linie gibt den Trend des derzeitig technisch Realisierbaren wider. Die Punkte 19 bis 21 zeigen die Einordnung der am IHP entworfenen Schaltungen. Bei Punkt 19 handelt es sich um die zuvor erwähnte Schaltung. Punkte 20 und 21 beziehen sich auf Simulationsergebnisse. Im Rahmen einer Dissertation wurde von Airbus zum Projektabschluss eine umfangreichere und weiter gefächerte Analyse des Standes der Technik 2014 erarbeitet.

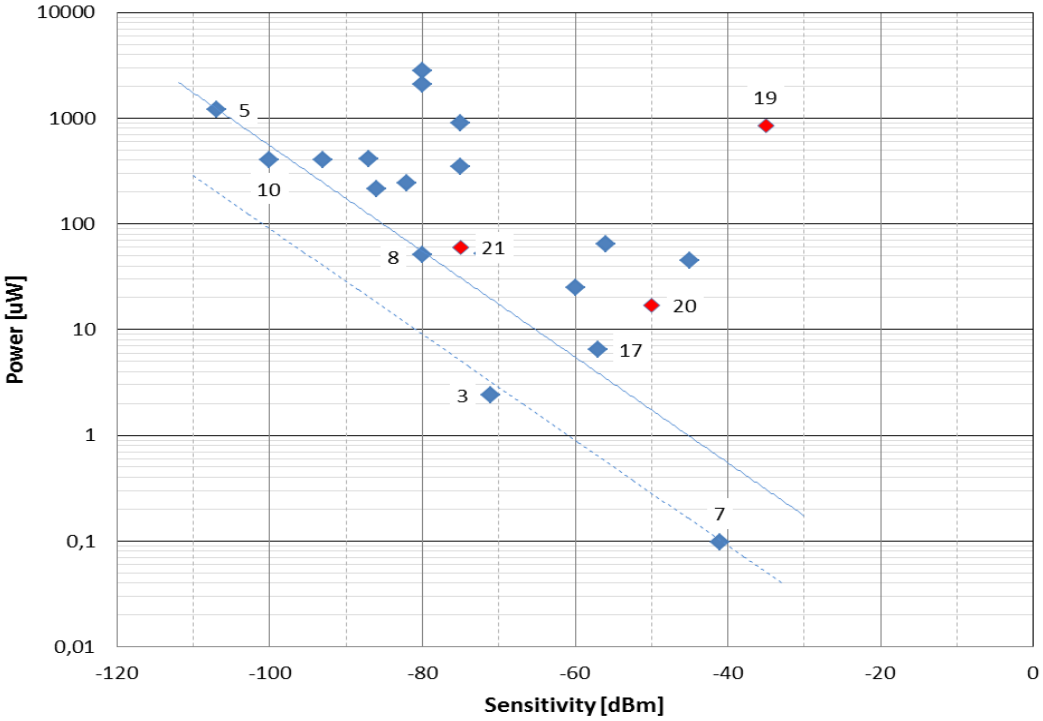
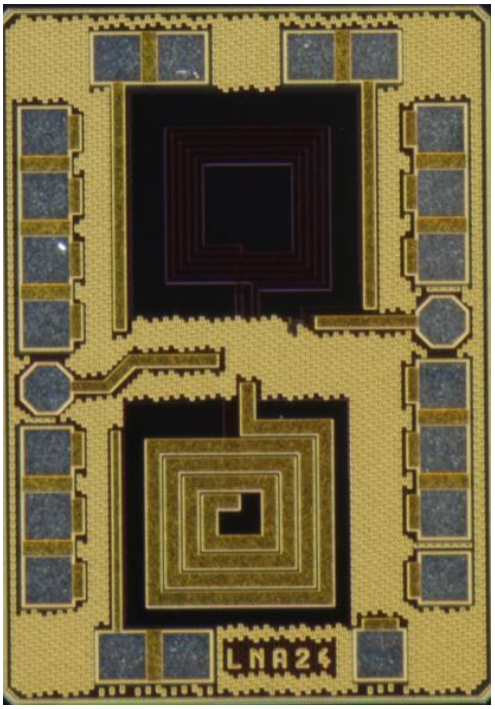
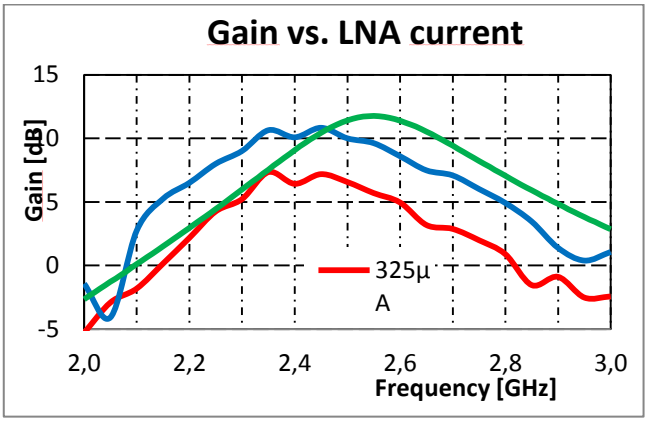


Bild 4: Stand der Technik 2012 zu Wakeup-Receivern

In 2013 wurden die Arbeiten zu analogen Kernschaltungen von Wake-up-Receivern (WuRx) fortgeführt. Zum einen entstanden weitere Schaltungen, um die Vergleichsmatrix zu Technologien, Schaltungstechnik und Frequenzband zu erweitern. Erste Schaltungen wurden gemessen.

Bild 5 zeigt einen rauscharmen Vorverstärker für den 2,4-GHz-Bereich mit integrierten Induktivitäten im Ein- und Ausgangskreis. Zur besseren Evaluierung im 50-Ohm-Messsystem wurde ein Messverstärker implementiert. Den Vergleich von gemessenen und simulierten Parametern zeigen die Bilder 6 und 7.





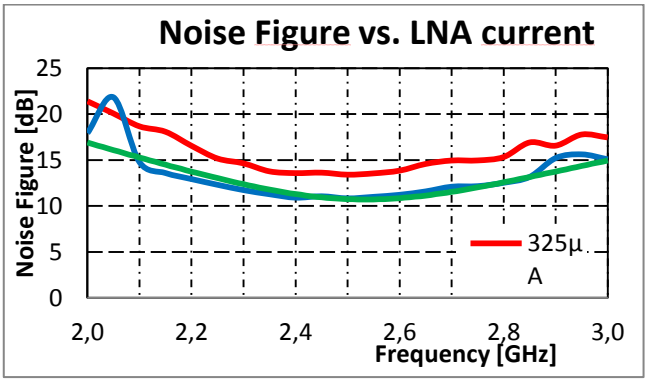


Bild 5: Chipfoto des 2,4-GHz-LNAs

Bilder 6 und 7: Messwerte des LNAs

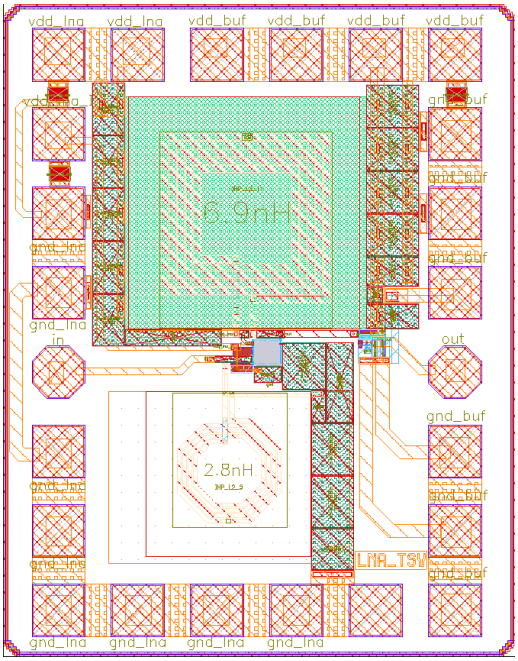
Die Ursachen für die um etwa 5 dB geringeren Verstärkungswerte und damit auch des entsprechend schlechteren Rauschverhaltens bei gleichem LNA-Strom sind in der kleineren Güte der integrierten Spule als auch im nicht ausreichend gelungenen Eingangsmatching auf der Leiterplatte zu begründen.

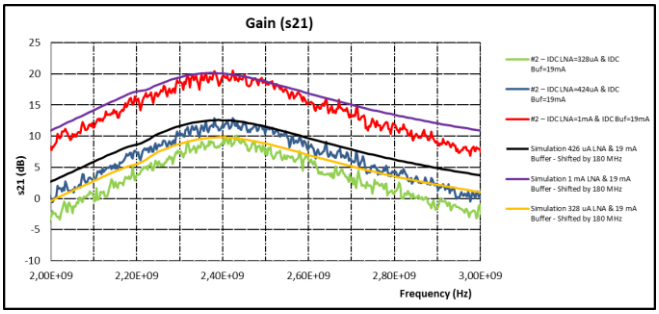
Aus den Untersuchungen zum Stand der Technik von Wake-Up-Receivern und weiterführenden Analysen anhand eigener, realisierter und gemessener Kernschaltungen solcher Empfänger werden Reichweite und Leistungsverbrauch im Wesentlichen durch die Empfindlichkeit des Envelopdetektor

und die Verstärkung des LNA bestimmt. Beim Envelopdetektor ist die physikalische Grenze auf Grund der quadratischen Kennlinie des Gleichrichters nahezu erreicht. Eine Steigerung der Empfindlichkeit um 20 dB bedingt eine um etwa 1 Dekade gesteigerte Stromaufnahme des LNA. Somit scheiden die bisher bewährten Konzepte solcher Schaltungen im Dauerbetrieb unter Maßgabe eines geringen Leistungsverbrauchs aus.

Die Arbeiten an der Variantenmatrix von rauscharmen Verstärkern (LNA) bei 2,5 GHz und Envelopdetektoren mit geringstem Stromverbrauch wurden im Jahr 2014 zum Abschluß gebracht.

Bild 8 zeigt einen 2,4-GHz-LNA mit integrierten Induktivitäten im Ein- und Ausgangskreis. Wie auch schon früher wurde zur besseren Evaluierung im 50-Ohm-Messsystem ein Messverstärker implementiert. Den Vergleich von gemessenen und simulierten Parametern zeigen die Bilder 9 und Tabelle 1. Bei den Simulationskurven wurden die unterschiedlichen Grade der Modellierung und deren Einfluss auf das Ergebnis dokumentiert. Es lässt sich leicht erkennen, dass eine möglichst genaue Modellierung mittels EM-Simulation den erreichten Messwerten näher kommt als die sonst übliche Modellierung mit den nur vom Designkit angebotenen Modellen. Für schmalbandige Anwendungen ist es unerlässlich, einen erhöhten Modellierungsaufwand zu betreiben und oft auch notwendig, sowohl den Eingangs- als auch den Ausgangskreis justierbar/abstimmbar zu gestalten.





Parameter	Simulation	Messung
I_{DC} LNA (µA	416	424
I_{DC} Buffer (mA	19	19
S_{11} (dB)	-22	-10.6
S_{21} (dB)	12	11.2
NF (dB)	10.9	11.3

Bild 8: Chipfoto des 2,4-GHz-LNAs

Bild 9 und Tabelle 1: Simulations- und Messwerte

Neben LNAs sind Envelopdetektoren und Komparatoren weitere Kernschaltungen von Low-Power-WuRx. Es wurden drei Versionen Envelopdetektoren entwickelt, aufgebaut und evaluiert (s. Bild 10). Die Ergebnisse sind in Tabelle 2 dargestellt. Während der Unter-suchungen in Wakeup-Receivern stellt sich heraus, dass die Envelopdetektoren auch noch sehr kleine Eingangssignale verarbeiten, die folgenden Komparatoren jedoch durch ihre physikalisch und technologisch bedingte Schaltschwelle die maximale Empfindlichkeit begrenzen. Um hier noch bessere Werte zu erreichen, ist eine vorhergehende Verstärkung des Ausgangssignals des Envelopdetektors notwendig.

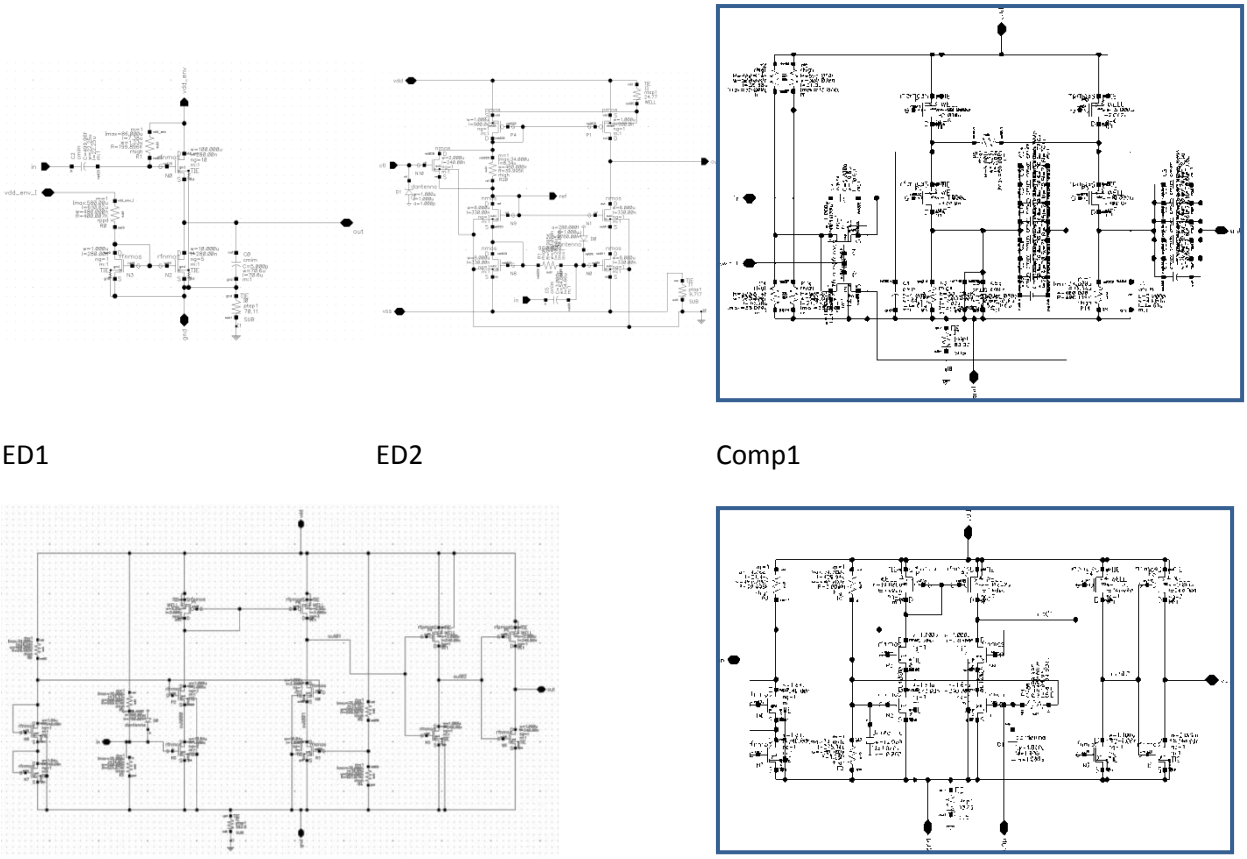


Bild 10: Envelopdetektor- und Komparatoren-Varianten

	ED 1	ED 2	ED 3
V_{DD}	1.5 V	3.5 V	1.5 V
I_{DD}	30 µA	12 µA	30 µA
Sensitivity Messung. Simulation	 -30 dBm -40 dBm	 -17 dBm -24 dBm	 -29 dBm -46 dBm

Tabelle 2: Ergebnisse der Envelopdetektoren

Neben dem Betrieb von Wake-Up-Systemen im Duty-Cycle-Modus (s. andere Projektpartner) ergibt sich ein vielversprechender, alternativer Ansatz mit dem Superregenerativempfänger. Durch seinen periodischen Betrieb kommt er auch einem geringen Leistungsverbrauch entgegen. Empfindlichkeiten von besser -100 dBm werden in der Literatur berichtet (Ref. 1 bis 3). Problematisch ist hingegen die zuverlässige Einstellung sicherer Arbeitspunkte und damit an dieser Stelle ein notwendiger Mehraufwand an Schaltungstechnik. Zur Untersuchung der Realisierbarkeit solch eines Superregenerativempfängers (SRR) im WuRx wurden gegen Mitte des Berichtszeitraumes zwei wesentliche Kernschaltungen entwickelt und eingesteuert. Zum ersten wurde ein Frontend bestehend aus LNA, LC-Oszillator und Envelopdetektor entworfen. Alle Schaltungsteile wurden so gestaltet, dass bei der Evaluation wichtige Einflußgrößen wie Ströme, Zeitverhalten und Frequenz extern beeinflusst werden können und somit das Verhalten der Schaltungen möglichst umfassend untersucht werden kann. Bild 11 zeigt das Blockschaltbild des realisierten Superregenerativempfängers. Tabelle 3 präsentiert Simulationsergebnisse und Bild 12 das Layout. In Bild 13 werden die verschiedenen Signale innerhalb des Frontends dargestellt.

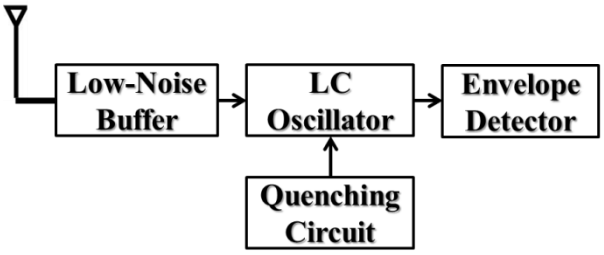


Bild 11: Blockschaltbild des SRR-Frontends

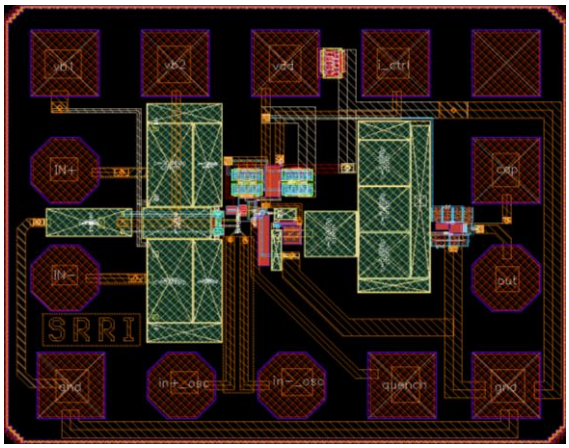


Bild 12: Layout des SRR-Frontends

Parameter	Wert
Supply voltage [V]	1.5
Quench current [µA]	10.5
LNB current [nA]	60
Center frequ. [MHz]	868
Chip area [mm²]	0,06

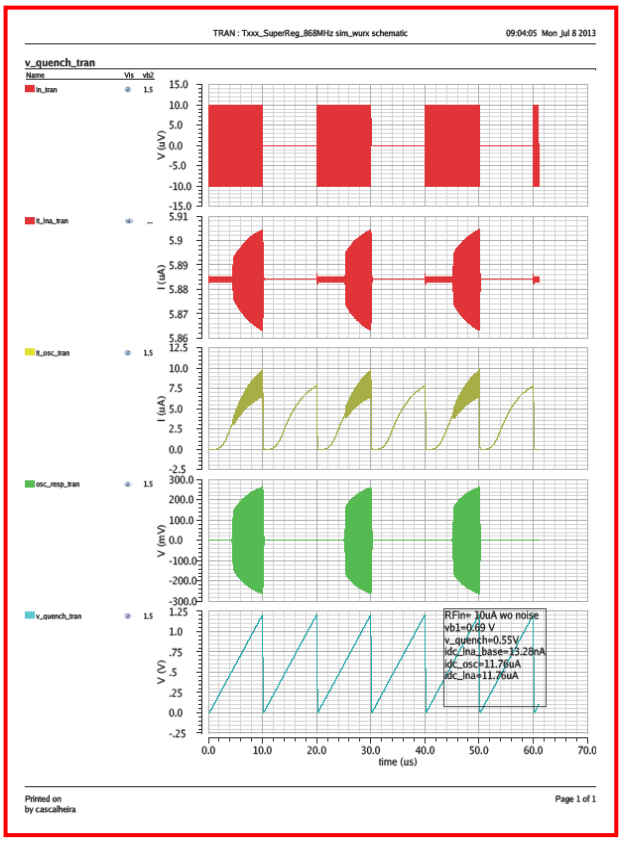


Tabelle 3: Simulationsparameter

Bild 13 Typische Signale im SRR-Frontend

Anfang 2014 begann die Evaluierung der Schaltungen zum Superregenerativempfänger. Die prinzipielle Funktionsweise der Schaltungen konnte nachgewiesen werden. Die simulierten Parameter wurden nur teilweise erreicht. Aufgrund der Arbeit der Schaltung am Schwingeinsatz waren Manipulationen an den Arbeitspunkten während der Messungen sehr diffizil und hatten oft nicht den erhofften Erfolg. Die Untersuchungen zeigen, dass die zu überwindenden Herausforderungen bei der Umsetzung dieses Konzeptes beträchtlich sind und wir uns hier noch in der Anfangsphase befinden. Bis zum Projektende war eine Umsetzung neuer Ideen zur Konsolidierung des Ansatzes zeitlich nicht mehr möglich.

Weitere, für die Funktion des Superregenerativempfängers wichtige Schaltungen betreffen die Einstellung optimaler Arbeitspunkte unter Low-Power-Bedingungen. Zu diesem Zweck wurde eine zweite Schaltung zur Generierung einer Referenzspannung entwickelt. Sie liefert eine stabile Ausgangsspannung von etwa 400 mV über einen weiten Betriebsspannungs- und Temperaturbereich und ist damit auch für den Einsatz mit Spannungen von 1,0 V und kleiner geeignet. Bild 14 zeigt das Layout. Tabelle 4 listet die simulierten und gemessenen Parameter auf. Die gemessenen Abhängigkeiten von Betriebsspannung und Umgebungstemperatur sind in den Bildern 15 und 16 dargestellt.

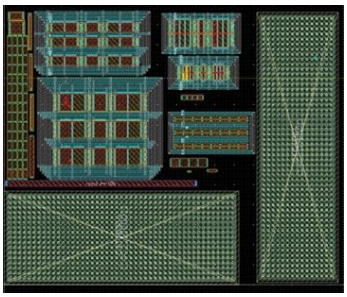
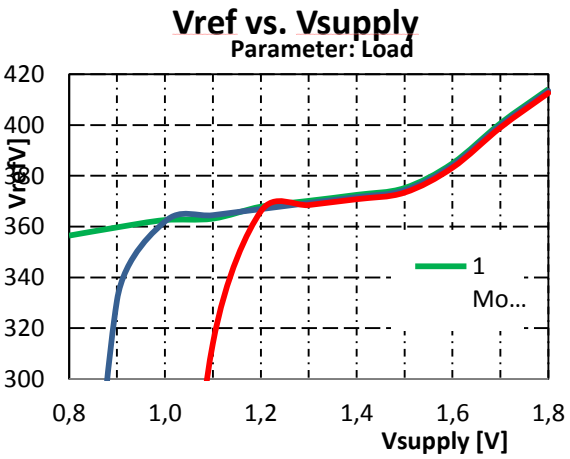


Bild 14: Layout der Low-Power-Referenz

Parameter	Gemessen	Simu-liert	Bedingunggen
Output voltage [mV]	368	436	V_{DD} = 1.2 V, ϑ = 25 °C, R_L = 1 MΩ
Output voltage variation [%]	1.8 20	± 2.6	0 °C < ϑ < 100 °C, V_{DD} = 1.2 V 0.8 V < V_{DD} < 1.8 V
Power supply rejection ratio [dB]	40	40	V_{DD}= 1.2 V, AC: 200 mV_{PP} @25 kHz
Supply current I_{DD} [nA]	480 14	400	V_{DD} = 1.2 V, ϑ = 25 °C, R_L = 1 MΩ V_{DD} = 1.2 V, ϑ = 25 °C, R_L = ∞

Tabelle 4: Messwerte der Spannungsreferenz



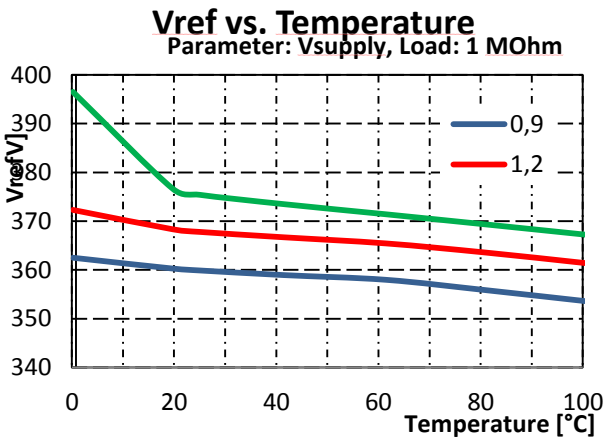


Bild 15: Betriebsspannungsabhängigkeit **Bild 16: Temperaturverhalten**

Die Arbeiten zu den Referenzquellen wurden in der Folge um Stromquellen und integrierte Spannungsregler erweitert. Ein weiteres Design für eine Spannungsreferenz wurde ebenfalls entworfen (s. Bild 17). Die Evaluierungen dieser Schaltungen fallen außerhalb des Projektzeitraumes.

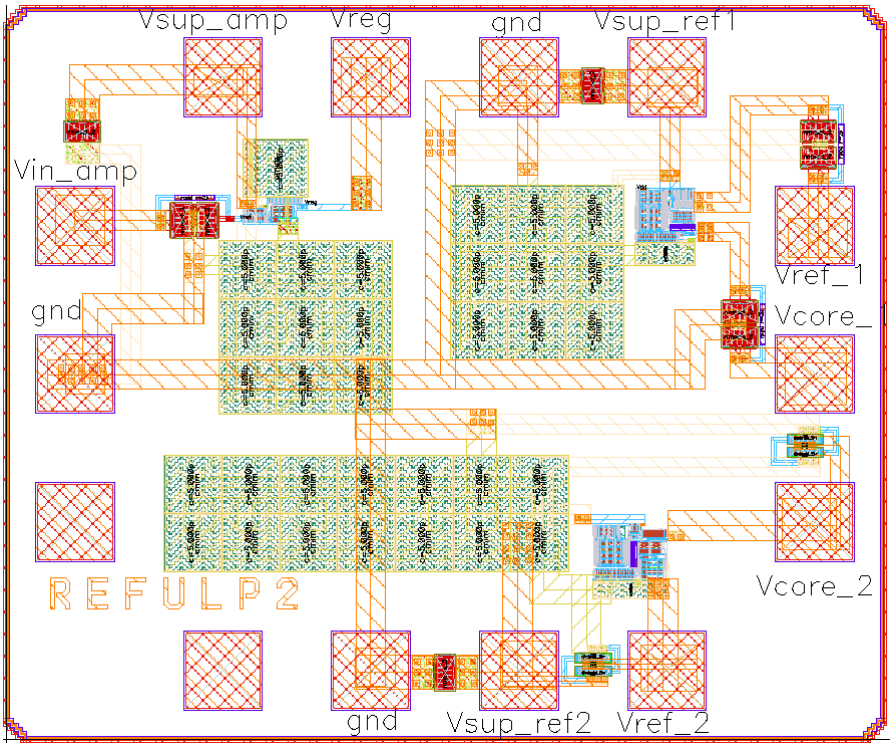


Bild 17: Layout der Low-Power-Referenzen der 2. Generation

2.1.2 Optimierung von SiGe Komponenten

Im UAP 3.3 war u. a. die These zu untersuchen, ob „ungestresste“ SiGe-Transistoren (HBT) beim Einsatz in Low-Power-Schaltungen Vorteile bringen. Nach ausgiebigen Diskussionen mit den Baulelementephysikern des IHP und Auswertungen von Messungen an gestressten HBTs wurde eine Verschlechterung der Transistorparameter nach erfolgtem Stress bestätigt. Der für eine Degradierung der Transistorkennwerte maßgebliche Stress tritt jedoch bei Anwendungen wie WuRx nicht in Erscheinung. Somit kann der Effekt einer nachträglichen „Heilung“ nicht vorbeugend genutzt werden.

Da der Ansatz zu „gestressten“ HBTs für Low-Power-WuRx nicht weiter ausbaufähig ist, wurde in 2013 entschieden, diese Arbeiten einzustellen und stattdessen die Potenziale des SiGe-HBT bei sehr kleinen Strömen und moderaten Frequenzen zu untersuchen. Es wurden mehrere Testschaltungen entworfen und evaluiert. Tabelle 5 und Bild 19 illustrieren die erreichten Ergebnisse eines 868-MHz-LNAs.

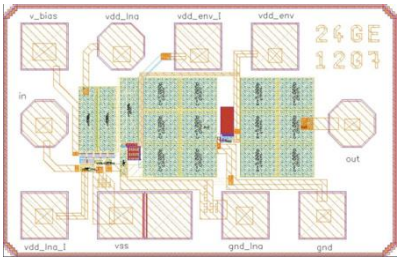


Bild 18: Layout eines SiGe-LNA

Parameter	Wert	Bedingungen
Supply current [µA]	40 … 1300	V_{CC} = 1.5 V
Gain range [dB]	0 … 25	0.8 V < V_{DD} < 1.8 V
Center frequency [MHz]	868	
S11 [dB]	-27	I_{CC} = 180 µA @ 1,5V
S21 [dB]	18	I_{CC} = 180 µA @ 1,5V
1 dB compression point [dBm]	-21	I_{CC} = 180 µA @ 1,5V
3rd order intercept point [dBm]	13	I_{CC} = 180 µA @ 1,5V
Noise figure [dB]	9	I_{CC} = 180 µA @ 1,5V

Tabelle 5: Messwerte des SiGe-LNAs

Als eine wesentliche und bedeutende Erkenntnis dieser Untersuchungen ist die Tatsache hervorzuheben, dass gleiche dynamische Parameter bei etwa 30 % weniger Leistungs-verbrauch gegenüber einer gleichwertigen Lösung in reiner CMOS-Schaltungstechnik erreicht werden.

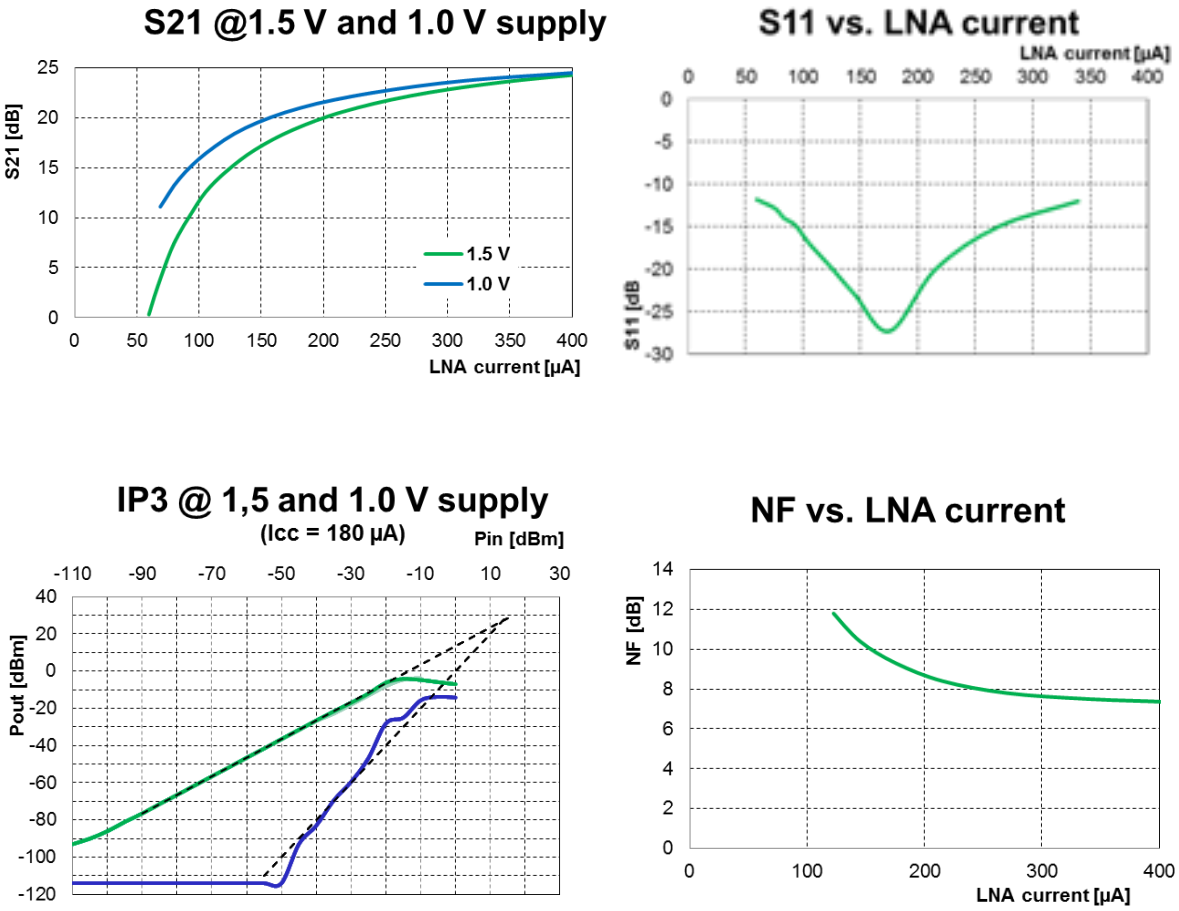


Bild 19: Dynamische Messwerte des 868-MHz-SiGe-LNAs

Die Untersuchungen zum Einsatz des SiGe-HBT wurden 2014 vervollständigt. Die Ergebnisse der Variantenmatrix sind in den Entwurf eines Low-Power-WuRx eingegangen. Ein aufgebauter Demonstrator reagiert auf OOK-modulierte Aufweck-Signale. Tabelle 6 zeigt die hiermit erreichten Kennwerte, Bild 20 den Demonstratoraufbau.

Parameter	Wert
Power consumption [µW]	600
Center frequency [GHz]	2.4
Noise Figure [dB]	12
Sensitivity @ 390 µA SiGe LNA [dBm]	-57

Tabelle 6: Kennwerte WuRx-Demonstrator **Bild 20: WuRx-Demonstrator**

2.1.3 RF- und IF-Filter

Neben SAW- und MEMS-Strukturen stellen Spulen hoher Güte ein weiteres Mittel zur Verbesserung der Schaltungseigenschaften dar. Bei gleichem oder geringerem Stromverbrauch lassen sich so höhere Verstärkungen realisieren. Seit einiger Zeit besteht am IHP die Möglichkeit durch Einsatz eines selektiven Rückseitenätzens (LBE) die Substratdicke unterhalb integrierter Strukturen (u. a. auch Spulen) soweit zu reduzieren, dass die Substratverluste verringert werden und damit insbesondere bei integrierten Spulen die Güte deutlich erhöht wird. Um dies zu untersuchen wurden Testschaltungen (LNAs) mit integrierten Spulen entworfen. Die Berechnungen ergeben eine Verdoppelung der Güte der Spulen bei 2,4 GHz und somit eine Verdopplung der Verstärkung bei gleichem Strom oder umgekehrt.

2013 wurde ein Doppelchip mit zwei identischen LNAs entworfen und in der SG13S-Technologie des IHP produziert (s. Bild 21). Der Unterschied zwischen beiden LNAs besteht nur darin, dass eine Schaltung unterhalb der die Verstärkung bestimmenden Spule ein LBE-Fenster erhält. Somit lassen sich direkte Vergleiche anstellen und Aussagen zur Praxistauglichkeit der LBE-Option treffen.

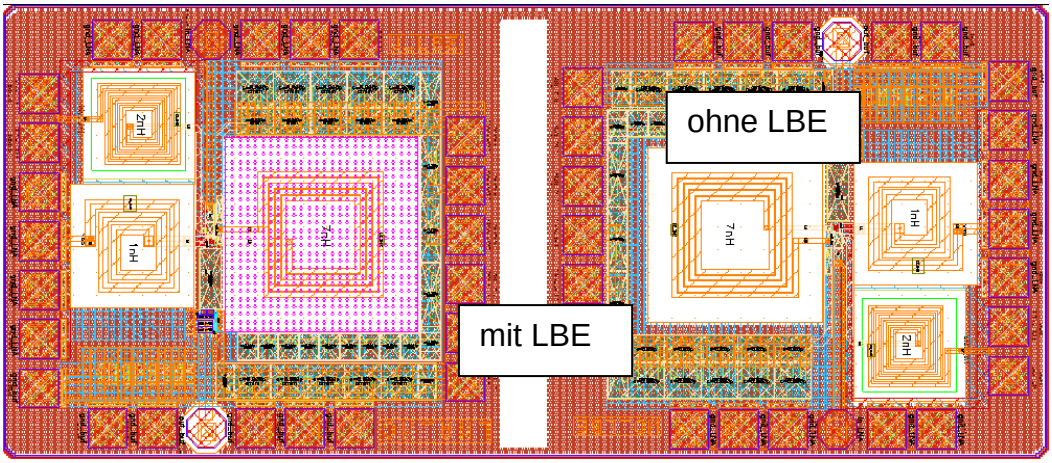


Bild 21: Layout des LBE-LNA-Doppelchips

Durch einen Layoutfehler in einer der eigens entworfenen Induktivitäten konnte auch nach einem Reparaturversuch kein zufrieden stellender Messaufbau realisiert werden. Deshalb gab es ein Redesign in 2014. Leider konnte auch an diesem Chip der Vorteil höherer Güten mittels LBE nicht demonstriert werden. Die Fehleranalyse ergab, dass das LBE-Fenster deutlich weiter ausgefallen ist und somit die aktiven Strukturen (CMOS- und HBT-Transistoren) sowohl von LNA als auch Nachverstärkerstufe zerstört wurden. Somit waren keine vergleichenden Messungen möglich. Fehleranalyse und Schlussfolgerungen für den IHP-Prozessschritt liegen jenseits des Zeitrahmens des Projektes.

Als Konsequenz aus der Vergleichsmatrix wurde ein 2,4-GHz-LNA mit abstimmbaren Ein- und Ausgangskreisen entworfen und in der SG13S-Technologie des IHP prozessiert (s. Bild 21). Tabelle 7 zeigt die Messwerte der realisierten Schaltung. Die Bilder 23 und 24 zeigen anschaulich die Abgleichbereiche von Ein- und Ausgangskreis. Trotz Einbeziehung parasitärer Effekte mittels EM-Simulation konnte die Mittenfrequenz nicht getroffen werden. Ein Redesign außerhalb des Projektes wird dies korrigieren

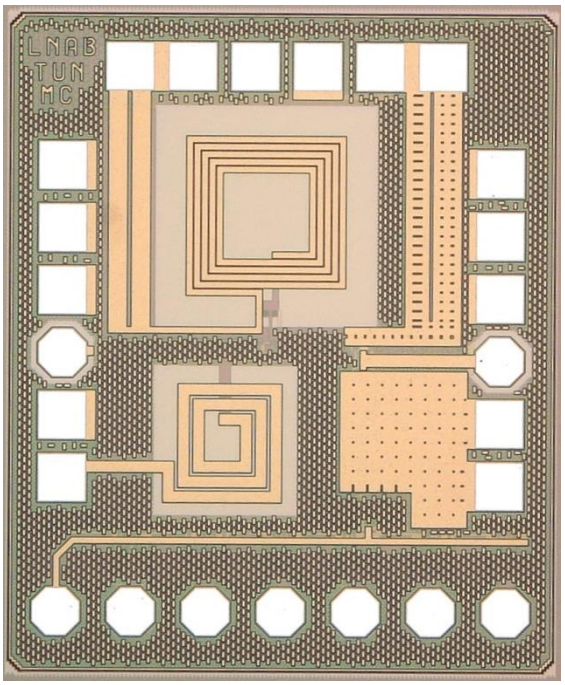


Bild 22: Chipfoto des abgleichbaren 2,4-GHz-LNAs

	Parameter	Gemessen	Simuliert	Bedingungen
LNA	Gain @200 µA [dB]	14	15	@ 250 µA
	Center frequency [GHz]	2.37	2.45	
	LC tank tuning range [GHz]	2.2 … 2.38	2.33 … 2.54	
	Input matching range [GHz]	2.27 … 2.36	2.3 … 2.6	
	S11 [dB]	-22		@ 250 µA
	IIP3 [dBm]	-9		@ 250 µA
	NF [dB]	12	15	@ 250 µA
Buffe-	Supply current [µA]	12	20	@ 3V
SPI	Supply current [µA]	65	60	@ 1.2 V
DAC	Supply current [µA]	1.6	1.6	@ 2.5 V

Tabelle 7: Vergleich der berechneten und gemessenen Parameter

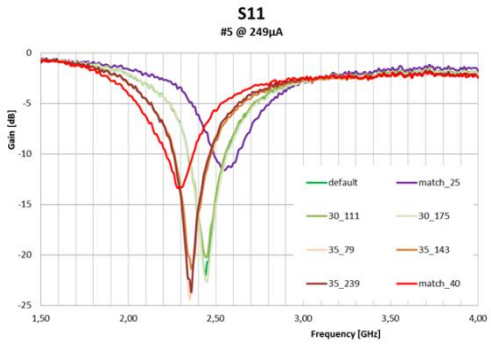


Bild 23: Abgleichbereich von S11

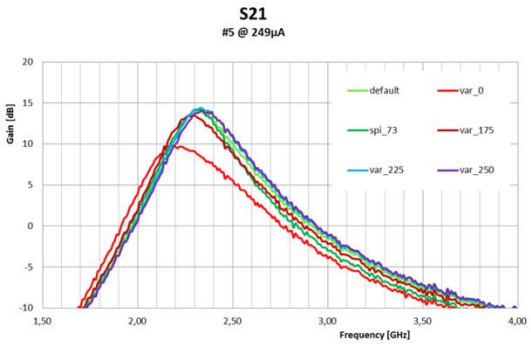


Bild 24: Abgleichbereich von S21

2.1.4 Innovative Wakeup-Verfahren auf Basis von SAW Resonatoren

Entsprechend dem Projektplan wurde untersucht, ob SAW Komponenten für einen Wakeup-Empfänger innerhalb der Si Technologie implementiert werden können. Eine solche Möglichkeit sind SAW Korrelatoren, die das Aufwecksignal in der HF-Domäne korrelieren. Die besondere Herausforderung sind hier Fragen der Technologie, insbesondere der Insertion Loss (Inband-Dämpfung). SAW Devices, welche als Standardbaulemente auf speziellen piezzoelektrischen Substraten gefertigt werden (z.B. Lithiumniobat) habe eine sehr gute Qulität. Die Untersuchungen zu integrierten SAW Komponenten ergaben zwar die prizipielle Möglichkeit, aber die notwendigen Parameterwerte können nicht erreicht werden. Zum Beispiel klingt die Oberflächenwelle wegen der höheren Verluste im Schichtsystem auf dem Si-Substrat zu schnell ab, um noch einen geeigneten Korrelator zu verwirklichen.

Im Zusammenhang mit diesen Überlegungen ergab sich jedoch ein neuartiger SAW-basierter Zugang, welcher recht vielversprechend scheint. Dieser wurde im Projekt auch weiter verfolgt. Die Grundidee ist, einen externen SAW Resonator mit hoher Güte für eine Zeitdauer von einigen Mikrosekunden vom Antennensignal „aufzuladen“ um danach eine Spannungsspitze in einem parallelen Schwingkreis zu erzeugen. Durch diese passive Verstärkung kann das Signal soweit angehoben werden können, dass die Überwindung der quadratischen Diodenkennlinie ohne einen vorgeschalteten LNA möglich ist. Dieses ist von Bedeutung, da der LNA als erste Verstärkerstufe für die Identifikation eines Wakeup-Signales eine entscheidende Rolle spielt, aber auch einen großen Teil der Gesamtenergie verbraucht.

Das SAW-basierte Verfahren wurde mittels eines einfachen ASICs mit einem geeigneten Schalttransistors erprobt und die grundsätzliche Funktion verifiziert. Analyse der gemessenen Resultate (eine Anhebung um einen Faktor von etwa 10) und der Vergleich zu Simulationen ergaben, dass eine deutliche Verbesserung durch ein weiterentwickeltes System möglich sein sollte. Laut Simulationen könnte ein optimales System Ziel eine Anhebung von etwa 20 erreichen. Bild 25 zeigt die Testplatine mit dem ASIC Chip in der Mitte und dem kommerziellen SAW Resonator im unteren Teil. Das Ausgangssignal bei optimaler Einstellung ist in Bild 26 dargestellt. Ein Vorteil einer solchen Lösung wäre, dass die benötigte Filterung auf ein schmales Empfangsband automatisch durch die Eigenschaften des SAW Resonators gegeben ist. Das Konzept führte zu einem Patent während der Projektlaufzeit.

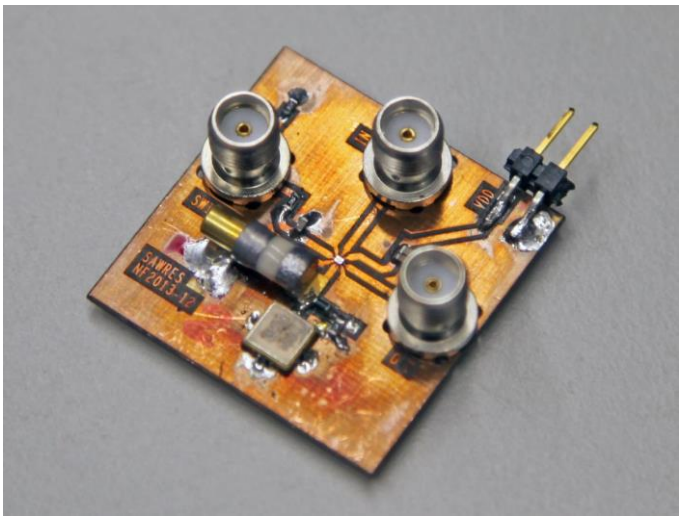


Bild 25: Testplatine für die erste Erprobung eines SAW Resonators als passiver Verstärker

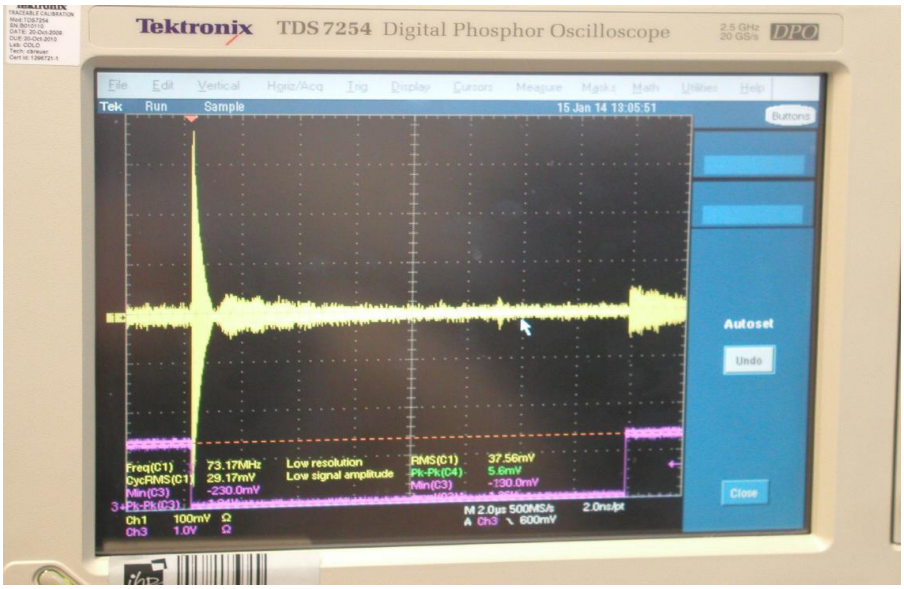


Bild 26: beobachtete passive SAW Verstärkung um einen Faktor von etwa 10

Als Weiterentwicklung wurde das Konzept untersucht, den gepulsten SAW Resonator mit einem Superregenerativempfänger zu kombinieren. Der Vorteil hierbei ist, dass der anschwingende Oszillator im Empfänger einfach gehalten werden kann und deshalb stromsparsam ist. Üblicherweise darf der Oszillator nur sehr schmalbandig in dem relevanten Frequenzband schwingen, um die geforderte Frequenzselektivität des Empfängers zu erreichen. Bekannte Schaltungen stabilisieren beispielsweise die Oszillatorfrequenz mit SAW Filtern oder Resonatoren, aber dieses führt zu einem besonders hohen Energieverbrauch. Wenn dagegen der Initialpuls zum Anschwingen aus dem vorgeschalteten SAW Resonator kommt, wurde die Filterung im Frequenzband bereits von diesem durchgeführt und die natürliche Frequenz des Oszillators ist weitgehend irrelevant. Es wurde eine solche Schaltung entwickelt, dessen zentrale Einheit in Bild 26 dargestellt ist. Die beiden Blöcke auf der linken Seite stellen das einfachere SAW System dar, nämlich den SAW Resonator welcher über

einen NMOS Schalttransistor zeitweilig an die Antenne angeschlossen ist. Wenn der aufgeladene Resonator von der Antenne getrennt wird, entsteht ein Puls, welcher den nachfolgenden Oszillator anstößt. Da der Resonator nur die Energie in seinem Resonanzband akummulieren kann, erhält man einen Puls, dessen Größe proportional zum eingehenden Wakeup-Signal während der Aufladezeit ist. Der Oszillator ist eine sehr einfache Hartley-Schaltung, welche extrem wenig Energie benötigt. Bis zum Projektende wurde ein Empfänger mit der Schaltung as Bild 27 und einer nachfolgender Gleichrichtung mit Schwellendetektion entworfen und als ASIC hergestellt (Bild 28). Simulationen sagen voraus, dass diese Schaltung als Wakeup-Empfänger deutlich weniger Energie verbraucht als die ISS Version. Das System wurde als weiteres Patent angemeldet.

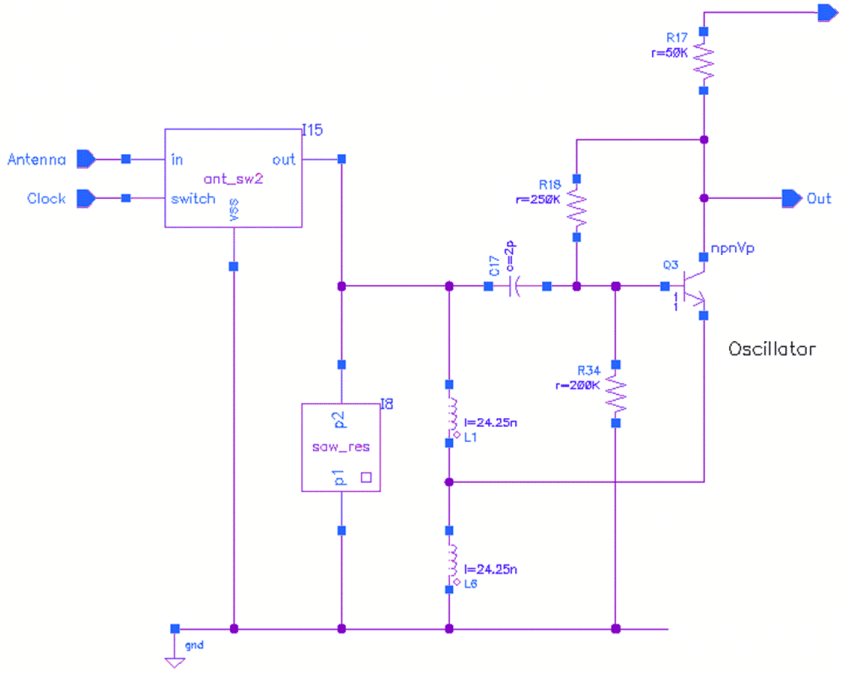


Bild 27: Gepulsten SAW Resonator mit nachfolgendem Superregenerativempfänger.

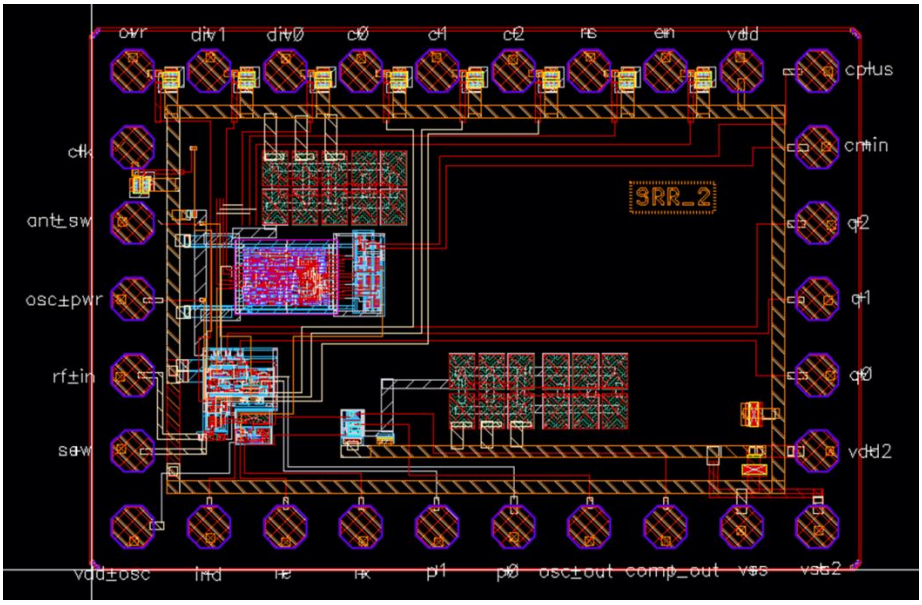


Bild 28: Layout eines Empfängers nach dem Prinzip von Bild 26

2.2 Sicherer Wake-Up Receiver für drahtlose Sensorknoten

Die Verwendung von Wake-Up Receiver in drahtlosen Sensornetzwerken ermöglicht es die Lücke zwischen Energieverbrauch und Reaktivität zu schließen. In klassischen Netzwerken werden zum Verringern des Energieverbrauchs alle Komponenten des Sensorknotens deaktiviert. Erst wenn der Knoten eine Aktion ausführen oder Daten zu versenden hat, werden die notwendigen Komponenten reaktiviert. In der Phase, wenn alle Komponenten deaktiviert sind, kann der Knoten allerdings auch keine Daten empfangen.

Insbesondere in Multi-Hop Netzwerken in denen einen Knoten sowohl Datenquelle als auch Zwischensystem ist, führt das zeitweise Deaktivieren des Knotens zu zahlreichen Problemen. Durch den Einsatz von Duty-Cycle-Protokollen, bei denen ein gemeinsamer Rendezvous-Zeitpunkt zwischen den Knoten ausgehandelt wird, lassen sich die Probleme teilweise lösen. Jedoch sind diese Protokoll sehr starr, da ein Knoten einen Rendezvous-Zeitpunkt abwarten muss, bevor er mit benachbarten Knoten kommunizieren kann. Damit ist eine asynchrone Datenübertragung nicht möglich.

Durch den Einsatz eines Wake-Up Receivers, der einen minimalen Energieverbrauch bei ständiger Empfangsbereitschaft bereitstellt, lassen sich die bisherigen weitestgehend Probleme umgehen. Allerdings sind Wake-Up Receiver sehr anfällig für sogenannte Depletion Attacks. Hierbei wird einem Knoten ständig ein Wake-Up Signal zugespielt, so dass dieser seinen Energievorrat sehr schnell aufbraucht.

Zu Vermeidung von Depletion-Attacks können sichere Wake-Up Codes verwendet werden. Diese sind wesentlich komplexer als einfache Wake-Up Signale stellen aber sicher, dass ein Empfänger nur von einer vertrauenswürdigen Quelle geweckt werden kann. Im Folgenden wird die Umsetzung eines solchen sicheren Wake-Up Receivers skizziert. Die Entwicklung erfolgte im Rahmen des Aeternitas Projektes und basiert auf dem Wake-Up Receiver des Fraunhofer IIS.

2.2.1 Hardware-Plattform für die Entwicklung eines sicheren WakeUp-Empfängers

Für das Anwendungsszenario eines WUR-basierten Multi-Hop Sensornetzwerkes wurde vom IHP die IHPStack Plattform ausgewählt. Der IHPStack verwendet ein modulares Design aus einer beliebigen Anzahl an Module, die über einen einheitlichen Connector untereinander verbunden sind. Für diesen Stack existieren bereits Module, die Rahmen von Aeternitas weiterverwendet werden sollen. Im Rahmen von Aeternitas soll der vorhandene Stack um den sicheren WakeUp-Receiver erweitert werden. Hierbei wird zunächst eine kombinierte Lösung angestrebt. Diese Lösung besteht aus einem FPGA-Module und einem Wake-Up Receiver Module. Im Folgenden werden der IHPStack und die Module im Einzelnen vorgestellt. Anschließend wird ein möglicher Integrationspfad zu einer Single-Chip Lösung skizziert.

IHPStack

Der IHPStack wurde initial für das Messen von Grundwasserpegeln entwickelt. Das System sollte hierbei in die Pegelrohre integriert werden und die mechanischen Brunnenpfeifen ersetzt. Ziel war ein autarker Einsatz des Knotens mit einer Laufzeit von mehreren Jahren. Um dieses Ziel zu erreichen, wurden ausschließlich Low-Power-Komponenten eingesetzt und die Anzahl der Schaltkreise auf ein Minimum reduziert. Um neue zusätzliche Anforderungen erfüllen zu können

wurde ein modularer Aufbau gewählt. Hierbei wird das System aus einer beliebigen Anzahl an Modulen zusammengesetzt. Die einzelnen Module sind die über den Module Component Interconnect (MCI) verbunden. Der MCI ermöglicht hierbei ein nahezu wahlfreies Austauschen von Modulen.

Bild 29: IHPStack, ein modularer Sensorknoten für Prototypenentwicklung.

Ein Sensorknoten besteht minimal aus einer Stromversorgung, einem Mikrocontroller, Sensoren, lokalem Speicher und einem Kommunikationsinterface. Beim IHPStack wird jede dieser Anforderungen als einzelnes Modul umgesetzt. So kann der Sensorknoten leicht an andere Anforderungen, wie z.B. Funkfrequenz, Stromversorgung, Speicherbedarf oder Sensorik, angepasst werden.

Für den Aeternitas-Knoten können aus den bereits vorhandenen Modulen der 868MHz Transceiver, der MSP430 Microcontroller, die Batteriestromversorgung und das USB-Entwicklungsmodul übernommen werden.

FPGA-basierte Entwicklungsplattform

Für die Bereitstellung einer sicheren Authentifizierung von Sendern, muss der von Fraunhofer bereitgestellte WakeUp-Receiver AET868x um zusätzliche digitale Hardware erweitert werden. Da das Design der Algorithmen unabhängig von der eigentlichen WakeUp-Technologie ist, ist eine Fertigung von separaten Modulen (WakeUp-Receiver und Security Module) ohne Anpassungen möglich. Um eine schnelle Entwicklung und Erprobung der Algorithmen zu gewährleisten, sollen diese zunächst auf einem FPGA umgesetzt werden. Im Folgenden kann eine Integration in eine Single-Chip-Lösung erfolgen.

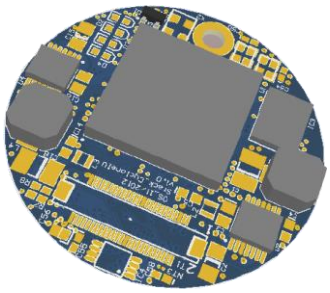


Bild 30: Altera FPGA Module für den IHPStack als Hardware-Platform für das Security Module des Wake-Up Receivers

Als FPGA-Plattform wurden hierzu die FPGAs von Altera ausgewählt. Diese sind als Entwicklungsplattformen verfügbar und können demnach schnell eingesetzt werden. Darüber hinaus wurde der vom IHP verwendete Mikrocontroller IHP430x bereits auf diesen FPGA portiert, so dass eine schnelle Wiederverwendung in Aeternitas gegeben ist.

Um das Gesamtkonzept eines sicheren Multi-Hop-Netzwerkes testen zu können, wurde ein FPGA-Modul für den IHPStack erstellt. Dieses kann in den Stack als zusätzliches Modul oder als Ersatz für den bereits vorhandenen MSP430-Mikrocontroller eingesetzt werden. In Verbindung mit den bereits vorhandenen Transceiver-, Sensor- und Batterie-Modulen kann zeitnah ein Test der Gesamtkonfiguration durchgeführt werden. Lediglich der Stromverbrauch kann in dieser Konfiguration nicht den Zielanforderung genügen, da das FPGA-Modul nicht als Low Power Device konzipiert ist. Diese Anforderung wird jedoch durch die anschließende Integration des Ansatzes in eine Single-Chip-Lösungen erfüllt.

Innerhalb des IHPStacks werden die Module über den MCI verbunden. Dieser definiert eine einheitliche Pin-Belegung für die verschieden Signaltypen eines Sensorknotens. Für die Integration, (siehe Bild 30) des WakeUp-Receivers, muss dieser mit dem Security Modul verbunden werden. Das Security Modul stellt die Verbindung vom Mikrocontroller und zum Radio Transceiver her. Erst wenn das Security Modul eine gültig Sequenz des WakeUp Signals (WUP_A/B) erkannt hat, wird eine Interrupt (Irq), WakeUP-Signal, für den Mikrocontroller ausgelöst.

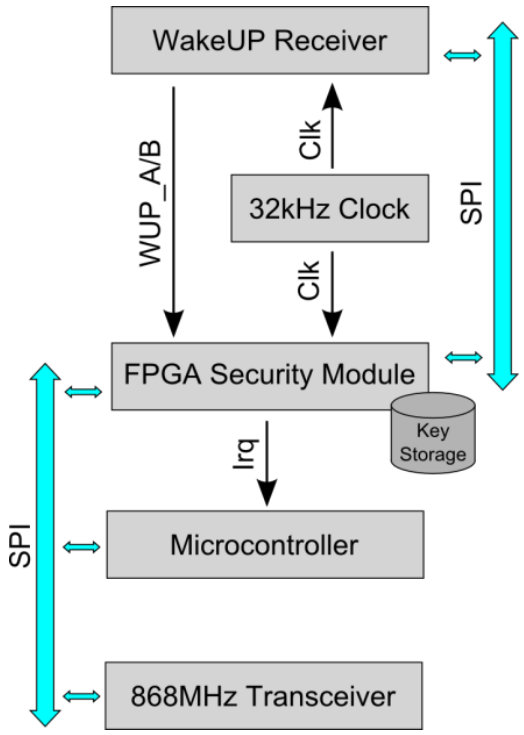


Bild 31: IHPStack Datenverbindungen

Im ersten Integrationsschritt sind WakeUp Receiver und Security Modul als separate Module definiert. Dies hat den Vortrag, dass im Folgenden neue Entwicklungen an dem FPGA evaluiert werden können und neue WakeUp-Receiver ICs leicht in den Stack eingebunden werden können.

AET868x Wake-Up Receiver-Modul

In den ersten Projektmonaten wurde die Entwicklung des sicheren Wakes mittels der bereits zu Projektbeginn vorhandenen Wake-Up Receiver von Fraunhofer IIS durchgeführt. Obwohl der Receiver nur eine geringe Reichweite und einen sehr begrenzten Operationsbereich hatte, konnten die wesentlichen Komponenten des Algorithmus entwickelt werden.

Parallel zur Entwicklung des sicheren Wake-Up Receivers wurde von den Projektpartner der Wake-Up Receiver weiterentwickelt und in der IHP in-house Fab gefertigt. Für die fertigen Module wurde durch das IHP ein zusätzliches Wake-UP Module entwickelt. Da sich parallel zur Entwicklung des Wake-Up ICs gezeigt hat, dass das der bisher verwendete Transceiver IC wesentliche Schwächen bei hohen Sendeleistungen aufweist, wurde eine kombiniertes IHPStack Modul entwickelt und gefertigt. Das Modul verfügt über den AET868(x) Wake-Up Receiver und ein CC1120 Transceiver. Bild 32 zeigt eine Draufsicht auf das Modul.

Das Modul wird über den MCI (Connector in der oberen Bildhälfte) in den Stack eingebunden. Um den Aufbau des Sensorknotens zu vereinfachen, verfügt das Modul über einen Antennenumschalter. Damit kann das Modul mit einer einzigen Antenne betrieben werden. Solange der Wake-Up Receiver aktiv ist, wird der Antennenpfad auf diesen geschalten. Sobald der Transceiver CC1120 aktiviert wird, erfolgt ein aktives Umschalten des Antennenpfades auf den Transceiver.

Bild 32: AET868x Wake-Up Receiver Modul mit CC1120 Transceiver für den IHPStack Sensorknoten

Durch die Kombination des Wake-Up Receivers mit dem Transceiver konnte die Anzahl der notwendigen Stack-Module entsprechend reduziert werden. Das Transceiver-Modul kann zudem auch ohne das FPGA-Module verwendet werden. In dieser Konfiguration muss auf das sichere Wake-Up verzichtet werden oder dieses als Software-Variante in der MCU umgesetzt werden.

Integrationspfad

Die Umsetzung eines sicheren WakeUp-Transceivers (SecWUT) als Single-Chip-Lösung erfordert die Integration des WakeUP-Receivers, des Security Moduls, eine Transceivers und des Low-Power Mikrocontroller (LP-µC). Ziel war die Entwicklung der einzelnen Module im Rahmen des Aeternitas

Projektes durch die verschiedenen beteiligten Institute. Durch die Umsetzung des modularen Ansatzes, konnten diese Entwicklungen parallel erfolgen. Bild 33 zeigt den geplanten die Integrationspfad für die Single-Chip Lösung.

Zunächst erscheint eine Kombination des Security Moduls und des WUR als sinnvoll. Eine derartige Lösung könnte in verschiedenen Sensorknoten in Kombination mit einem handelsüblichen 868MHz Transceiver und einem LP-µC eingesetzt werden. Durch die Integration des Transceivers in den SecWUR kann die Anzahl der notwendigen ICs auf dem Sensorknoten weiter reduziert werden. Des Weiteren kann in einem derartigen Design das Routing des 868MHz HF-Signals wesentlich vereinfacht werden.

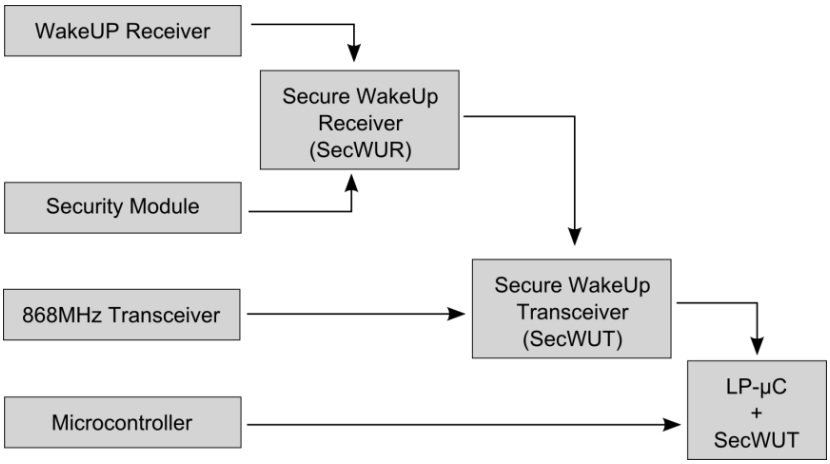


Bild 33: Integrationspfad für die Erstellung eine Single-Chip Lösung eines sicheren WakeUp-Receivers.

Als letzter Schritt kann der SecWUT mit dem LP-µC verbunden werden. Dies würde die Anzahl der notwendigen Chips auf ein Minimum reduzieren. Durch die Verwendung von Power-Gates können nicht benötigte Schaltungsteile des ICs bis zum Empfang eines gültigen WakeUp-Signals deaktiviert werden. Dieser Schritt bedingt jedoch, dass der SecWUT in der 0,25µm Technologie des IHP vorliegt, da der LP-µC nur in dieser Technologie mit einem non-volatile Speicher gefertigt werden kann.

Durch Schwierigkeiten bei der Umsetzung der einzelnen Komponenten, wurde die vollständige Integration der Lösung nicht mehr erreicht. Im Rahmen des Projektes wurden jedoch die wesentlichen Voraussetzungen für die Single-Chip Lösung geschaffen, so dass diese nach Bedarf im Folgenden umgesetzt werden kann.

2.2.2 Authentifizierungsverfahren für einen WakeUp-Empfänger

Die Funktionsfähigkeit eines Sensornetzes wird wesentlich durch die Energieverbrauch der einzelnen Knoten bestimmt. So kann insbesondere in dünnen Multi-Hop Netzwerken der Ausfall einzelner Knoten zum Ausfall ganzer Netzteile führen. Aus diesem Grund ist die Haushaltung der Energiereserven der Knoten von entscheidender Wichtigkeit. Mit dem Einsatz eines WUR, kann die Anzahl von unnötigen Wachphasen und damit der Gesamtenergieverbrauch entscheidend reduziert werden. Dem entgegen tritt jedoch die Gefahr von unautorisierten Aufwachkommandos. In einem ungeschützten System können Dritte durch stetiges Aufwachen die Energie von Knoten vollständig aufbrauchen und damit die Funktionsfähigkeit von Sensornetzen nachhaltig beschädigen.

Aus diesem Grund soll der von Fraunhofer entwickelte WakeUp Empfänger um eine sichere Authentifizierung ergänzt werden. Die hierfür notwendig Hardware-Plattform wurden bereits im vorangegangenen Abschnitt beschrieben. In diesem Abschnitt erfolgt eine Übersicht der Anforderungen an einen sicheren Wake-Up Empfänger.

Anforderungen an einen SecWUR

Für die Auswahl eines Algorithmus für den SecWUR wurden zunächst die Anforderungen, die an einen solchen Algorithmus gestellt werden zusammengetragen. So wurden drei Kernanforderungen erarbeitet, die folgen genauer erläutert werden.

Niedrige Datenrate

Wesentliche Einsparungen beim Energieverbrauch des WUR konnten durch eine Reduzierung der Datenrate erzielt werden. Hierbei besteht eine lineare Beziehung zwischen Energieverbrauch und Datenraten. Demzufolge kann eine maximale Energieeinsparung bei der minimalen Datenrate erzielt werden. Eine niedrige Datenrate erhöht jedoch den Zeitbedarf für die Übertragung eines Datensatzes und damit die Latenz des WakeUp-Signals.

Für den SecWUR wird demzufolge nach einem Algorithmus gesucht, bei dem möglichst wenige Daten zwischen Sender und Empfänger übertragen werden müssen.

Einweg-Authentifizierung

Sichere Authentifizierungsverfahren basieren meist auf einem Mehrwege-Hand-Shake dem mehrere Datensätze zwischen den Kommunikationspartner ausgetauscht werden. Der WUR nur Daten empfangen kann, wird nach einem Algorithmus gesucht, der lediglich Daten vom Sender zum Empfänger überträgt und ohne eine Antwort auskommt.

Einmal Passwörter

Das Übertragungsmedium Luft ist ein gemeinschaftliches Medium, d.h. jeder Teilnehmer kann alle Nachrichten in seinem Empfangsbereich empfangen. Ein gerichtetes Zustellen von Nachrichten ist möglich. Aus diesem Grund wird ein Algorithmus gesucht, der eine Wiederverwendung von übertragenen Nachrichten (Replay) wirksam verhindert.

Algorithmen, die ein Wiederverwenden von Passwörtern verhindern, benötigen eine Synchronisation zwischen den Kommunikationspartnern. Demzufolge muss der ausgewählte Algorithmus Re-Synchronisation Verfahren bereitstellen.

HMAC-based One-Time password Algorithm (HOTP)

Als ein Algorithmus, der die im vorangegangenen Abschnitt genannten Anforderungen erfüllen kann, wurde die HMAC-basierte Passwort-Generierung basierend auf dem RFC4226 identifiziert. Der Algorithmus nutzt einen 160-bit SHA-1 Hash zum Generieren des Passwortes. Wie in der folgenden Formel dargestellt, nutzt der Hash den Schlüssel *K* und Text *text* als Eingabewerte.

$$\boldsymbol{HMAC(K, text)} = \boldsymbol{H((K0 \oplus opad) || H((K0 \oplus ipad) || text))}$$

Sowohl Sender als auch Empfänger müssen Kenntnis über die beiden Eingabewerte besitzen. Der *HMAC(K, Text)* wird als WakeUp-Sequenz übertragen. Wenn der Empfänger aus seinen

Eingabewerten, den gleich HMAC errechnet, wird die Sequenz als gültig identifiziert und der Knoten aufgeweckt.

In dem vorgeschlagenen Algorithmus entspricht *text* der ID des Knotens oder einer Gruppen-ID. Der Schlüssel *K* ist ein Geheimnis, das regelmäßig erneuert wird, um Replay-Angriffen zu begegnen. Hierzu wird der Schlüssel aus einer Pseudozufallszahlenfolge gebildet. Für das Bilden der Zahlenfolge kann ebenfalls das SHA-1 Verfahren verwendet werden. Ein Update des Schlüssels erfolgt jeweils nach dem Empfang eines gültigen Schlüssels und nach dem Ablauf eines Gültigkeitszeitraumes. Der Zeitraum kann durch den Nutzer bestimmt werden. Wobei ein kürzerer Zeitraum die Robustheit des Algorithmus verringert und ein längerer Zeitraum den Schutz gegen Brute-Force-Angriffen herabsetzt.

Die Synchronität zwischen den Knoten wird über die 32 kHz Clock gewährleistet. Hierbei werden Uhrquarze mit einer Genauigkeit von 20 ppm eingesetzt. Damit haben die Knoten eine Gangungenauigkeit von 26,73 s pro Monat. Dementsprechend müssen die Knoten aufgeweckt werden. Im Wachzustand führen die Knoten eine Re-Synchronisation der Uhren durch.

Der Algorithmus erzeugt einen 160-bit HMAC. Da Sender und Empfänger den HMAC jedoch separat berechnen, ist es nicht zwingend notwendig, dass der komplette HMAC übertragen wird. Dies bietet die Möglichkeit die Latenz und die Robustheit des Algorithmus zu beeinflussen. So lässt sich die Latenz entscheidend verkürzen, wenn nur 20 statt der kompletten 160-Bit übertragen werden. Alternative kann die Robustheit erhöht werden, wenn nur ein prozentualer Anteil des empfangenden HMAC korrekt sein muss. In beiden Fäll wird jedoch der Schutz gegenüber Brute-Force-Angriffen verringert.

Energieverbrauch und Laufzeitabschätzung

Wie bereits erläutert wurde, wurde im Rahmen des Projektes zunächst eine Software-Lösung des sicheren Wake-Up Receivers erstellt. Die Lösung verzichtet auf den Einsatz des Security-Moduls und ist damit auf Off-the-shelf Komponenten lauffähig. Im Folgenden wird eine Abschätzung des Energieverbrauchs und der Laufzeit des Sensorknotens für die Software- als auch für die Hardware-Lösung gegeben.

Software-Lösung

Der Energieverbrauch des WakeUp-Subsystems der Software-Lösung wird durch den Leerlaufverbrauch des WUR, dem Empfangen des Schlüssels und durch die Berechnung des Schlüssels bestimmt.

Die aktuelle Umsetzung des WUR unterstützt die Verwendung von verschiedenen Datenraten. In der niedrigsten Datenrate werden 32 Bps übertragen und in der höchsten 8192 Bps. Dem gegenüber steht ein Stromverbrauch von 2 µA (32 Bps) und 123,2 µA (8192 Bps). Um den Verbrauch des WUR im Leerlauf möglichst gering zu halten. Erfolgt die Übertragung des WakeUp-Signals in zwei verschiedenen Phase. In der ersten Phase wird ein Bit des Signals mit der niedrigsten Datenrate übertragen. Die folgenden 19 Bit werden mit der höchsten Datenrate übertragen. Damit kann der Empfänger im Leerlauf den Äther mit der niedrigsten Datenrate abtasten. Erst wenn ein gültiges WakeUp-Symbol empfangen wurde, wird in den höchsten Modus umgeschaltet. Der Leerlaufverbrauch des WUR beträgt demzufolge bei einer Spannung von 3V 6µJ.

Das Empfangen des Schlüssels setzt sich aus der ersten Phase und der zweiten Phase zusammen. So werden in der ersten Phase 6,19 µJ und der zweiten Phase 56,6 µJ verbraucht. Dies entspricht einem Gesamtverbrauch von 62,79 µJ pro WakeUp-Sequenz.

Für die Berechnung des SHA-1 Wertes werden die in Tabelle 8 angegebenen Werte genutzt. Der Gesamtverbrauch es SHA-1 beträgt 40,63 µJ, wobei diese Werte von einer Komponente in der 0,25 µm Technologie entsprechen, in 0,13 µm sind die Werte noch geringer.

Komponente	Stromaufnahme 2.5V [mA]	Dauer bei 32.768kHz clock [ms]	Clock-Zyklen	[µJ]
SHA-1	6,5	2.5	82	40,63

Tabelle 8: Energieverbrauch der SHA1 Hardware-Einheit

Unter der Annahme, dass die Gültigkeit eines Schlüssel 30 bzw. 60 Sekunden beträgt und ein Mal pro Stunde ein WakeUp-Signal gesendet wird, ergeben sich für das SecWUR die Laufzeit aus Tabelle 9. Hierbei wurde davon ausgegangen, dass das Modul mit einem Akku mit einer Energie von 3240mJ (1,2V 1700mAh) genutzt wird.

Komponente	Energie/Tag [mJ]	Laufzeit [Jahr]
WUR	174,31	59,78
SecWUR (30s)	636,92	41,48
SecWUR (60s)	232,81	48,91

Tabelle 9: Laufzeit des WUR bzw. SecWUR bei der Verwendung eines Standard-Akku (1,2V 2700mAh)

Hardware-Lösung

Zur Abschätzung des Energieverbrauchs des Hardware-basierten Wake-Up Receivers wurde die Implementierung in die 0,13 µm Technologie des IHPs übertragen. Anschließend wurde die Schaltung mittels des Werkzeugs PrimePower simuliert.

Hierbei wurde ein Energieverbrauch von insgesamt $2{,}34 \times 10^{-2}$ mW festgestellt. Dieser Verbrauch wird jedoch nur erreicht, wenn alle Komponenten des security Moduls ständig aktiv sind. Beim der Umsetzung des TOTP Algorithmus ist dies jedoch nicht der Fall. Einzig der Timer ist ständig aktiv. Dieser jedoch einen Verbrauch von $0{,}8 \times 10^{-3}$ mW. Der größte Energieverbrauch ist der SHA-1 ($1{,}03 \times 10^{-2}$ mW) und der Prozessor ($2{,}7 \times 10^{-3}$ mW). Beide Komponenten sind jedoch nur ein alle 30 Sekunden für wenige Millisekunden aktiv. Der Duty Cycle lässt sich mit 1/1000 abschätzen. Damit liegt der durchschnittliche Verbrauch bei lediglich 12.8 µW.

Beim Empfang eines Wake-Up Signals wird der Symboldekoder aktiviert. Dieser hat einen Energieverbrauch von lediglich 3 µW pro Wake-Up Pattern.

Restrisikobetrachtung

Um die Wirksamkeit des Algorithmus gegen Angriffe Dritter zu überprüfen, wurde zunächst möglichen Angriffsmethoden gesucht. Hierbei konnten die folgenden drei Methoden identifiziert werden.

Replay

Beim Replay Angriff wird eine empfangene Nachricht erneut an dem Empfänger gesendet. Besitzt dieser keinen Schutz gegen entsprechende Angriffe, wird er diese akzeptieren und dem Angreifer ein entsprechendes Vertrauen entgegenbringen.

Durch die Verwendung der One-Time-Schlüssels und des stetigen Erneuerns, ist ein Replay-Angriff nicht möglich. Der durch den Algorithmus genutzte Schlüssel ist 2^160 Bit groß. Damit ist eine Wiederverwendung eines Schlüssels nahezu ausgeschlossen. Ein Angreifer kann einen Schlüssel nur dann verwenden, wenn der Empfänger diesen noch nicht empfangen hat und auch denn kann er diesen Schlüssel nur genau einmal verwenden, da er nicht auf den folgenden Schlüssel schließen kann. Darüber hinaus besitzt der empfangene Schlüssel nur eine Gültigkeit von 30 oder 60 Sekunden.

Ein Replay Angriff kann damit ausgeschlossen werden.

Man-in-the-Middle

Beim Man-in-the-Middle Angriff versucht ein Angreifer unmittelbarer Teilnehmer der Kommunikation zu werden und sich einem Empfänger als gültiger Sender vorzustellen. Dies ist aber nur dann möglich, wenn der Angreifer Kenntnis über den Schlüssel erlangt. Da der Schlüssel lediglich auf dem Knoten gespeichert und nicht unverschlüsselt übertragen wird, muss der Angriff physischen Zugriff auf einen Knoten erlangen. Gelingt ihm das nicht, ist ein Man-in-the-Middle Angriff nicht möglich.

Die sichere Speicherung von Schlüssel ist Bestandteil von verschiedenen Forschungsarbeiten, die teilweise auch am IHP durchgeführt werden. Unter der Annahme, dass der Schlüssel sicher auf dem Knoten gespeichert wird, kann ein Man-in-the-Middle Angriff auf das System ausgeschlossen werden.

Brute-Force

Der Brute-Force Angriff ist einfach und kann von Jedermann leicht durchgeführt werden. Hierbei werden alle möglichen Varianten eines Schlüssels durchgeführt werden. Dabei hängt die Wahrscheinlichkeit eines erfolgreichen Angriffes von der Größe des Schlüsselraumen und von der Gültigkeitsdauer eines Schlüssels ab. Für den vorschlagenden Algorithmus ergeben sich die Tabelle 10 angegeben Wahrscheinlichkeiten.

Schlüssellänge (bit)	Schlüsselgültigkeits-zeitraum (sec)	Wahrscheinlichkeit (%)
8	30	5,6596734
20	30	0,0013201
32	30	0,0000003
8	60	11,3193468
20	60	0,0026402
32	60	0,0000006
8	90	16,9790203
20	90	0,0039603
32	90	0,0000009

Tabelle 10: Wahrscheinlichkeiten eines erfolgreichen Brute-Force Angriffes bei verschiedenen Schlüssellängen und Gültigkeitszeiträumen

Die Ergebnisse der Untersuchungen zeigen, dass bei einer Schlüssellänge von 20-bit bereits eine hohe Sicherheit geboten werden kann.

2.2.3 Evaluierung des sicheren Wake-Up Receivers als Software-Lösung

Für die Evaluierung des sicheren Wake-Up Receivers wurde diese mit einem Low Duty Cycle Protokoll verglichen. Sowohl die Software-Lösung des Wake-Up Receivers als auch das Protokoll wurden für das Betriebssystem langOS entwickelt. Im Folgenden wird zunächst das Betriebssystem langOS, das Low Duty Cycle Protokoll und der Time-based One-Time Pad Algorithmus vorgestellt. Anschließend werden die beiden Lösungen mit einander verglichen.

langOS

Das Betriebssystem langOS wurde zusammen mit dem IHPStack im Rahmen des des IQlevel Projektes entwickelt. Das Betriebssystem ist vollständig in C umgesetzt und speziell für den MSP430 entwickelt. Es verfolgt konsequent eine low power Ansatz in dem es den Controller automatisch in einen minimalen Energiemodus schaltet sobald keine Aktivitäten registriert werden. Darüber hinaus enthält das Betriebssystem die notwendigen Routing-Algorithmen für das angestrebte Multi-Hop-Verfahren. Aus diesen Gründen wurde langOS als System für die Umsetzung der Aeternitas-Anwendungsszenario ausgewählt.

langOS wurde zum Abschluss des Projektes unter der EUPL unter sourceforge veröffentlicht. Durch die Offenlegung der Quelle und die frei Nutzung durch andere Nutzer wird eine breite

Anwendergemeinde adressiert, so dass zum einen die Bekanntheit der Ergebnisse gesteigert werden kann und zum anderen Fehler in der Implementierung leichter gefunden werden. langOS wird am IHP in verschiedenen Projekten eingesetzt und hat damit bereits eine breite Modulbasis, die auch in zukünftigen Projekten verwendet werden kann.

Fair-Energy Trade Multi-Hop Routing

Die Nutzung von Multi-Hop Routingverfahren in drahtlosen Sensornetzwerken hat sich als effiziente Lösung zur Überbrückung von größeren Entfernungen etabliert. Es wurde in verschiedenen wissenschaftlichen Veröffentlichungen gezeigt, dass mit einem verhältnismäßig geringen Energieverbrauch Daten über größere Entfernungen zuverlässig übertragen werden können. Allerdings ist die praktische Verbreitung von Multi-Hop Sensornetzwerken gering. Dies ist unter anderen durch zwei Probleme begründet. Zum einen steigt mit der Größe des Netzwerkes der Aufwand für eine effiziente Strukturierung des Netzwerkes. Dies wiederum führt insbesondere bei der Nutzung von Rendezvousverfahren zu einer nicht akzeptierbaren Paketverzögerung. Zum anderen sind bei den meisten Multi-Hop Routingverfahren einzelne Knoten wesentlich stärker belastet als andere. Dies führt dazu, dass deren Energiereserven schneller aufgebraucht werden. Was wiederum zu einem frühzeitigen Ausfall von ganzen Netzsegmenten führen kann.

Am IHP wurde ein Multi-Hop Routingverfahren entwickelt, dass sich durch einen besonderes fairen Verbrauch der Energie unter den Knoten auszeichnet und die Paketverzögerung von der Datenquelle zur Senke auf ein Minimum reduziert. Das Verfahren basiert auf dem DLDC-MAC, welches zunächst für Single-Hop Netzwerke entwickelt wurde. Zur Verwendung des Verfahrens innerhalb eines Multi-Hop Netzwerkes wurde dieses um die Nutzung von Crosslayer-Informationen erweitert. Mittels der zusätzlichen Informationen erfolgt ein zeitlich global geordneter Zugriff auf das Medium, so dass Knoten, die weiter von der Senke entfernt sind, ihre Daten zuerst senden können. Damit können die Daten innerhalb eines vollständig geordneten Netzwerkes innerhalb einer Periode von jedem Sensor zu Senke übertragen werden. Die Optimierung erfolgt jedoch zu Lasten der Paketverzögerung in der entgegengesetzten Richtung. Zur Sicherstellung eines fairen Verbrauchs der Energie innerhalb des Netzwerkes wurde mit der Strongest Energy Chain Metrik eine spezielle Routing-Metrik entwickelt und in das Protokoll integriert. Die Metrik ermittelt auf allen Pfaden zur Senke den größten Minimalwert der verfügbaren Energie, Bild 34 zeigt ein Beispiel für ein einfaches Multi-Hop Netzwerk mit sieben Knoten oder einer Senke.

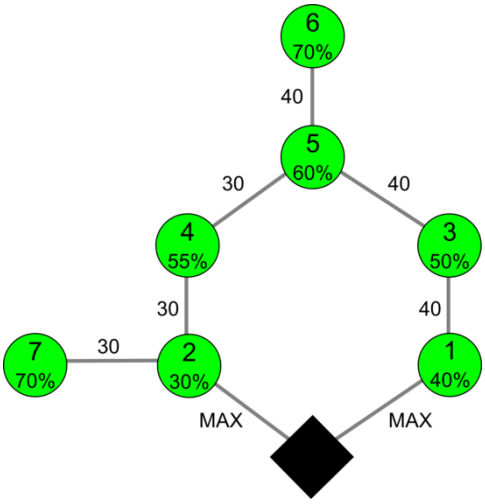


Bild 34: Beispielnetzwerk der SEC-Metrik. Knoten 6 sendet seine Daten über die Knoten 5, 3 und 1, da auf dieser Route die minimalen Energiereserven größer sind.

Der Knoten 6 sendet seine Daten bei der Verwendung der SEC-Metrik über die Knoten 5, 3 und 1. Die minimalen Energiereserven (Knoten 1 mit 40%) dieser Route sind größer als auf der alternativen Route 5-4-2 (Knoten 2 mit 30%). Durch die Verwendung der SEC-Metrik kann erreicht werden, dass die Knoten 2 und 1 ihre Energie gleichmäßig verbrauchen und damit die minimale Lebenszeit des Netzwerkes maximiert wird.

Das Verfahren wurde für den IHPnode implementiert und innerhalb der Simulationsumgebung Castallia evaluiert. Im Rahmen des Aeternitas Projektes erfolgt aktuell die Inbetriebnahme eines Multi-Hop Netzwerkes auf Basis des IHPnode. Die Ergebnisse der Protokollentwicklung konnten bereits im Rahmen des Projektes auf einer internationalen Konferenz und in Form eines Journalbetrages präsentiert werden. Im verbleibenden Projektzeitraum soll das Rendezvous-basierte DLDC MAC durch ein Wake-Up basiertes Verfahren ersetzt werden. Hierdurch kann die Paketverzögerung in beiden Richtungen auf ein Minimum reduziert und damit eine weitere wesentliche Schwachstelle des Multi-Hop Routingverfahrens beseitigt werden.

TOTP-basierter Wake-Up Algorithmus

Im ersten Jahr des Projektes wurde eine Evaluierung der Anforderungen an den zu verwendenden Authentifizierungsalgorithmus durchgeführt. Anschließend erfolgte eine Untersuchung von vorhandenen Ansätzen. Hierbei hat sich gezeigt, dass der Hash-based one-time password Algorithmus (RFC4226) ein geeigneter Kandidat zu sein scheint. Der Algorithmus verwendet den HMAC-SHA-1 und einen Zähler zum Erzeugen eines „unendlichen“ Passwortstroms. Eine bidirektionale Kommunikation zwischen den Teilnehmer ist nicht notwendig. Für den sicheren Wake-Up Empfänger wurde letztendlich der Time-based one-time password (TOTP) Algorithmus (RFC6238) ausgewählt und umgesetzt. Dieser Algorithmus ist eine Erweiterung des HOTP und verwendet einen Timer zum Inkrementieren des Zählers. Der Zähler wird in festgelegten Zeitschritten von allen Teilnehmern inkrementiert und muss damit nicht beim Empfang des Wake-Up Signals ermittelt werden. Damit ist der Algorithmus für ressourcenschwache Geräte wesentlich besser geeignet.

Für die Umsetzung des TOTP auf den Sensorknoten waren jedoch Modifikationen erforderlich. Das RFC6238 schlägt die Verwendung eines Radio-Zeitsignals vor, welche jedoch auf dem Sensorknoten nicht zur Verfügung steht. Stattdessen wird als Zeitquelle der lokale 32kHz Uhrenquarz der Sensorknoten verwendet. Darüber hinaus wird die finale Modulo-Operation des HOTP ausgelassen. Stattdessen wird das gesamte 32-bit Ergebnis der HOTP *truncate*-Funktion übertragen. Auf dem Empfänger kann jedoch beim modifizierten TOTP eine variable Anzahl an notwendigen Bit festgelegt werden. Damit werden Bits, die nicht empfangen wurden, bei der Überprüfung ausgelassen und eventuelle Übertragungsfehler kompensiert. Ein Wake-Up Pattern ist gültig, wenn eine minimale Anzahl an Bits übertragen wurde und diese mit dem erwarteten Pattern übereinstimmen. Außerdem wird der TOTP Schlüssel bereits mit dem Inkrementieren des Counters erzeugt. Hierdurch wird der Rechenaufwand beim Empfang eines Wake-Up Pattern minimiert.

Durch die Verwendung des lokalen Uhrenquarzes sind Sender und Empfänger nicht synchronisiert. Für die Kompensation von Bit-Verlusten beim Empfang des Wake-Up Pattern ist es jedoch notwendig, dass Sender und Empfänger synchronisiert sind. Hierzu wurde die in Bild 35 dargestellte Start-Up Synchronisation eingefügt.

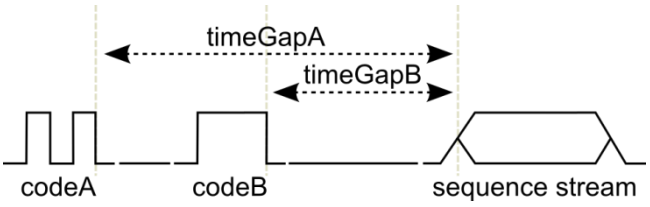


Bild 35: Start-Up Synchronisation von Sender und Empfänger mittels festvorgegebener Zeitgrenzen bei der Symbolübertragung.

Der Sender sendet vor dem Wake-Up Pattern zunächst genau einmal den CodeA und den CodeB mit der niedrigsten Datenrate. Das Pattern folgt diesen Codes nach einer fest vorgegebenen Pause mit der höchsten Datenrate. Der Empfänger kann mit dem Empfang der initialen Codes den Startzeitpunkt des Wake-Up Patterns bestimmen und dieses synchronisiert empfangen. Hierzu benutzt der Symbol Decoder, wie in Bild 36 dargestellt, einen lokalen Timer, der nach dem Empfang der initialen Codes initiiert wird. Mit jedem Timer-Tick wird die Bitstelle des Paketpuffers inkrementiert. Wird ein Bit nicht empfangen, wird die Stelle im Puffer ausgelassen und über den *mask*-Eintrag nicht in die anschließende Überprüfung mit einbezogen.

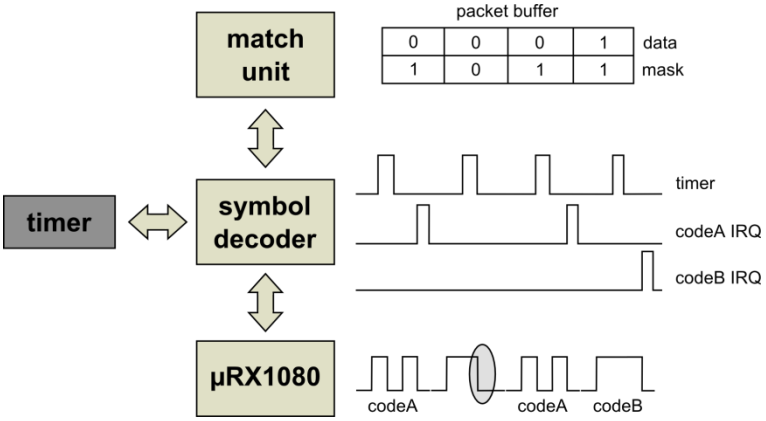


Bild 36: Synchronisierten Empfangen des Wake-Up Pattern. Beim Auftreten eines Übertragungsfehlers (grauer Kreis) wird kein Interrupt ausgelöst. Das zugehörige Bit im Empfangspuffer wird ausgelassen.

Da an Stelle des mittels der Modulo-Operation reduzierten Wertes immer das vollständige Ergebnis der HOTP *truncate*-Funktion übertragen wird, kann auch beim Auslassen von einzelnen Bits durch den modifizierten TOTP eine vergleichbare Sicherheit bereitgestellt werden.

Neben der Synchronisation von Sender und Empfänger zum Empfang des Patterns ist zusätzlich eine globale Synchronisation notwendig. Jeder Knoten inkrementiert seine lokalen Zähler auf welchem das Wake-Up Pattern basiert nach festen Zeitschritten über seinen lokalen Uhrenquarz. Beim Empfang des Patterns müssen Sender und Empfänger jedoch insoweit synchron sein, dass sie beide das gleiche Pattern erwarten. Da dies durch den natürlichen Drift des Uhrenquarzes (ca. 20 ppm) nicht über einen längeren Zeitraum (> 19 Tage) sichergestellt werden kann, wurde eine Resynchronization eingeführt. Hierzu generiert jeder Knoten eine begrenzte Anzahl an gültigen Schlüssel (z.B. 8 Schlüssel), die zeitlich in der Vergangenheit und in der Zukunft zum erwarteten Schlüssel liegen. Ein empfangendes Pattern wird nun immer mit allen speicherten Schlüsseln verglichen. Bei einer erfolgreichen Authentifizierung erfolgt anschließend durch den Mikrocontroller eine Resynchronisation der Schlüsselindizies. Hierbei müssen drei Möglichkeiten unterschieden

werden. Der Schlüssel entspricht dem erwarteten Schlüssel. In diesem Fall ist keine zusätzliche Aktion notwendig. Der empfangene Schlüssel liegt in der Zukunft. In diesem Fall, wird der lokale Zähler auf den Wert des empfangenden Schlüssels gesetzt. Liegt der Schlüssel in der Vergangenheit, sendet der Empfänger seinen aktuellen Zählerwert an den Sender und dieser aktualisiert seinen Zähler entsprechend.

Vergleich des secure Wake-Up Empfängers mit einer LDCP-basierten Lösung

Zum Vergleich beider Ansätze wurde der Stromverbrauch des Sensorknotens während seiner gesamten Lebenszeit untersucht. Hierzu wurden zunächst Messungen an einem Knoten durchgeführt, um festzustellen wie viel Energie in den jeweiligen Phase (Senden, Empfange und Idle) verbraucht wird. In Tabelle 11 sind die Ergebnisse der Messung zusammengefasst.

Parameter	Name	Value [mA]
TX power	TXpwr	24,0
RX power	RXpwr	22,0
Active power	activePwr	2,0
Idle power	idlePwr	0,021
WUR @64 Baud	minWur	0,0012
WUR @8192 Baud	maxWur	0,0867

Tabelle 11: Stromverbrauch des IHPnode in den verschiedenen Phasen (Senden, Empfangen, Idle).

Ausgehend von den Messwerten wurde mittels der Formel (3) der Energieverbrauch eines Knotens *pwrCon* für verschiedene Längen des Duty Cycles *period* und Anzahl an Nachbarn *neighbors* ermittelt. Die Anzahl der Nachbarn hat einen wesentlichen Einfluss auf den Stromverbrauch eines Knotens, da sie die Anzahl der Pakete bestimmt, die ein Knoten während einer Periode senden und empfangen muss. Für jedes empfangene Paket muss zudem ein Wake-Up Pattern empfangen werden. Die Länge der Sende- und der Receive-Phase ergibt sich wesentlich aus der Anzahl an Pakete und der Sendezeit pro Paket *sendTime*. Darüber hinaus haben wir für den MSP430F1612 die Zeit ermittelt, die dieser für die Berechnung eines neuen Schlüssels *hashTime* benötigt. Bei einer Taktrate von 4MHz benötigt der Knoten 48 ms.

$$idleTime = 3600 - wakeUpTime \times rxPkts - sendTime \times (2 \times rxPkts + 1) - \frac{3600}{patternLifeTime} \times hashTime \quad (1)$$

$$rxPkts = neighbors \times \frac{3600}{period} \quad (2)$$

$$pwrCon = idleTime\ x\ (idlePwr + minWur) + rxPkts \times wakeUpTime \times maxWur + rxPkts \times sendTime \times RXpwr + (rxPkts + 1) \times sendTime \times TXpwr + \frac{3600}{patternLifeTime} \times hashTime \times activePwr \quad (3)$$

Für eine Bewertung der Ergebnisse wurde ein Vergleich mit einer Implementierung eines Low Duty Cycle Protokolls durchgeführt. Dieses verwendet Rendezvouszeiten zum Austausch von Informationen und kann damit auf die Verwendung eines Wake-Up Receivers verzichten. Allerdings muss bei der Verwendung von Rendezvouszeiten eine sogenannte Guard Time eingeführt werden. Die Guard Time dient dem Kompensieren des lokalen Clock Drift und wächst mit der Länge des Duty Cycles. Ein Vergleich der Ergebnisse ist in Bild 37 zu sehen.

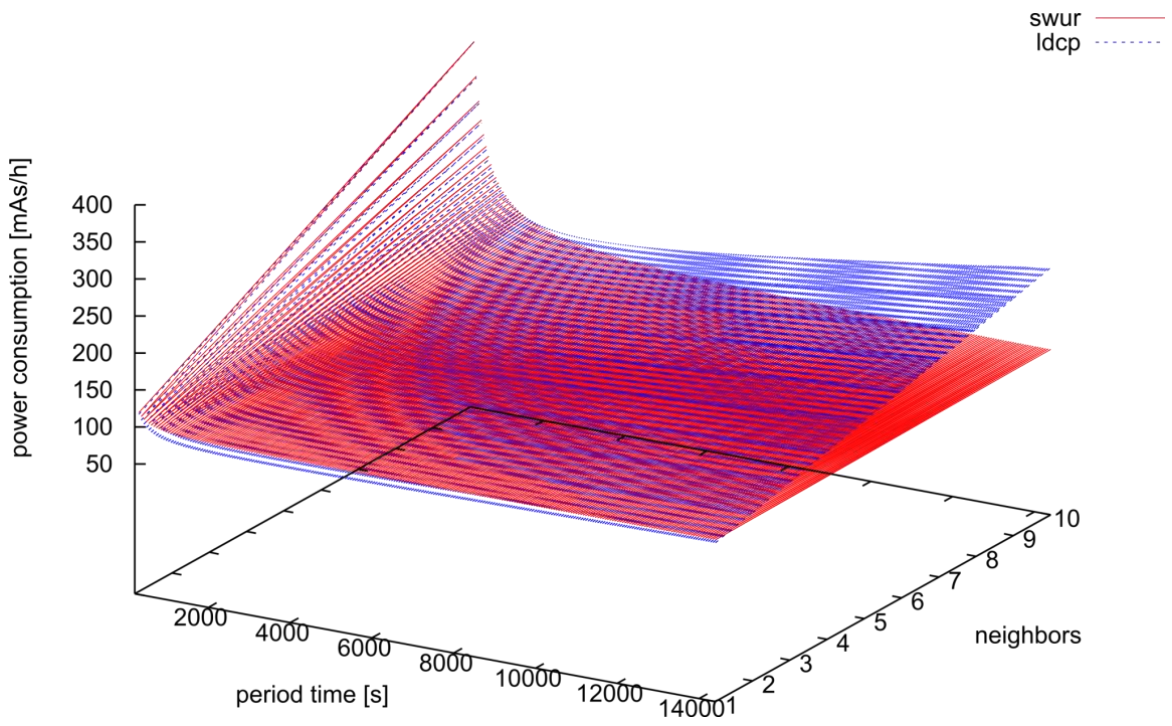


Abbildung 37: Vergleich des Stromverbrauches eines Sensorknotens in Abhängigkeit von der Länge des Duty Cycles und der Anzahl der Nachbarn bei der Verwendung des secure Wake-Up Receivers (swur) oder eines Low Duty Cycle Protokoll (ldcp).

Wie aus **Abbildung** ersichtlich, wächst der Stromverbrauch mit einem längeren Duty Cycle und einer größeren Anzahl an Nachbarn bei der Verwendung des sicheren Wake-Up Receivers nicht an. Für eine geringe Anzahl an Nachbarn ist der Stromverbrauch ähnlich dem Low Duty Cycle Protokoll. Erhöht sich jedoch die Anzahl der Nachbarn, hat dies einen wesentlich stärken Einfluss auf das Low Duty Cycle Protokoll als auf das Konzept des sicheren Wake-Up Receivers. Hier zeigt das Konzept wesentliche Vorteile gegenüber dem Low Duty Cycle Protocol.

2.2.4 Integration des sicheren Wake-Up Receivers in den IHPstack als Demonstrator

Nach dem das Konzept des Wake-Up Receivers mittels der Software-Implementierung erfolgreich umgesetzt werden konnten, wurde im folgenden Schritt das Konzept als Hardware-Lösung umgesetzt. Hierdurch soll der Energieverbrauch des Sensorknotens während der Idle-Phase auf ein Minimum reduziert werden. Um die Komplexität der Hardware-Lösung möglichst gering zu halten, wurde die Software-Lösung hinsichtlich einer möglichst effizienten Partitionierung untersucht. Hierzu wurden unter anderem die Code-Größe und die Menge des benötigten Speichers ermittelt. Tabelle 12 fast die ermittelten Größen zusammen und stellt sie in Relation zum Speicherplatz eines MSP430F1612.

Module	Text	%	Data	BSS	%
overall	53620	97.5	894	1257	43.0
wakeup	1728	3.1	0	90	1.8
swup	1268	2.3	148	50	4.0
keymgmt	308	0.6	0	356	7.1
swcore	1492	2.7	0	86	1.7
symdec	1594	2.9	2	76	1.6
hmacsha1	518	0.9	0	0	0.0
sha1	24208	44.0	24	0	0.5

Tabelle 12: Code- und RAM-Größe der Wake-Up Receiver Implementierung. Die Messungen erfolgten auf einem MSP430F1612 mit 55kB Flash und 5kB RAM. Der Programmcode wurde mittels des msp430-gcc (Version 4.5.3) erzeugt.

Aus Tabelle 12 wird ersichtlich, dass die SHA1 Implementierung *sha1* und der Symboldekoder *symdec* die größten Komponenten des Wake-Up Receivers darstellten und im Folgenden als reine Hardware-Module implementiert werden sollten. Darüber hinaus ist ein Timer für die Synchronisation zwingend erforderlich. Für das Umkonfigurieren der Datenrate zwischen den initialen Codes und dem Wake-Up Pattern im Wake-Up Receiver wird ein SPI Master benötigt. Dieser sollte ebenfalls als Hardware-Modul in den sicheren Wake-Up Receiver integriert werden, damit der Mikrocontroller nur dann aufgeweckt werden muss, wenn das vollständige Pattern empfangen und geprüft wurde.

Das *wakeup*- und das *swup*-Modul beinhalten Programmtext, der zum Senden des Wake-Up Pattern und zur Resynchronisation verwendet werden. Diese Module benötigen den Transceiver und sind nur aktiv, wenn der Knoten aufgeweckt wurde. Aus diesem Grund werden sie auch im finalen Entwurf des Wake-Up Receivers in Software umgesetzt.

Ausgehend von Evaluierung von der Software-Implementierung des Konzeptes des sicheren Wake-Up Receivers und den Ergebnissen der Analyse der Größe des Programmtextes erfolgte das Hardware-Software Co-Design.

Die Module SHA1, Timer und SPI Master sind typische Hardware-Module, die auch in anderen ASICs Anwendung finden. Sie sind am IHP als vollständige Implementierungen bereits vorhanden. Der Symboldekoder lässt sich aufgrund seiner geforderten Eigenschaften ideal in Hardware umsetzen. Der HMAC und die Implementierung des Schlüsselupdates sind jedoch Module, die sich als reine Hardware-Komponenten nur sehr schwer umsetzen lassen. Aus diesem Grund werden diese Komponenten in die Firmware eines eingebetteten Controllers integriert. Hierzu wird ein Controller als VLIW-Kern implementiert, der per Software konfiguriert und angepasst werden kann. Der Controller verfügt über einen kleinen Programm- und Datenspeicher zur Ablage der Firmware und temporärer Daten. Ein Überblick über die Komponenten des sicheren Wake-Up Receivers gibt Bild 36. Das Konfigurieren des ASICs erfolgt über ein SPI-Slave Modul. Über dieses Modul kann der

Mikrocontroller den Programm- und den Datenspeicher auslesen und beschreiben. Außerdem ist ein Zugriff auf den IO-Bus möglich, worüber die Register der Peripherien gelesen und beschrieben werden können.

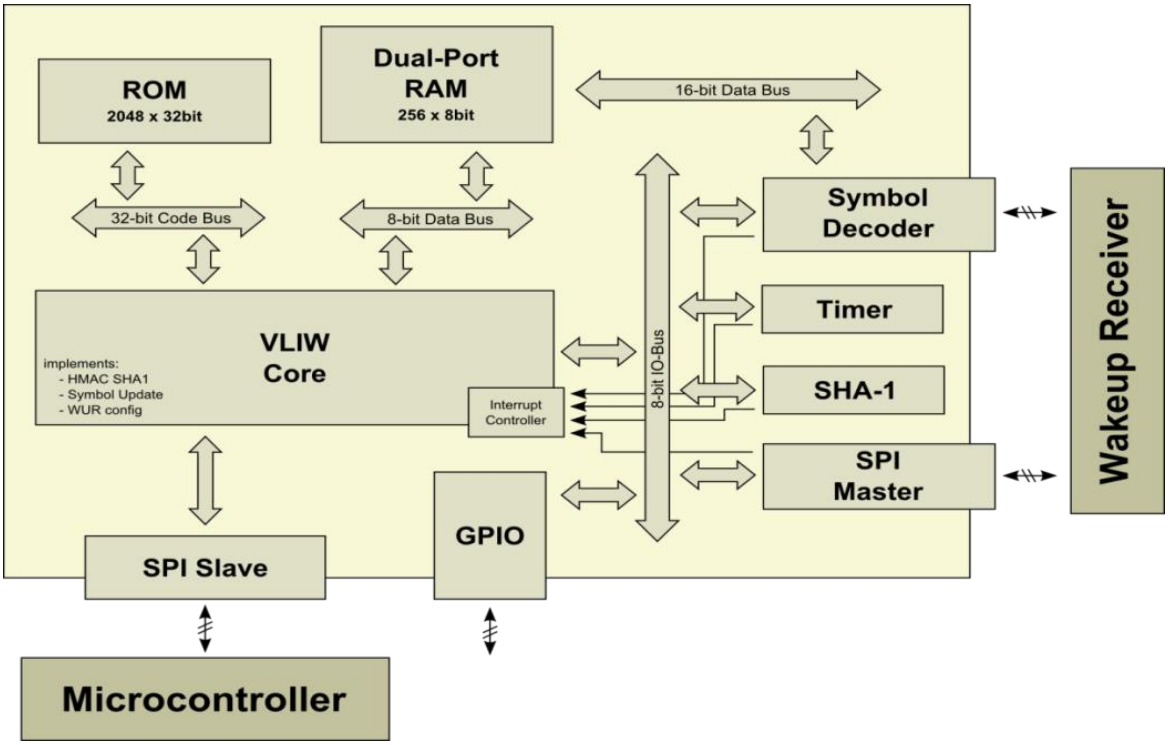


Bild 38: Blockdiagramm des sicheren Wake-Up Receivers

Der Controller verfügt über einen 8-bit VLIW Kern in Harvard-Architektur, der zwei Instruktionen parallel ausführen kann. Jede Instruktion wird innerhalb von zwei Takten abgearbeitet. Damit kann bei idealer Nutzung des Instruktionswortes eine Instruktion pro Takt ausgeführt werden. Der Kern ist als RISC Register-Register-Maschine implementiert. Es besitzt drei Funktionseinheiten (LD/ST, ALU und JUMP), von denen jeweils zwei gleichzeitig aktiv sein können. Die ALU und die JUMP Einheit arbeiten nur auf Register. Die Register müssen zuvor über die LD/ST-Einheit geladen werden. Der Kern verfügt über 8 generell-purpose Register und 4 shadow Register, die bei der Interrupt-Behandlung eingeblendet werden. Entsprechend der Harvard-Architektur sind die Speicher über dedizierte Busse angeschlossen. Darüber hinaus verfügt der Kern über einen separaten 8-bit IO-Bus über welchen die Register der Peripherien geschlossen sind. Zur Reduzierung des Strombedarfs wurde ein Clock-Gate integriert, welches vom Prozessor selbständig aktiviert und über einen Interrupt deaktiviert werden kann. Das Clock-Gate schaltet das Taktsignal des Prozessorkerns. Die Peripherien werden über dedizierte Enable-Signale gesteuert.

Das Design des VLIW Kerns ist unabhängig vom sicheren Wake-Up Receiver und kann in beliebigen ASICs zur Steuerung von Prozessen eingesetzt werden. Nichtsdestotrotz wurden beim Entwurf des Kerns die Anforderungen aus der Analyse des Konzeptes des sicheren Wake-Up Receivers einbezogen. Der Kern wurde hinsichtlich eines minimalen Funktionsumfangs optimiert, um den Stromverbrauch geringstmöglich zu halten. Hierbei muss trotzdem die Ausführung des Schlüsselupdates inklusive der HMAC-Operation innerhalb Schlüssellebenszeit (30 Sekunden bzw.

983.000 Takten bei 32 kHz) möglich sein. Zudem müssen ausreichend Reserven für die Auswertung und das Weiterleitung der Ergebnisse des Symboldekoders vorhanden sein.

Tabelle 13 zeigt einen Vergleich des Ressourcenbedarfs des VLIW Kerns mit anderen Ansätzen. Der Kern benötigt insgesamt 848 LUTs und 316 Register. In Verbindung mit dem SHA1 Modul des IHPs erhöht sich der Ressourcenbedarf auf 3.171 LUTs und 1.165 Register. Ein Vergleich mit 16-bit Controller IHP430x zeigt, dass den VLIW Kern nur ein Viertel an Ressourcen benötigt und damit entsprechend weniger Energie verbraucht. Die Konfigurationen MERCORA und LienDesai sind Implementierung des HMAC-SHA1 Algorithmus. Der Vergleich zeigt, dass VLIW Ansatz inklusive der Peripherien nur 10 % mehr Ressourcen benötigt als das LienDesai Design. Der MERCORA Ansatz ist wesentlich kleiner, jedoch nur als kommerzielle Modul verfügbar und damit nicht ohne zusätzliche Kosten nutzbar. Darüber hinaus beinhalten diese Ansätze nur den HMAC-SHA1, die Programmlogik für das Schlüsselupdate und die Auswertung der Symboldekoderergebnisse müssen zusätzlich umgesetzt werden.

Konfiguration	LUTS	Registers	Total
IHPvliw8	848	316	906
IHPvliw8 inkl. SHA1	3.171	1.165	3.551
IHP430x	4.107	960	4.535
MERCORA	-	-	1.047
LienDesai	-	-	3.268

Tabelle 13: Vergleich des Ressourcenbedarfs des VLIW8 Kerns mit alternativen Ansätzen

2.3 Zusammenfassung und Anschlussfähigkeit der Resultate

Die zum Teil spekulativen Ansätze zu innovativen Wakeup-Komponenten aus dem Projektplan haben sich in manchen Fällen bewährt, in anderen war eine weitere Verfolgung nicht sinnvoll. So sind die in den Si Chip integrierten SAW Filter technisch machbar, aber die Parameter dieser Komponenten sind für den Einsatz in einem Wakeup-Empfänger nicht ausreichend. Der Ansatz, durch Stressvermeidung bei SiGe HBT Transistoren die Parameter zu verbessern, führte zu dem Ergebnis, dass die angedachte vorbeugende Vermeidung ohne relevante Auswirkung ist. Zwar ist eine Degradierung teilweise reversibel, aber dieser Effekt ist erst bei hohen Leistungen und Temperaturen signifikant. Die Testschaltungen für Superregenerativempfänger konnten das Funktionsprinzip nachweisen. Dieser Zugang ist vielversprechend für Wakeup-Empfänger, welche eine konkurrenzfähige andersartige Architektur im Vergleich zum ISS Konzept haben. Die systematischen Studien zu low-power Frontends sind als erfolgreich zu bewerten. Es ergibt sich eine Variantenmatrix, welche verschiedene Technologien, Frequenzbereiche, und Schaltungstechniken vergleicht und beispielsweise LNAs mit einem Energieverbrauch unter 1 mW enthält. Ebenfalls erfolgreich war die Arbeit zur Entwicklung von low-power Referenzquellen, welche zu zwei verschiedenen funktionsfähigen Varianten führte.

Die Ergebnisse zu SAW-Resonator basierten WU-Empfängern haben sich im Laufe des Projektes ergeben und gehen über den Projektplan hinaus. Der Ansatz ist innovativ und scheint vielversprechend zu sein, sowohl in der Form als passiver Verstärker als auch zum Aufbau eines neuartigen energiesparsamen Superregenerativempfängers. Zu beiden Varianten wurden Patente angemeldet und erteilt. Diese Forschungsrichtung wird am IHP weiter geführt werden. Das Ziel ist, einen auf dem Prinzip aufbauenden IHP-eigenen Wakeup-Receiver zu entwickeln. Zu Projektende wurde bereits eine Zusammenarbeit mit einer Spezialfirma für SAW Komponenten begonnen, um eine weitere Variante zu untersuchen.

Die Untersuchungen zum secure wakeup entwickelten sich während der Projektlaufzeit zu einem größerem Schwerpunkt als ursprünglich vorgesehen und führten zu wertvollen Resultaten für das IHP. Zur Erfüllung der Sicherheits-Anforderungen von Airbus wurde der TOTP Algorithmus angepasst, geeignete Verfahren für die Synchronisation und Adressierung wurden erarbeitet, und die Komponenten wurden in VHDL und Software verwirklicht. Hierbei wurden theoretische Überlegungen, Simulationen, und Hardware/Software Entwicklung durchgeführt. Das Resultat ist eine verifizierte und vollständige Sicherheits-Lösung für Wakeup-Empfänger, welche mit dem Fraunhofer IIS System kompatibel ist. Die Forschung am IHP hat einen Schwerpunkt auf drahtloses Sensornetzen mit einem speziellen Fokus auf Sicherheitsfragen. Hierfür ist der secure wakeup eine wichtige Ergänzung. Das Sicherheitssystem wurde erfolgreich in den TANDEM-Stapel implementiert, wobei eine neue Ebene mit FPGA und eine weitere mit dem Haupt- und Wakeup-Radio erzeugt wurden. Zu Projektende konnte die Multihop-Funktion vorgeführt werden, wenn auch nicht in dem erhofften Umfang in einem größeren Sensornetz.

Die Anschlussfähigkeit und Verwertungsperspektiven der Resultate sind wie folgt:

- Die Ergebnisse zu innovativen Wakeup-Komponenten fliessen in weitere Projekte ein.
- Die low-power Referenzen und die SiGe LNAs werden weiter geführt, wobei der LNA als IP-Block übernommen wird.
- Die Untersuchungen zu beiden Varianten der SAW-Resonator-basierten Syteme werden weitergeführt mit dem Ziel, einen IHP-eigenen Wakeup-Empfänger zu entwickeln.
- Eine weitere Variante des SAW-Resonator Konzeptes wird mit einer externen Firma entwickelt.
- Der secure wakeup bildet als fertige Lösung einen Ausbau des IHP-Know-How im Bereich von Sensorknoten und Sicherheit, welche bei weiteren Projekten eingebracht wird.
- Es wird ein ASIC angestrebt, welches den IIS Wakeup-Empfänger mit dem secure wakeup kombiniert.

2.4 Aus dem Projekt hervorgegangene Publikationen und Patente

A Tiny Scale VLIW Processor for Real-time Constrained Embedded Control Tasks, Oliver Stecklina, Michael Methfessel, DSD 2014 17th Euromicro Conference on Digital Systems Design (Verona, Italy)

A Secure Wake-up Scheme for Low Power Wireless Sensor Nodes, Oliver Stecklina, Stephan Kornemann, Michael Methfessel , MSSNC 2014 4th International Workshop on Mobile Systems and Sensors Networks for Collaboration (Minneapolis, USA)

A Fair Energy Trade Multi-Hop Routing in Wireless Sensor Networks, Oliver Stecklina, Peter Langendörfer, Christian Goltz, WMNC 2013 6th Joint IFIP Wireless and Mobile Networking Conference (Dubai, VAE)

A lifetime Forecast scheme for a Distributed Low Duty Cycle Multi-Hop Routing in Wireless Sensor Networks, Oliver Stecklina, Peter Langendörfer, Christian Goltz, 2013: International Journal of Business Data Communications and Networking. (IJBDCN), 9(4)

Aufweckempfängerschaltung PCT/EP2014/072041, DE 10 2013 220 713.1

SAW-stabilized super regenerative receiver for sensor node wakeup, DE 10 2015 206 665.7

2.5 Referenzen

[1] A. Vouilloz, M. Declercq, C. Dehollain, "A low-power CMOS superregenerative receiver at 1 GHz", IEEE Journal of Solid-State Circuits, vol. 36, pp. 440-451, 2001

[2] B. Otis, Y. H. Chee, J. Rabaey, “A 400µW-RX, 1.6mW-TX super-regenerative transceiver for wireless sensor networks”, IEEE International Solid-State Circuits Conference, Feb. 2005, pp. 396–397

[3] J.-Y. Chen, M. P. Flynn, J. P. Hayes, “A fully integrated auto-calibrated super-regenerative receiver in 0.13-µm CMOS”, IEEE Journal of Solid-State Circuits, vol. 42, no. 9, pp. 1976–1985, Sept. 200742, no. 9, pp. 1976–1985, Sept. 2007

[4] M. Nenadovic, G. Fischer , " An Integrated, Low-Power, Temperature-Compensated CMOS Operational Amplifier for Application in Medical Device Tracking“, in IHP SiGe 0.25 µm BiCMOS technology ", ICECS – IEEE International Conference on Electronics, Circuits and System, Young Professionals/PhD Forum, 2014