Kapitel 1

Einleitung

1.1 Motivation

Das *Internet of Things* (IoT) und die Industrie 4.0 sind anhaltende Themen sowohl in der aktuellen Forschung als auch beim Ausbau und der Weiterentwicklung neuer Kommunikationsstandards. Sogenannte Wake-Up-Empfänger liegen dabei verstärkt im Fokus des wissenschaftlichen Interesses. Für die drahtlose Anbindung mobiler Sensorknoten sowie sogenannter intelligenter Objekte an das IoT stellen sie eine Schlüsseltechnologie dar. Wake-Up-Empfänger sollen einen raschen Verbindungsaufbau mit möglichst kurzen Antwortzeiten und möglichst langen Betriebszeiten bei gleichzeitig langen Wartungsintervallen ermöglichen.

Typischerweise werden dabei Sensorwerte, Aktorbefehle oder Statusabfragen selten – d.h. höchstens alle paar Minuten – und ereignisbasiert – also unregelmäßig und nicht in festen Zeitintervallen – abgefragt oder übermittelt. In beiden Fällen rüstet ein Wake-Up-Empfänger auf der Gegenseite einen sogenannten IoT-Knoten aus und muss den Nachrichtenkanal kontinuierlich auf Kommunikationsanfragen überwachen. Abbildung 1.1 zeigt die schematische Darstellung eines solchen Knotens mit typischen Komponenten.

Die hohe wirtschaftliche Relevanz dieser Technologie drückt sich unter anderem in der Berücksichtigung bei der Definition des neuen 5G-Mobilfunkstandards aus, bei dem *Massive Machine-Type Communication* (mMTC) und das IoT als eines von drei Hauptanwendungsfeldern von zukünftiger mobiler Kommunikation definiert werden. Die Mehrzahl der Verbindungen wird hier zwischen Maschinen und nicht zwischen Mensch

und Maschine erwartet. Das Datenvolumen zu übermittelnder Nachrichten (*payload*) liegt im Bereich nur einiger Byte bis maximal weniger Kilobyte.

Unterschieden wird zwischen Anwendungen, die lediglich eine Kurzstreckenverbindung (*short-range IoT*) benötigen und solchen, die großflächige Areale überspannen. Eine einfache Möglichkeit beide Szenarien abzudecken, stellt die Anbindung von lokalen Netzwerken mit kurzer Reichweite an die bestehende Wide-Area-Infrastruktur des Internets oder privater Netzwerke über Gateways dar. Folglich kann die drahtlose Mittel- und Kurzstrecken-Kommunikation aus Sicht der Endgeräte in den meisten Fällen als ausreichend betrachtet werden. Die Firma Ericsson prognostiziert entsprechend in ihrem Mobility-Report das größte Wachstum im IoT-Sektor bei den Kurzstrecken-Geräten [1]. Eine Übersicht der prognostizierten Endgeräte-Zahlen ist in Abbildung 1.2 dargestellt.

Zur drahtlosen Kommunikation stehen theoretisch Funk, Licht bzw. Infrarot, Ultraschall oder niederfrequente Nahfeldübertragung (NFC) zur Verfügung. Unter diesen Möglichkeiten bietet bei der geforderten Mobilität der Knoten allerdings allein Funk die spektrale, räumliche und zeitliche Kapazität, um moderne IoT-Anforderungen zu erfüllen.

1.1.1 Latenz und Verlustleistung

Da IoT-Knoten mobil und autonom sein müssen, lassen sich ihre wesentlichen Anforderungen auf ihre Kommunikationsschnittstelle übertragen. Als Energieversorgung kommen nur Batterien oder anwendungsspezifische Energie-Harvesting-Lösungen (EH-Lösungen) in Frage. Batterielose RFID-

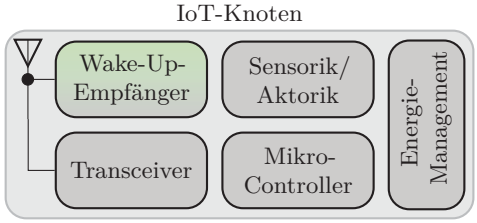


Abbildung 1.1: Aufbau eines IoT-Knotens mit typischen Komponenten und Wake-Up-Empfänger.

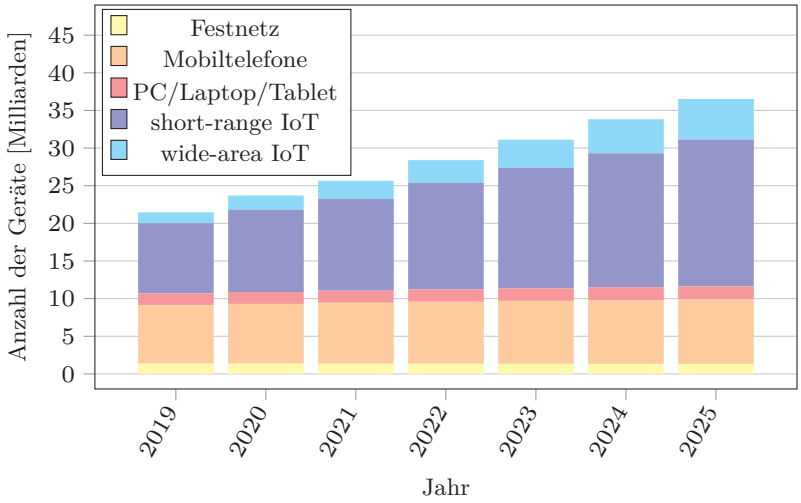
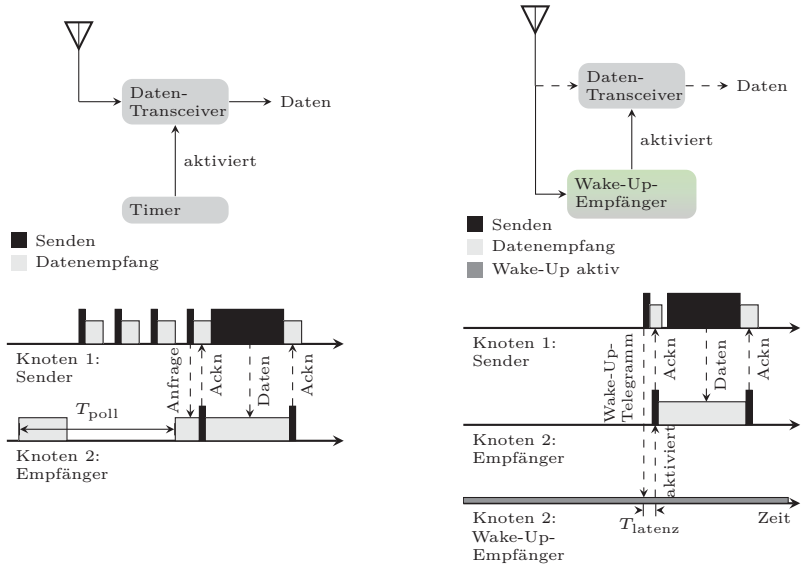


Abbildung 1.2: Marktanalyse und Prognose über Anzahl von vernetzen Geräten [1].

bzw. Backscatter-Lösungen als Konkurrenztechnologie haben dagegen den Nachteil, dass entsprechende Reader-Stationen nicht überall verfügbar sind. Ihr Einsatz erfordert durch ihre Größe und die üblichen Reichweiten von deutlich unter zehn Metern ggf. umfangreiche Umbauten in der gegebenen Infrastruktur. Auch die regelmäßige Belastung des Funkmediums mit bis zu zwei Watt Sendeleistung stellt eine deutliche Einschränkung hinsichtich der Koexistenz und Anzahl gleichzeitig addressierbarer Knoten dar.

Gerade im Kontext des prognostizierten hohen Volumens von IoT-Geräten erscheint ein regelmäßiger Batteriewechsel an hunderttausenden von Geräten unrealistisch oder gar unmöglich. Im Papier *5G-Strategie für Deutschland* des Bundesministeriums für Verkehr und digitale Infrastruktur wird daher eine „Batterielaufzeit vernetzter Sensoren von zehn Jahren und mehr“ gefordert [2].

Zur Realisierung solcher Laufzeiten aus begrenztem Energievorrat wie einer Batterie, werden im Ansatz ohne Wake-Up-Empfänger die geringen Aktivitäts- und Datenraten in den genannten Szenarios ausgenutzt. Der Empfänger wird zu einem Großteil der Zeit in einen Schlafmodus versetzt. Er wird zyklisch für nur einige Millisekunden eingeschaltet, um auf potentielle Nachrichten zu lauschen. Sofern keine Nachricht empfangen wurde,



(a) Zeitbasiertes Rendezvous-Schema. **(b)** Rendezvous-Schema mit zusätzlichem Wake-Up-Empfänger.

Abbildung 1.3: Rendezvous-Schemata: Konzepte zur Kommunikationseinleitung [4].

kehrt der Empfänger in den Schlafmodus zurück, um nach dem Ablauf einiger Sekunden erneut zu lauschen. Der Arbeitszyklus zwischen Aktivität und Schlafmodus (Tastverhältnis bzw. *Duty Cycle*) wird so auf ein Verhältnis von etwa $1/1000$ bis $1/10\,000$ eingeschränkt. Ist dem Transmitter der Einschaltzeitpunkt des Empfängers nicht bekannt, muss er seine Anfragen so oft verschicken, bis er vom Empfänger eine Bestätigung (*Acknowledge*, kurz Ackn.) erhält. In der Literatur wird dieses Verfahren als pseudo-asynchrones oder transmitter-initiiertes Rendezvous bezeichnet [3]. Ein Schema dieses Verfahrens ist in Abbildung 1.3a dargestellt.

Werden die Sende- und Empfangszeitpunkte dagegen synchronisiert, können die unnötigen Kommunikationsanfragen an den Empfänger entfallen. Die andernfalls bei vergeblichen Sendeversuchen verschwendete Energie wird eingespart. Allerdings macht dies eine regelmäßige Synchronisation der Uhren bei Sender und Empfänger erforderlich, die ansonsten auseinanderdriften. Das synchrone Verfahren spart Energie sowohl auf Sender- als auch auf Empfängerseite. Jedoch ist dadurch in dem System eine

Totzeit (Latenz) eingeführt, durch die Nachrichten höchstens alle paar Sekunden – oder unter sehr strengem Energie-Budget nur alle paar Minuten – übermittelt werden können [5]. Wichtig ist die Feststellung, dass die Reduktion der Latenz mit einer Erhöhung der Verlustleistung einhergeht. Niedrige Latenz und niedrige Verlustleistung sind im allgemeinen nicht gleichzeitig zu erreichen.

In Anwendungen, bei denen Anfragen quasi in Echtzeit bedient werden müssen, sind derartige Verzögerungen nicht tolerierbar. Auch bei Systemen, die eine Nutzerinteraktion erfordern (*Human Machine Interface* (HMI)), ist auf Latenzen im Bereich unter 100 ms zu achten. Grundsätzlich gilt in diesen Fällen, dass der Zeitpunkt der Kommunikationsanfrage unbekannt ist, aber innerhalb weniger Millisekunden darauf reagiert werden muss.

Wake-Up-Empfänger lösen den Kompromiss aus Latenz und Verlustleistung auf. Durch verschiedene schaltungs- oder systemtechnische Ansätze können niedrige Verlustleistungen im Mikrowattbereich realisiert werden, ohne dass eine erhöhte Latenz in Kauf genommen werden muss. Die verschiedenen Techniken werden im Abschnitt 2.4 (Stand der Technik) bzw. bei der Diskussion des Lögungsvorschlags in dieser Arbeit (Kapitel 3) vorgestellt und verglichen.

Abbildung 1.3b zeigt das Rendezvous-Schema zwischen Nachrichtenquelle und -senke, sofern der Empfangsknoten mit einem Wake-Up-Empfänger ausgestattet ist. Die Kommunikationsanfrage (im Folgenden Wake-Up-Telegramm) wird vom Wake-Up-Empfänger empfangen und ausgewertet. Daraufhin aktiviert er den im Schlafmodus befindlichen Datenempfänger, der eine Bestätigung über seine Empfangsbereitschaft an den Sender schickt. Die Kommunikation ist eingeleitet und kann abgewickelt werden. Dieses Verfahren ermöglicht, den Energieverbrauch in einem drahtlosen Sensornetzwerk (WSN) deutlich zu reduzieren [6]. Als Latenz T_{latenz} wird im Folgenden die Zeit vom Aussenden des ersten Bits eines Wake-Up-Telegramms bis zum Auslösen des Aktivierungs-Signals im Wake-Up-Empfänger definiert, wie in Abb. 1.3b illustriert.

Wake-Up-Empfänger sind somit ein entscheidendes Element für IoT-Anwendungen mit hohen Anforderungen an die Reaktionszeit! Einige dieser Anwendungen werden im nächsten Abschnitt beschrieben.

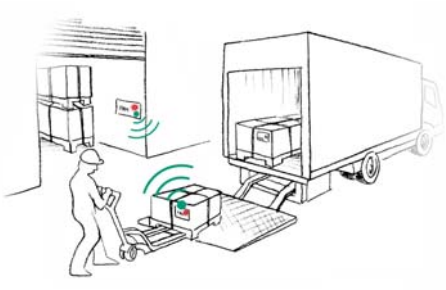
1.1.2 Anwendungsfelder

Logistik

Im Anwendungsfeld der Logistik könnte sich ein mit einer IoT-Schnittstelle ausgerüstetes intelligentes Objekt durch ein räumlich begrenztes stationäres Funkfeuer bewegen. Sofern das besagte Funkfeuer einen Gebäude- oder Lagerhallenzugang ausleuchtet, kann das Objekt so selbstständig den Durchgang erkennen und eine vorprogrammierte Aktion einleiten: Im Falle einer angestrebten Diebstahlsicherung zum Beispiel unmittelbar einen Alarm auslösen. In einem solchen Fall einfacher Fernsteuerung oder ereignisbasierter Aktorik (Alarm) kann der Transceiver auf dem Knoten (Abb. 1.1) weggelassen werden. Dieses Szenario macht insbesondere eine robuste Datenübertragung mit *Forward Error Correction* (FEC) erforderlich.

Verwendet man anstelle einer einfachen Funkbake dagegen ein Gateway mit Rückkanal, besteht die Möglichkeit, für eine Tracking-Operation weitere Kommunikationsprotokolle zu aktivieren und beispielsweise ein Logistik-System automatisch über seine Ankunft zu informieren. In Konkurrenz dazu stehen kommerziell etablierte Technologien wie Barcode- oder RFID-Reader. Jedoch sind diese Systeme aufgrund ihrer geringen bis mäßigen Reichweite in ihrer Flexibilität eingeschränkt. Sie bieten lediglich die Möglichkeit, die Zu- und Abgänge von Objekten zu erfassen. IoT-Lösungen erlauben dagegen alle vorhandenen Objekte innerhalb eines vom Gateway ausgeleuchteten Bereichs abzufragen, Statusinformationen abzurufen oder Steuerbefehle auszulösen. So könnte ein entsprechend ausgestatteter Knoten auf Anfrage ein Lichtzeichen geben. In dieser als *Pick-by-Light* bezeichneten Anwendung können gesuchte Objekte innerhalb von großen Arealen oder Regalkomplexen mit einer Vielzahl von Lagergegenständen noch schneller und einfacher gefunden werden.

Darüber hinaus ist ein solches System leicht skalierbar, indem beispielsweise die Anzahl der Gateways und somit Größe des erfassten Bereichs erhöht wird, in welchem sich mit IoT-Knoten ausgestattete Objekte adressieren lassen. Die Überwachung großer Lagerhallen-Komplexe oder freier Logistik-Areale, bei denen die Gateways in regelmäßigen Abständen an der Decke oder an Laternenmasten angebracht sind, ist somit denkbar. Einige der beschriebenen Beispiel-Szenarien sind in den Abbildungen 1.4 illustriert.



(a) Geo-Fencing

(b) Objekt-Suche

(c) Pick-by-light

Abbildung 1.4: Illustration von Anwendungs-Szenarios für IoT-Knoten [7].

Üblicherweise ist in logistischen Anwendungen mit einer dynamischen Netzwerk-Struktur zu rechnen. Das bedeutet, dass aus Sicht eines lokalen Netzwerkes (z. B. bei einem Umschlagplatz) einzelne Knoten das Netzwerk ständig, aber unregelmäßig, betreten oder verlassen. Synchrone oder pseudo-asynchrone Netzwerke, wie die zuvor beschriebenen, müssten bei jedem dieser Zugänge sicherstellen, dass die Uhr des neu ankommenden Knotens einsynchronisiert wird, was zu übermäßiger Kanalbelegung ohne echten Datenaustausch führt und am Energievorrat der Knoten zehrt.

Ein auf geringe Antwortzeit, hohe Lebensdauer und Adressierbarkeit hin ausgelegter Wake-Up-Empfänger löst diese Schwierigkeiten [8]. Gegenüber einem synchron ausgelegten Netzwerk kann die mittlere Leistungsaufnahme pro empfangenem Datenpaket durch einen Wake-Up-Empfänger mehr als halbiert werden [9, S. 16ff]. Ist durch den Wake-Up-Empfänger die Möglichkeit von gruppenweiser oder individueller Adressierung gege-

ben, reduziert dies das Datenaufkommen auf dem Kommunikationskanal, indem nur angesprochene Knoten aktiviert werden und antworten. Hierdurch wird gleichermaßen die Wahrscheinlichkeit von Datenkollisionen reduziert, als auch unnötiger Stromverbrauch bei Knoten vermieden, die nicht gemeint sind.

Multihop-Netzwerke

Ist eine hochvolumige Installation von Gateways nicht möglich oder wünschenswert, besteht die Möglichkeit, das Netzwerk als Multihop-Netzwerk auszuführen. Auf diese Weise können Netzwerke aufgespannt werden, die die intrinsische Reichweite einzelner Knoten überschreiten. Hierzu werden zur Überbrückung der Strecke weitere Knoten als Relais eingesetzt. Gleichsam ist es auch möglich, die Reichweite eines Knotens bewusst einzuschränken, indem seine Sendeleistung (z. B. auf $-10\,\mathrm{dBm}$) reduziert wird und so unter bestimmten Umständen im gesamten Netzwerk Energie zu sparen [10].

Da diese Netzwerkstruktur ein ständiges Überwachen des Kommunikationskanals auf potentiell weiterzuleitende Nachrichten notwendig macht, profitieren Multihop-Netzwerke in vielfacher Hinsicht vom Einsatz von Wake-Up-Empfängern [11]. Durch die Möglichkeit einer rein asynchronen Nachrichtenabwicklung kann auch hier der Mehraufwand zur ständigen Synchronisation des Netzwerks vollkommen entfallen. Wie im vorherigen Abschnitt beschrieben, wird der Energieaufwand für das Lauschen reduziert, ohne dass die Latenz nennenswert ansteigt. Dies wirkt sich positiv auf die Gesamt-Übermittlungsdauer zwischen Ursprungs- und Zielknoten aus. Zu deren Ermittlung muss die Anzahl der nötigen Sprünge (Hops) mit der (durchschnittlichen) Latenz zwischen den verwendeten Relais-Knoten multipliziert werden. Insbesondere große Netzwerke mit einer hohen Anzahl von Knoten profitieren hiervon. Der Energiebedarf pro Knoten bleibt konstant, während er beim synchronen Netzwerk linear mit der Anzahl der Knoten wächst [12].

Anwendungen für solche Sensornetze sind beispielsweise in der Land- und Forstwirtschaft zu finden, wo Umwelt- oder Wachstumsparameter abgefragt werden sollen, aber keine Infrastruktur vorhanden ist, um eine entsprechende Zahl von Gateways zu installieren.

1.2 Anforderungen

Aus den beschriebenen Anwendungsszenarios lassen sich die spezifischen Anforderungen an den Wake-Up-Empfänger ableiten, die in diesem Abschnitt definiert werden sollen. Die betrachteten Schlüsselparameter sind Empfänger-Empfindlichkeit, Formfaktor, Lebensdauer bzw. Leistungsaufnahme, Störfestigkeit, Frequenz-Diversität und der Kostenfaktor, die sich alle in gegenseitiger Abhängigkeit zueinander befinden.

Frequenz-Diversität

Angesichts des in Abbildung 1.2 beschriebenen Wachstums ist es vorteilhaft einen Empfänger vorzusehen, welcher agil – d.h. ohne Rekonfiguration der Hardware – in verschiedenen Frequenzbereichen eingesetzt werden kann. Auf diese Weise können Datenpakete und Wake-Up-Nachrichten auf das verfügbare Spektrum aufgeteilt werden. Die Anzahl der IoT-Knoten innerhalb eines Netzwerks und die Datensicherheit profitieren davon, dass nicht alle Teilnehmer den gleichen Frequenzbereich nutzen, da die Wahrscheinlichkeit von Paket-Kollisionen bei gleichzeitiger Übertragung reduziert wird. Darüber hinaus kann unter schwierigen Ausbreitungsbedingungen bei Mehrfrequenz-Aussendung die erforderliche Empfindlichkeit des Empfängers reduziert werden (vgl. Abschnitt 6.3).

In Deutschland und Europa sind die ISM-Bänder bei 433 MHz und 868 MHz von Interesse. Für einen internationalen Gebrauch (z. B. bei global versendeten Gütern) kommen beispielsweise die Bänder bei 784 MHz, 902 MHz – 928 MHz und 960 MHz für Amerika, Australien und Asien hinzu. Dagegen ist die Kurzstrecken-Kommunikation bei 2,4 GHz und 5 GHz weltweit lizenzfrei gestattet. Allerdings sind diese Bänder durch privaten Internet-Konsum über Wi-Fi sehr stark belastet, was einen störungsfreien Betrieb erschwert. Die Reichweiten sind durch höhere Pfadverluste deutlich eingeschränkt, auch wenn innerhalb der Bänder deutlich mehr Bandbreite zur Verfügung steht.

Die Forderung an Frequenz-Diversität beeinflusst den Formfaktor üblicherweise insofern, als dass die Zahl externer Komponenten stark ansteigt, um mit Schaltern und Filtern hoher Güte die gewünschten Frequenzbänder auszuwählen.

Formfaktor

Um die Anforderungen hinsichtlich Mobilität und Knotendichte bzw. Skalierbarkeit der Knotenanzahl zu bedienen, ist es erforderlich, dass einzelne IoT-Knoten möglichst klein sind. Um beispielsweise als Etikettierung (*tag*) oder Statussensor auch an kleine Objekte, z. B. Werkzeuge oder Gegenstände des täglichen Gebrauchs wie Autoschlüssel etc. angebracht zu werden, sollte die Bauform des Knotens so klein wie möglich sein und je nach Anwendung eine Platinengröße von $1\,\mathrm{cm}^2 - 4\,\mathrm{cm}^2$ nicht überschreiten. Erforderliche Komponenten auf dem Knoten sind gemäß Abbildung 1.1 die Energieversorgung inklusive eventueller Regelungsschaltungen und Wandler, ein Mikrocontroller, ein Transceiver, der Wake-Up-Empfänger, eine Antenne, und ggf. Sensorik- und/oder Aktorik-Komponenten. Darüber hinaus sind je nach Ausführung noch Komponenten zur HF-Anpassung und Filter-Elemente – z. B. *Surface Acoustic Wave* (SAW) – sowie Schalter zur Frequenzselektion notwendig.

Ein typisches SAW-Filter für das deutsche 868-MHz-ISM-Band ist das Epcos B3717 mit einer 3-dB-Bandbreite von 7 MHz und Abmessungen von $3 \times 3\,\mathrm{mm}^2$. Antennen können abhängig von Antennengewinn und Frequenzbereich als *Sourface Mounted Device* (SMD-Bauteil), gedrucktes Element oder geschraubte Drahtantenne ausgeführt werden. Um den Anforderungen an den Formfaktor mit Blick auf die Antennenbauformen gerecht zu werden, sind Frequenzen über 300 MHz vorzuziehen.

Batterielösungen sind grundsätzlich bereits ab Spannungen von 1,2 V und aufwärts verfügbar. Achtet man jedoch für eine lange Lebensdauer auf geringe Selbstentladung von ein bis zwei Prozent und hohe Energiedichte, schränkt sich die Auswahl für kleine Packungsgrößen im Wesentlichen auf lithiumbasierte Zellen mit einer Nennspannung zwischen 2,5 V – 4,2 V ein [13]. Eine Übersicht verschiedener Energieversorgungsmöglichkeiten befindet sich für *Energy Harvester* (EH) und in Frage kommende Batterieformen in den Tabellen 1.1 und 1.2. Die Einträge wurden so ausgewählt, dass IoT-Knoten mit Abmessungen kleiner oder gleich $2 \times 2\,\mathrm{cm}^2$ realisiert werden können.

Verlustleistung, Stromaufnahme und Lebensdauer

Durch den allgemeinen Trend integrierte Schaltungen in immer kleineren kleineren Technologieknoten zu fertigen, nehmen auch die Betriebsspan-