



Detektiv für Funk-Kamerasysteme und WLAN-Sender

Aufgespürt – 2,45-GHz-Detektor

Funk-Kamerasysteme, WLAN-Netze, Bluetooth-Geräte, A/V-Sender u. a. arbeiten auf unterschiedlichen Frequenzen und mit unterschiedlichen Modulationsverfahren im lizenzfreien ISM-2400-Frequenzband. Der 2,45-GHz-Detektor ist ein mobiles Hand-Gerät zum Detektieren solcher Sender und ihres Standortes.

Finden und orten

Das 2,4-GHz-Band umfasst den Frequenzbereich von 2,400 bis 2,4835 GHz, es ist von der ITU als sogenanntes ISM-Band für die lizenzfreie Nutzung durch Short Range Devices (SRD, Funksender geringer Leistung) freigegeben. Der Name ISM (Industrial Scientific and Medical) sagt es: dieses Frequenzband kann durch ganz unterschiedliche Anwendungen belegt werden.

Die Lizenzfreiheit der hier betriebenen Funkgeräte besagt zwar, dass jeder, ohne eine Funklizenz zu beantragen, mit diesen Geräten arbeiten kann, allerdings ist die technische Konzeption der Sende- und Empfangsgeräte einigen Konventionen unterworfen. So dürfen je nach Geräteart bestimmte HF-Leistungen nicht überschritten werden, andere Systeme

wie WLAN oder Bluetooth unterliegen besonderen Normungen, um die Zusammenarbeit von Geräten unterschiedlicher Hersteller zu gewährleisten und die Nutzung des zugewiesenen Frequenzbereiches effektiv zu gestalten.

Leider hat die allgemein freigegebene Nutzung solcher Bänder vor allem einen Haken – die Anzahl der Kanäle ist naturgemäß begrenzt und so sind gegenseitige Störungen, wenn vielleicht auch nur kurzzeitig, weil einige Systeme mit Frequenzhopping arbeiten, trotz nominell geringer Reichweiten vorprogrammiert. Ein A/V-Sendesystem ist also kaum ununterbrochen störungsfrei zu betreiben, wenn man im Empfangsbereich des A/V-Empfängers ein Bluetooth-Handy betreibt oder gar ein WLAN im gleichen Haus nutzt.

Und die geringe Leistung sowie die hohe Frequenz haben auch dazu geführt, dass die Sende- und Empfangstechnik immer kompakter wird. Abbildung 1 zeigt drei Beispiele dafür. Die Kompaktheit führt allerdings auch zu negativen Erscheinungen – kleine Spionage-Funk-Kameras mit integriertem Sender sind heute nahezu überall völlig unauffällig unterzubringen. Geringe Stromaufnahmen ermöglichen sogar lang andauernden Batteriebetrieb. Betreibt man solche Systeme ohne Kenntnis des Beobachteten, so ist das schon einmal strafbar. Dazu kommt, dass im Falle der A/V-Systeme jeder, der einen A/V-Empfänger besitzt, mithören und mitsehen kann. Wie unangenehm so etwas werden kann, ist immer

Technische Daten: DET 245

Spannungsversorgung:	9-V-Blockbatterie 6LR61
Frequenz:	2,45 GHz
Stromaufnahme:	60 mA
Freifeldreichweite:	bis 5 m



Bild 1: 2,4-GHz-Sendesysteme sind extrem kompakt realisierbar und somit auch gut unauffällig zu installieren. Links ein komplettes Mini-Kamera-Sendersystem, rechts ein Mini-WLAN-Sender, in der Mitte ein Bluetooth-Stick, der sogar noch einen Speicherkartenleser enthält. Besonders Geräten wie letzterem Bluetooth-Stick sieht man seine Hauptfunktion zunächst nicht an.

wieder einmal in TV-Magazinsendungen zu sehen, wenn sich TV-Teams aufmachen, heimlich installierte Sender in Läden, Sonnenstudios oder Hotelzimmern zu orten und Beobachtete wie Beobachter damit zu konfrontieren.

Die kleinen, tragbaren Empfänger sind zwar gut zur allgemeinen Ortung von A/V-Systemen geeignet, können den direkten Senderstandort allerdings nicht punktgenau anpeilen.

Dies und die angestrebte universelle Einsetzbarkeit für alle ISM-Dienste bedingen ein Messgerät, mit dem der Sender möglichst punktgenau geortet werden kann. Das muss nicht extrem empfindlich in Bezug auf Empfangsreichweite sein, aber über eine möglichst hohe Richtwirkung verfügen, um tatsächlich punktgenau einen Sender finden zu können und nicht etwa einen anderen im Nachbarhaus damit anzupeilen.

Die Anwendung eines solchen Gerätes kann vielfältig sein – es kann zur Störungssuche genauso eingesetzt werden wie zum Optimieren und Abstimmen verschiedener 2,45-GHz-Systeme, aber auch zur o. a. Suche nach versteckten Sendern.

Es ist auch sehr nützlich für das Aufspüren verbotenerweise eingesetzter WLAN- und Bluetooth-Geräte in Betrieben, denn deren Einsatz ist im Allgemeinen streng reglementiert, um die Daten- und Kommunikationssicherheit in einer Firma zu gewährleisten. Ein unerlaubter, offener WLAN-Port kann fatale Folgen für die Datensicherheit haben!

Unser hier vorgestellter 2,45-GHz-Detektor kann genau diese Aufgaben erfüllen. Er verfügt über eine sehr wirksame Richtantenne, die Feldstärkeanzeige erfolgt sowohl optisch als auch akustisch.

Durch die extrem einfache Bedienung ist die Nutzung des Gerätes für jedermann möglich.

Funktion

Um die exakte Position einer Signalquelle mit dem 2,45-GHz-Detektor aufzuspüren, ist eine Antenne mit einem gutem Vor-Rück-Verhältnis und hoher Richtwirkung erforderlich. Aus diesen Gründen kommt hier eine Patch-Antenne zum Einsatz. Eine solche Patch-Antenne ist sehr einfach aufzubauen und kostengünstig zu produzieren. Sie besteht lediglich aus einer doppelseitigen Platine. Abbildung 2 zeigt die verwendete Patch-Antenne des 2,45-GHz-Detektors mit einem beispielhaften Richtdiagramm.

Abbildung 3 zeigt das Blockschaltbild des 2,45-GHz-Detektors.

Das Empfangssignal gelangt über die Patch-Antenne zum Front-End-Filter. Das Filter dient zur Selektion des Frequenzbandes ISM 2400. Anschließend gelangt das gefilterte Eingangssignal zum HF-Detektor. Er wandelt das Eingangssignal in eine Gleichspannung um. Diese gelangt dann zum Mikrocontroller, der eine Analog-Digital-Wandlung mit anschließender Auswertung des Daten-Signals vornimmt. Der Mikrocontroller steuert den LED-Bargraph, bestehend aus den 9 Leuchtdioden, entsprechend der Signalstärke des Empfangssignals an. Zusätzlich wird ein Signalgeber mit dem Mikrocontroller angesteuert, der ebenfalls je nach Empfangssignal-Stärke unterschiedliche Töne erzeugt. Somit gibt es eine

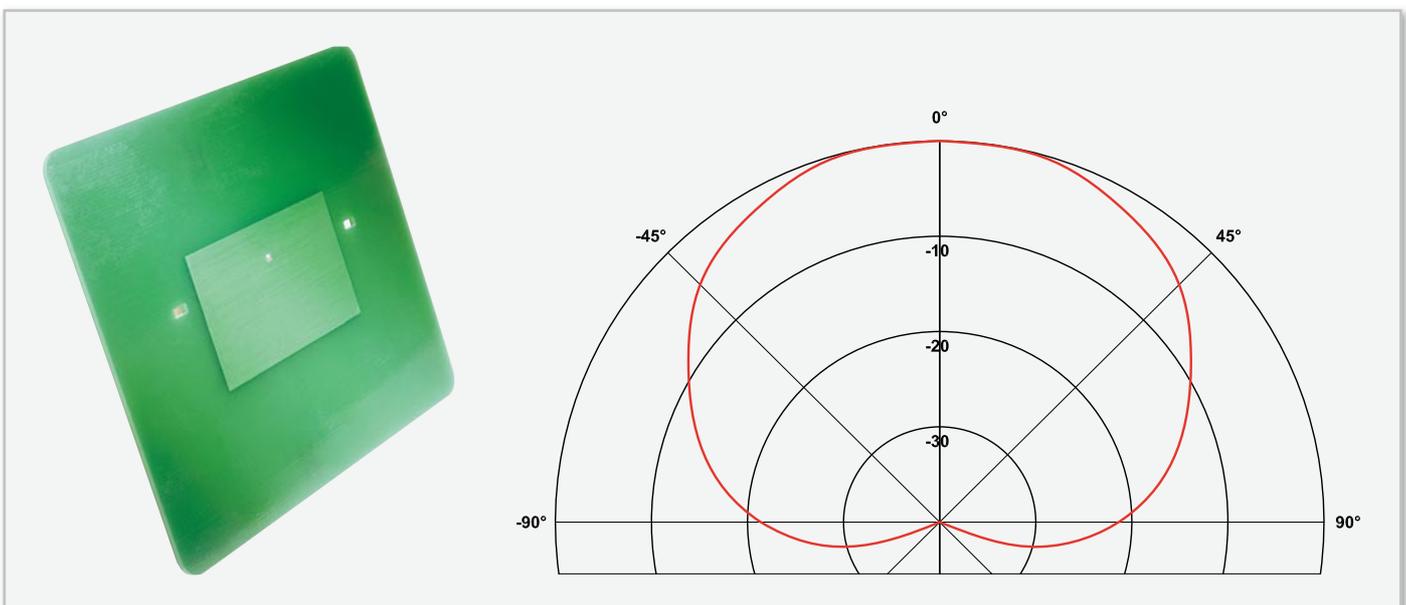


Bild 2: Patch-Antenne mit beispielhaftem Richtdiagramm

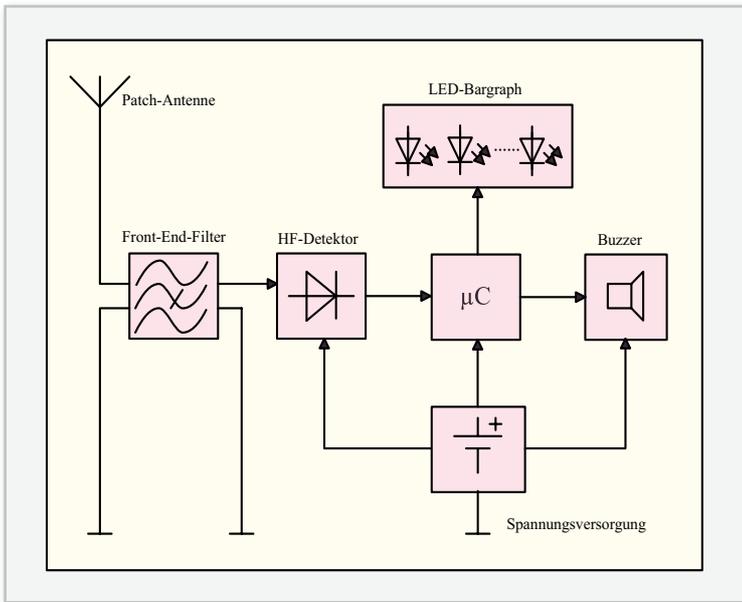


Bild 3: Blockschaltbild des 2,45-GHz-Detektors

optische und akustische Anzeige, ob und wie stark ein Signal empfangen wird. Je höher der empfangene Signalpegel, desto mehr Leuchtdioden werden vom Mikrocontroller angesteuert und umso höher ist der hörbare Ton des Signalgebers.

Die Batteriespannung des Gerätes wird mit einem Spannungsregler stabilisiert, um eine konstante Funktion über den gesamten nutzbaren Batteriespannungsbereich zu gewährleisten.

Schaltungsbeschreibung

Die Schaltung (Abbildung 4) wird mit einer 9-V-Blockbatterie BAT 1 betrieben. Der Spannungsregler IC 3 stabilisiert die Batteriespannung auf 3 V. Die Kondensatoren C 11 bis C 14 dienen zur Unterdrückung der Schwingneigung des Spannungsreglers.

Mit dem On-Taster TA 1 wird das Gerät eingeschaltet. Das bedeutet, dass das Gerät nur so lange in Betrieb ist, wie der Taster gedrückt und gehalten wird. Die Diode D 11 dient als Verpolungsschutz und der Widerstand R 14 als Sicherungselement. Die Leuchtdiode D 12 dient in Verbindung mit dem Vorwiderstand R 15 als Betriebsanzeige.

Fast die gesamte Schaltung wird mit der stabilisierten Betriebsspannung von 3 V versorgt. Ausgenommen ist der Signalgeber PZ 1. Er wird direkt mit der 9-V-Batteriespannung versorgt, um eine maximale Lautstärke zu erreichen.

Das Eingangssignal gelangt über die Patch-Antenne zum

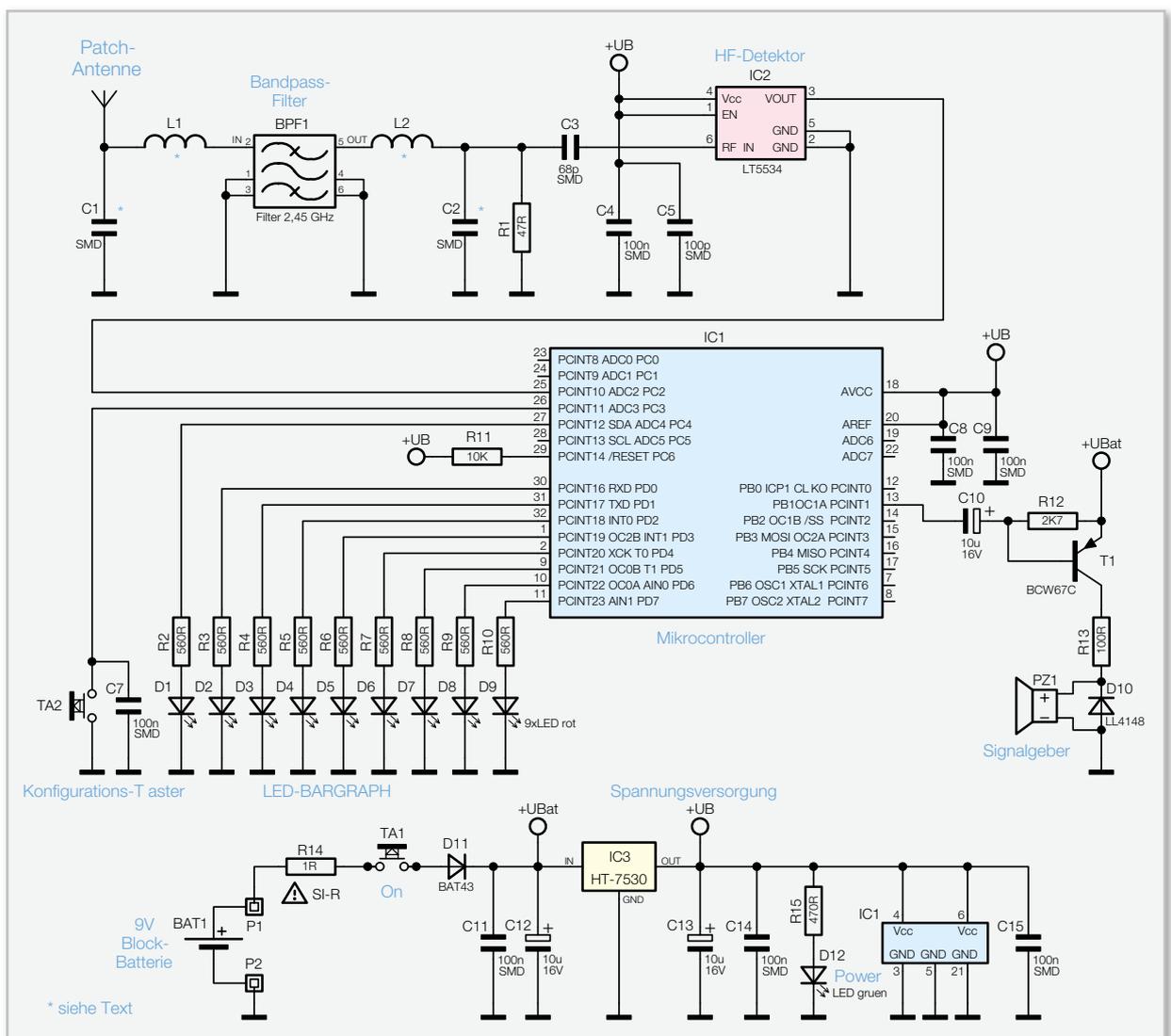
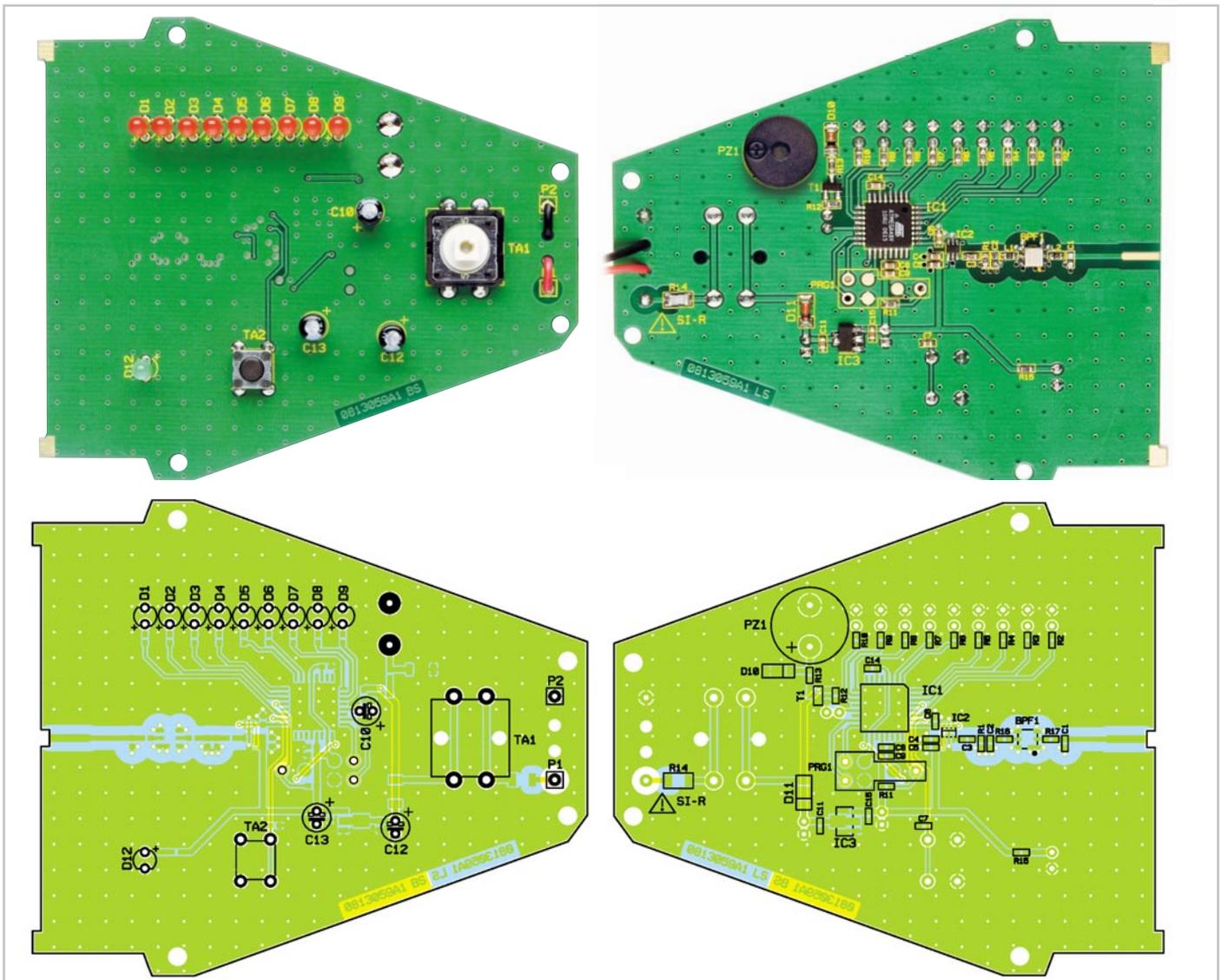


Bild 4: Schaltbild des 2,45-GHz-Detektors



Ansicht der fertig bestückten Platine des DET 245 mit zugehörigem Bestückungsplan, links von der Bestückungsseite, rechts von der Lötseite

Bandpassfilter BPF 1. Das Filter hat eine 3-dB-Bandbreite von 100 MHz und selektiert somit das gesamte Frequenz-Band von 2400 MHz bis 2484 MHz (ISM 2400).

Nach der Filterung wird das Signal dem HF-Detektor IC 2 zugeführt. Er wandelt das HF-Signal in eine Gleichspannung um. Dabei ist die Höhe der Gleichspannung abhängig vom Leistungspegel des HF-Signals. Die Induktivitäten L 1, L 2 und die Kondensatoren C 1, C 2 dienen zur Anpassung der Antenne und des HF-Detektors IC 2 an das Bandpassfilter BPF 1. Da die Patch-Antenne für eine Eingangsimpedanz von 50Ω ausgelegt ist und das Bandpassfilter BPF 1 ebenfalls eine Ein- und Ausgangsimpedanz von 50Ω hat, konnte auf eine Anpassung an dieser Stelle verzichtet werden. Das bedeutet, die Kondensatoren C 1 und C 2 sind nicht bestückt und die Induktivitäten L 1 und L 2 werden durch $0\text{-}\Omega$ -Widerstände ersetzt. Der Widerstand R 1 ist das einzige Anpass-Element und verbessert die Rückflusdämpfung des HF-Detektors um ca. 10 dB. Die Kondensatoren C 4 und C 5 dienen zum Abblocken der Betriebsspannung des HF-Detektors IC 2.

Der 8-Bit-Mikrocontroller IC 1 von Atmel übernimmt die Auswertung des Ausgangssignals VOUT des HF-Detektors IC 2. Er wandelt mit Hilfe seines internen 10-Bit-Analog-Digital-Wandlers ADC2 die analoge Gleichspannung in ein digitales

Datenwort. Nach der Auswertung des Datenwortes werden dann die entsprechenden Leuchtdioden D 1 bis D 9 über die Ports PC 4 und PD 0 bis PD 7 angesteuert. Die Widerstände R 2 bis R 10 dienen zur Strombegrenzung der Leuchtdioden. Zusätzlich wird mit dem Port PB 1 über den Transistor T 1 der Signalgeber PZ 1 angesteuert. Der Transistor dient dabei in Verbindung mit dem Widerstand R 12 als Treiber für den Signalgeber PZ 1. Je nach Stärke des Eingangssignals wird eine Frequenz zwischen 40 Hz und 500 Hz erzeugt.

Der Widerstand R 11 sorgt für einen definierten Reset des Mikrocontrollers IC 1 beim Zuschalten der Betriebsspannung. Um eine optimale Performance des 2,45-GHz-Detektors zu erreichen, ist eine Einstellung der Empfindlichkeits-Schwelle erforderlich. Diese wird bei der ersten Inbetriebnahme mit dem Taster TA 2 durchgeführt (siehe Bedienung/Abgleich).

Nachbau

Alle SMD-Bauteile sind bereits bei der Auslieferung des Bauesatzes bestückt. Es müssen lediglich die bedrahteten Bauteile eingelötet werden. Dazu zählen drei Kondensatoren, Elkos, ein Taster, der Signalgeber, 10 Leuchtdioden, ein Lötnagel

Stückliste: 2,45-GHz-Detektor DET 245

Widerstände:

0 Ω /SMD/0603	R16, R17
Sicherungswiderstand 1 Ω /SMD/1206	R14
47 Ω /1 %/SMD/0603	R1
100 Ω /1 %/SMD/0603	R13
470 Ω /1 %/SMD/0603	R15
560 Ω /1 %/SMD/0603	R2–R10
2,7 k Ω /1 %/SMD/0603	R12
10 k Ω /1 %/SMD/0603	R11

Kondensatoren:

68 pF/SMD/0603	C3
100 pF/SMD/0603	C5
100 nF/SMD/0603	C4, C7–C9, C11, C14, C15
10 μ F/16 V	C10, C12, C13

Halbleiter:

ELV07716/SMD	IC1
LT5534/SMD/Linear	IC2
HT7530/SMD	IC3
BCW67C/SMD	T1
LL4148	D10
BAT43/SMD	D11
LED, 3 mm, Rot	D1–D9
LED, 3 mm, Grün	D12

Sonstiges:

OFW B4041/SMD	BPF1
Mini-Drucktaster, B3F-4050, 1 x ein	TA1
Tastkappe, 10 mm, Grau	TA1
Mini-Drucktaster, 1 x ein, 1 mm Tastknopflänge	TA2
Sound-Transducer, 3 V, print	PZ1
9-V-Batterieclip	BAT1
1 Lötstift, 1 mm	
4 Kunststoffschrauben, 2,5 x 5 mm	
2 Schaumstoffstücke, 30 x 15 x 10 mm, selbstklebend	
1 Antennenaufkleber, bedruckt, Weiß	
1 Frontplatte, bearbeitet und bedruckt	
1 Klebeband, doppelseitig, 90 x 90 mm	
1 Sensor-Gehäuse, komplett, bearbeitet und bedruckt, Grauweiß	

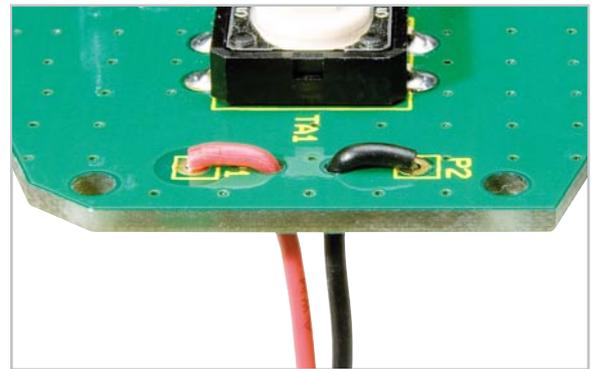


Bild 6: Basisplatte mit Batterieclip-Anschlüssen

und ein Batterieclip. Außerdem sind die Basisplatte und die Patch-Antenne miteinander zu verlöten. Alle Bauteile bis auf den Signalgeber und der Lötstift sind von der Platinenoberseite der Basisplatte zu bestücken und anschließend von der Unterseite zu verlöten. Bei den Elkos ist die Polung zu beachten. Die Bestückung der Leuchtdioden erfolgt in einem Abstand von 13 mm zur Platinenoberseite, siehe Abbildung 5. Die Leitungen des Batterieclips sind zunächst von der Unterseite der Basisplatte durch die Bohrung für die Zugentlastung zu führen und dann von der Unterseite zu verlöten, siehe Abbildung 6.

Bevor nun die komplett bestückte Basisplatte mit der Patch-Antenne verlötet werden kann, muss der Lötstift präpariert werden. Dazu ist der Lötstift von der Rückseite in die dafür vorgesehene Bohrung der Patch-Antenne zu stecken und so zu kürzen, dass er nicht mehr aus der Platine herausragt. Dann kann der Lötstift mit der Patch-Antenne verlötet werden. Anschließend ist die Patch-Antenne auf die Basisplatte zu schieben, so dass die beiden Platinen senkrecht zueinander stehen, und zu verlöten. Zum Schluss muss der Lötstift mit wenig Lötzinn auf die Leiterbahn der Basisplatte gelötet werden. Dabei ist zu beachten, dass der Lötstift flach auf der Leiterbahn aufliegt. Jetzt sind alle Lötarbeiten abgeschlossen. Als Nächstes ist der mitgelieferte Aufkleber direkt über das Patch der Antenne zu kleben. Die Position ist in Abbildung 7 gestrichelt angedeutet. Dies ist aufgrund der notwendigen ESD-Festigkeit (electrostatic discharge) erforderlich. Nun wird mit

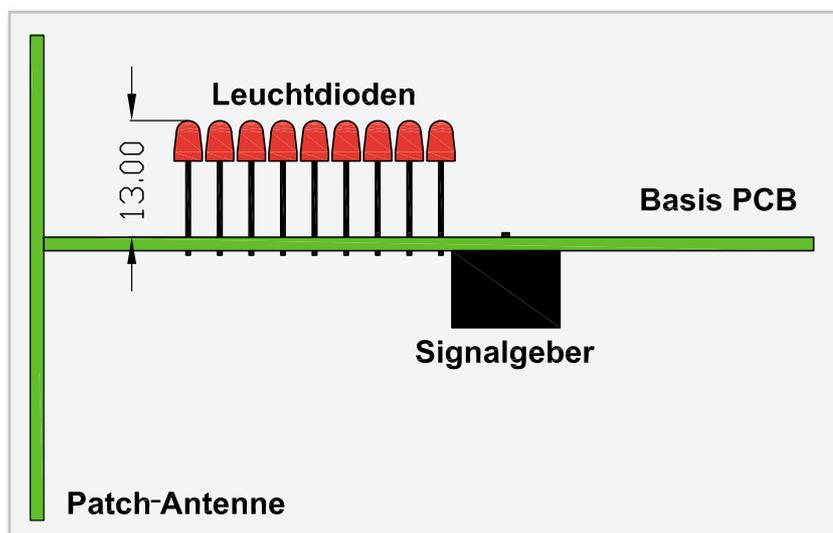


Bild 5: Seitenansicht der Basisplatte des 2,45-GHz-Detektors

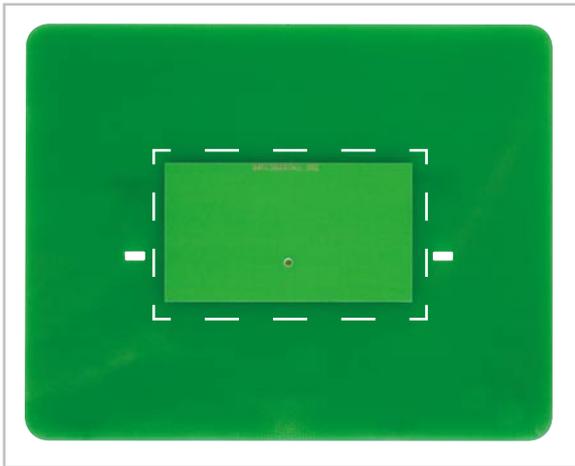


Bild 7: Patch-Antenne

dem mitgelieferten doppelseitigen Klebeband die Frontplatte in der Gehäuseoberschale befestigt. Dazu ist das Klebeband so zu positionieren, dass es keine Bohrungen überdeckt. Dies ist in Abbildung 8 schraffiert dargestellt. Daran anschließend ist die fertige Platinkombination mit den dazugehörigen Schrauben in der Gehäuseoberschale zu befestigen. Danach wird die Gehäuseunterschale mit der Gehäuseoberschale verschraubt. Anschließend erfolgt noch das Einkleben zweier Schaumstoffklebeteile in das Batteriefach und in den Batteriefachdeckel, um ein Verrutschen der Batterie zu verhindern. Zum Schluss ist eine 9-V-Batterie an den Batterieclip anzuschließen, der Batteriefachdeckel einzusetzen und zu verschrauben. Bild 9 zeigt das fertig aufgebaute Gerät.

Bedienung/Abgleich

Vor der Inbetriebnahme ist eine Einstellung der Empfindlichkeitsschwelle vorzunehmen, um eine hohe Empfindlichkeit und somit eine optimale Reichweite zum Aufspüren von ISM-Geräten zu erreichen. Dies ist erforderlich, um z. B. in Räumen mit einer hohen Deckenhöhe eine erfolgreiche Suche durchzuführen. Sollte diese Einstellung nicht vorgenommen werden, ist automatisch eine mittlere Empfindlichkeitsschwelle voreingestellt.

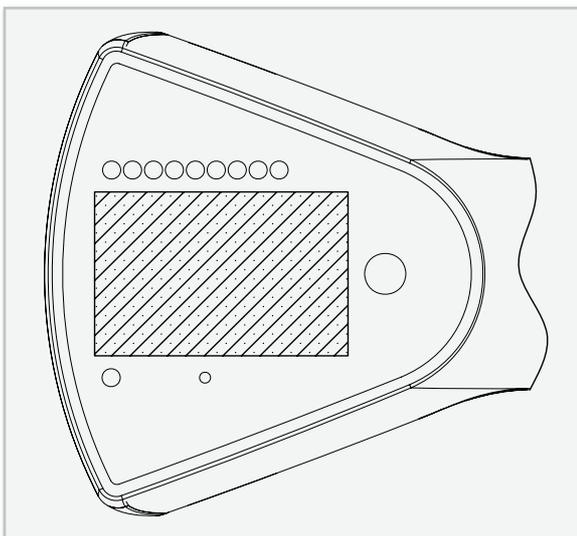


Bild 8: Gehäuseoberschale des 2,45-GHz-Detektors



Bild 9: Das fertig aufgebaute Gerät

Die Einstellung ist wie folgt durchzuführen:

- Mit einem dünnen Gegenstand, z. B. einer Büroklammer, den Taster TA 2 durch die dafür vorgesehene Bohrung in der Frontplatte gedrückt halten.
- Taster „On“ betätigen und ebenfalls gedrückt halten. Jetzt wird automatisch ein Leuchtdioden-Test durchgeführt, d. h., alle Leuchtdioden werden in Form eines Lauflichtes von unten nach oben hin angesteuert. Zusätzlich ertönt ein Ton vom Signalgeber. Anschließend beginnt der Einstellvorgang für die Empfindlichkeitsschwelle des Gerätes. Dazu werden die Leuchtdioden im Halbsekundentakt angesteuert. Das bedeutet, je mehr LEDs leuchten, desto empfindlicher ist der 2,45-GHz-Detektor. Die Bestätigung der gewünschten Empfindlichkeit erfolgt durch das Loslassen des Tasters TA 2. Ein Signalton bestätigt das Abspeichern der gewünschten Schwelle. Zusätzlich wird die eingestellte Empfindlichkeitsschwelle mit der entsprechenden Leuchtdiode signalisiert. Dies wird ebenfalls bei jeder Inbetriebnahme angezeigt.
- Taster „On“ loslassen

Nach dem Abgleich kann der 2,45-GHz-Detektor zum Einsatz kommen, um z. B. die besprochenen Funk-Kamerasysteme und bedingt auch WLAN-Router aufzuspüren.

Dazu ist, wie bei der Einstellung der Empfindlichkeitsschwelle, der Taster „On“ zu drücken und festzuhalten. Sobald man den Taster loslässt, schaltet sich das Gerät wieder aus. 9 rote Leuchtdioden zeigen im Betrieb die mit der Patch-Antenne empfangene relative Signalstärke an. Je mehr Leuchtdioden leuchten, desto stärker ist das empfangene Signal. Um die Anzeige besser beurteilen zu können, ist es erforderlich, sich mit dem Gerät sehr langsam zu bewegen. Sich dabei einmal um die eigene Achse zu drehen ist sehr hilfreich, um die Richtung eindeutig zu bestimmen. Eine akustische Anzeige unterstützt zusätzlich das Suchen der Geräte. Das bei geringer Feldstärke hörbare „Knattern“ verändert sich mit stärker werdender Signalstärke in einen Ton mit steigender Frequenz. Das unterstützt die visuelle Suche nach dem ertoteten Gerät.

ELV