Rolling-Code-Schaltsystem

Ein Wechselcodesystem erhöht die Sicherheit funkgesteuerter Schaltsysteme gegenüber solchen mit statischer Codierung erheblich. Insbesondere bei Zugangssteuerungen ist eine solche Wechselcodesteuerung von Bedeutung. Das Rolling-Code-Schaltsystem RCS100 besteht aus einem Zweikanal-Funk-Aufputzschalter und einem Zweikanal-Handsender, die verschlüsselt per Microchip-KEELOQ®-Rolling-Code miteinander kommunizieren. Dieses Verfahren gewährleistet eine besonders hohe Verschlüsselungssicherheit.

Clever geschaltet

Viele von uns benutzen schon seit Jahren ein Wechselcodesystem, teils ohne dies zu wissen – es ist der per Funk arbeitende Autoschlüssel vieler Automarken. Wie wertvoll ein solches System ist, wird dann klar, wenn es wieder einmal Polizeiberichte über Autodiebe gibt, die statische Schlüsselcodes per Funk abhören und so das Schließsystem des Autos später ganz einfach überwinden können. Inzwischen gehen zunehmend mehr Hersteller zu Wechselcodesystemen über. Eine Rolle spielen solche Systeme auch bei manchen hochwertigen Garagentoröffnern oder industriellen Schließsystemen. Als selbst aufzubauendes bzw. Stand-alone-System sind derartige Steuerungen jedoch bisher so gut wie nicht verfügbar.

Das ELV-Rolling-Code-Schaltsystem, bestehend aus dem Zweikanal-Funk-Aufputzschalter RCS100 SA2 und dem Zweikanal-Handsender RCS100 S32, bietet durch wechselnde Übertragungscodes eine hohe Sicherheit bei der Übertragung. Zur Verschlüsselung der Übertragungsdaten wird die KEELOQ®-Technologie aus dem Hause Microchip verwendet, die man speziell für schlüssellose Zugangssysteme (Keyless Entry) entwickelt hat. Die Übertragungsfrequenz liegt im störsicheren 868-MHz-Bereich.

Der Empfänger kann mit bis zu sechs Handsendern betrieben werden. Damit eignet sich das RCS 100 hervorragend als drahtlos arbeitendes Zugangssteuerungs-

Technische Daten:

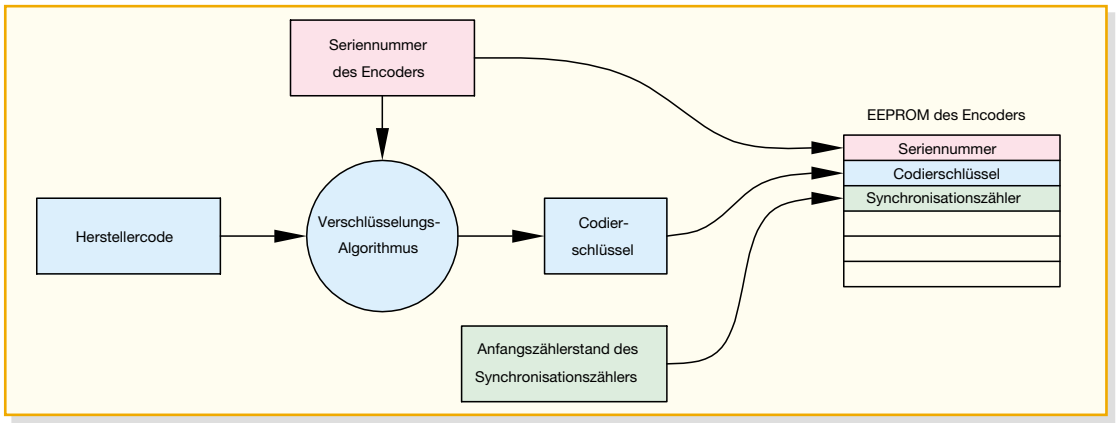
RCS100 SA2

Empfangsfrequenz:	868,35 MHz
Reichweite:	bis zu 100 m Freifeld
Anzahl der Handsender:	max. 6
Betriebsspannung:	230 V/50 Hz
Stromaufnahme:	16 mA
Anzahl der Schaltkanäle:	2
max. Anschlussleistung:	3680 VA
Gehäuse:	Schutzart IP 65
Abm. (B x H x T):	171 x 121 x 55 mm

RCS100 S32

Sendefrequenz:	868,35 MHz
Reichweite:	bis 100 m Freifeld
Betriebsspannung:	3 V
Spannungsversorgung:	2 x 1,5 V/LR44
Abm. (B x H x T):	30 x 68 x 13,5 mm

Bild 1: Programmierung des Encoder-Chips im Handsender



system für einen kleinen Kreis von Personen, etwa in der Familie, für Büros, Labors, Läden, kleine Werkstätten usw.

Die Handsender können zwei Kanäle schalten, wobei der eine mit zwei Tasten gezielt ein- und ausgeschaltet und der andere mit einer Taste umgeschaltet werden kann. Für den umschaltbaren Kanal ist am Empfänger auch eine Timerfunktion aktivierbar, so dass der Schaltkontakt nach dem Einschalten mit dem Handsender nach einer einstellbaren Zeit automatisch wieder ausgeschaltet wird.

Die KEELOQ®-Technologie

Bei der Übertragung mit der hier zum Einsatz kommenden KEELOQ®-Technologie ist eine besonders hohe Übertragungssicherheit gewährleistet. Da bei jeder Übertragung ein anderer Code übertragen wird, spricht man hier auch von Rolling-Code- oder Code-Hopping-Verfahren.

Da hier nicht nur einfach Codes nach einem bestimmten Schema gewechselt werden, sondern auch komplexe Identifizierungsmerkmale ausgetauscht werden, die zum einen der eindeutigen Identifizierung des tatsächlich zugehörigen Senders und zum anderen dem „Wiederfinden" nach mehreren Schaltversuchen außerhalb des Empfangsbereiches des Empfängers dienen, ergibt sich ein sehr sicheres, aber auch komplex arbeitendes Codesystem.

Bei jeder Übertragung wird ein 66 Bit langes Datenpaket übertragen, das sich aus 32 Bit verschlüsselten Daten, die von einem nichtlinearen Verschlüsselungs-Algorithmus erzeugt werden, und einem 34 Bit langen unverschlüsselten Teil, der aus der Seriennummer des Encoders, den Schaltzuständen und 2 Statusbit besteht, zusammensetzt.

Die Datenverschlüsselung lässt sich am einfachsten erklären, wenn man zunächst den Encoder betrachtet, der sich im Handsender befindet.

Codierung

Der Encoder-Chip wird programmiert ausgeliefert, bei der Programmierung werden, wie Abbildung 1 zeigt, im EEPROM des Chips drei für die Verschlüsselung wichtige Daten gespeichert:

- die 28-Bit-Seriennummer des Encoders, die beim Programmieren fortlaufend vergeben wird,
- der 64-Bit-Codierschlüssel, der mit einem Algorithmus aus der Seriennummer des Encoders und einem 64 Bit langen Herstellercode gebildet wird, und
- der Anfangszählerstand des Synchronisationszählers.

Wie man in Abbildung 2 sieht, werden die verschlüsselten Informationen, die mit dem KEELOQ®-Verschlüsselungs-Algorithmus codiert werden, durch den Codierschlüssel und den Synchronisationszähler beeinflusst.

Der Codierschlüssel setzt sich, wie beschrieben, aus dem Herstellercode und der Seriennummer des Encoders zusammen. Der Herstellercode sorgt dafür, dass die Verschlüsselung des Encoders nicht zu Systemen anderer Anbieter passt, es somit nicht zu systemübergreifenden Fehlschaltungen oder Codediebstahl kommen kann.

Mit der 28-Bit-Seriennummer lassen sich über 268 Millionen Encoder mit gleichem Herstellercode und unterschiedlichem Codierschlüssel, also mit unterschiedlicher Verschlüsselung, programmieren.

Der dritte Teil, der in die verschlüsselten Informationen eingeht, ist der Synchronisationszähler. Dieser wird bei jeder Datenübertragung um eins erhöht, und das sorgt zusammen mit dem Verschlüsselungsverfahren dafür, dass sich bei jeder Übertragung über 50 Prozent der verschlüsselten Datenbit ändern. Der Synchronisationszähler ist ein 16-Bit-Zähler, der 65.536 Übertragungen ermöglicht, ehe sich der übertragene Code wiederholen kann. Wenn man von zehn Übertragungen am Tag ausgeht, entspricht dies einer Zeit von ungefähr 18 Jahren!

Decodierung

Betrachten wir nun die Auswertung der übertragenen Daten auf der Empfangsseite.

Einen Überblick verschafft hier das Blockdiagramm in Abbildung 3.

Zuerst erfolgt eine Überprüfung, ob die (unverschlüsselt) übertragene Seriennum-

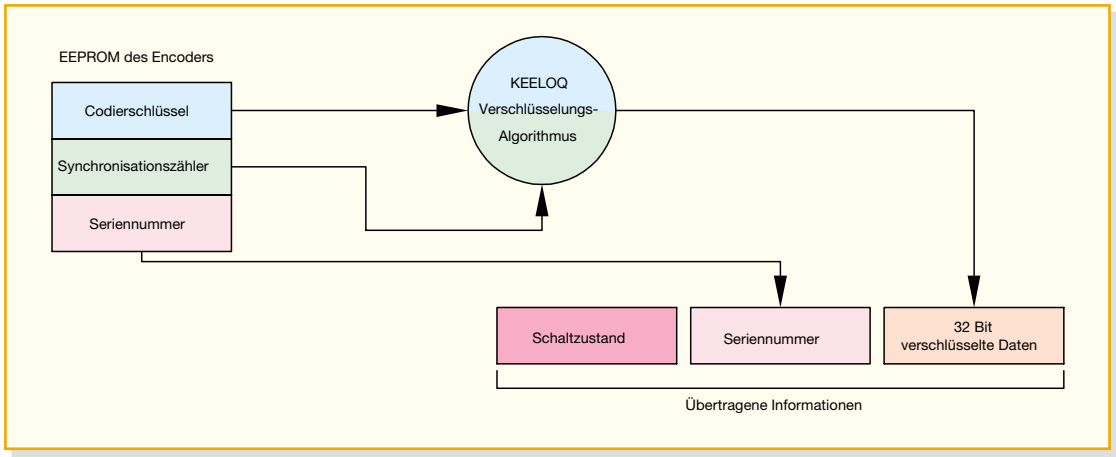


Bild 2: Prinzip der Datenverschlüsselung im Encoder

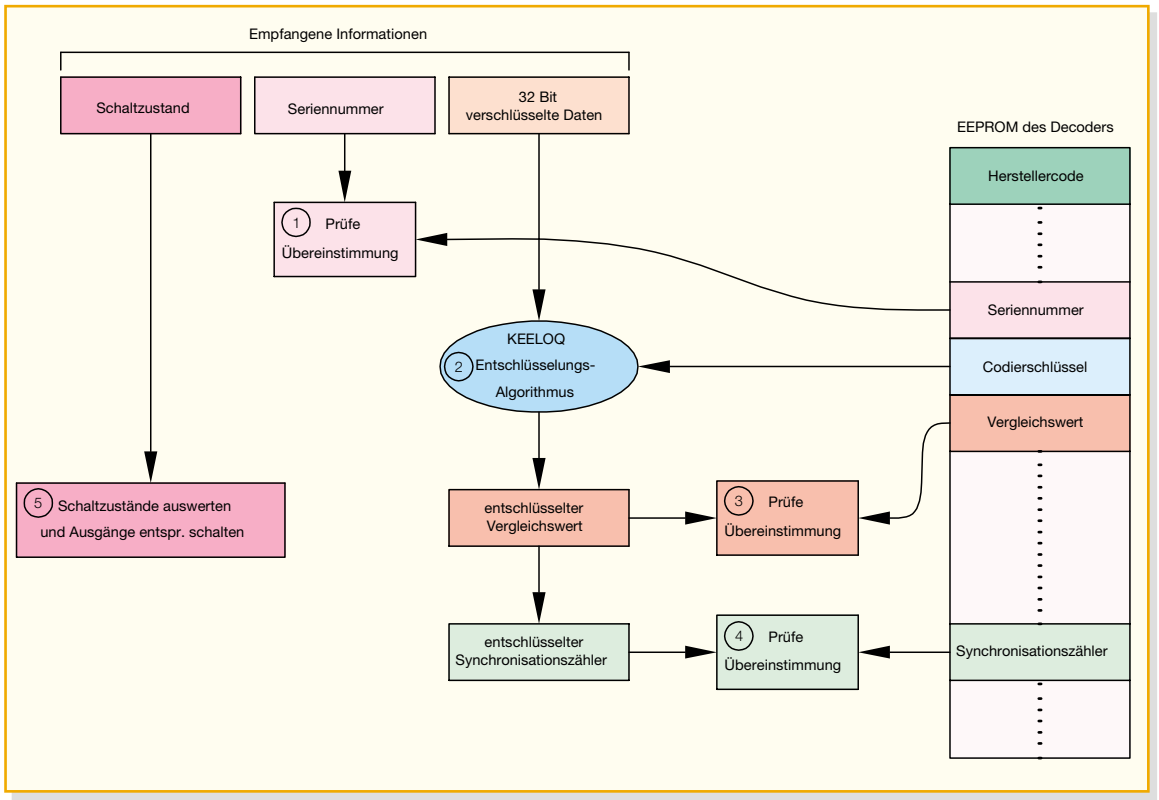


Bild 3: Auswertung der empfangenen Informationen

mer mit einer der Seriennummern, die im EEPROM des Empfängers abgelegt sind, übereinstimmt. Die Seriennummer des Handsenders wird beim Anlernen des Handsenders vom Empfänger zusammen mit dem Stand des Synchronisationszählers und einem 10 Bit langen Vergleichswert gespeichert.

Stimmt die Seriennummer überein, werden die verschlüsselten Daten decodiert.

Danach überprüft das System, ob der entschlüsselte 10-Bit-Vergleichswert mit dem im EEPROM gespeicherten Vergleichswert übereinstimmt. Stimmen diese Werte überein, wird jetzt der Stand des Synchronisationszählers, der ebenfalls verschlüsselt übertragen wurde, mit dem Zählerstand im EEPROM des Empfängers verglichen.

Wenn auch der Zählerstand in Ordnung ist, werden schließlich die übertragenen Schaltzustandsinformationen ausgewertet und die Ausgänge entsprechend geschaltet.

Wie die Überprüfung der Gültigkeit des Zählerstandes erfolgt, verdeutlicht Abbildung 4.

Hierzu kann man sich das Diagramm mit den drei Bereichen als eine Auswahlmaske vorstellen, die sich bei jeder erfolgreichen Übertragung weiter dreht und mit dem gespeicherten Synchronisationszählerstand auf den zuletzt übertragenen Zählerstand zeigt. Der ganze Kreis stellt die 65.536 möglichen Zählerstände dar. Die Hälfte der Zählerstände liegt im blockierten Bereich, mit diesen kann keine gültige Übertragung stattfinden. Dies ist ein Schutzmechanismus, um zu verhindern, dass sich Dritte mit aufgezeichneten Datenübertragungen Zugang zum System verschaffen und Schaltvorgänge auslösen können. Der akzeptierte Bereich umfasst die nächsten 16 Zählerstände nach der letzten gültigen Übertragung. In diesem Bereich werden die übertragenen Schaltzustände sofort ausgewertet und umgesetzt, der übertragene Zählerstand wird gespeichert.

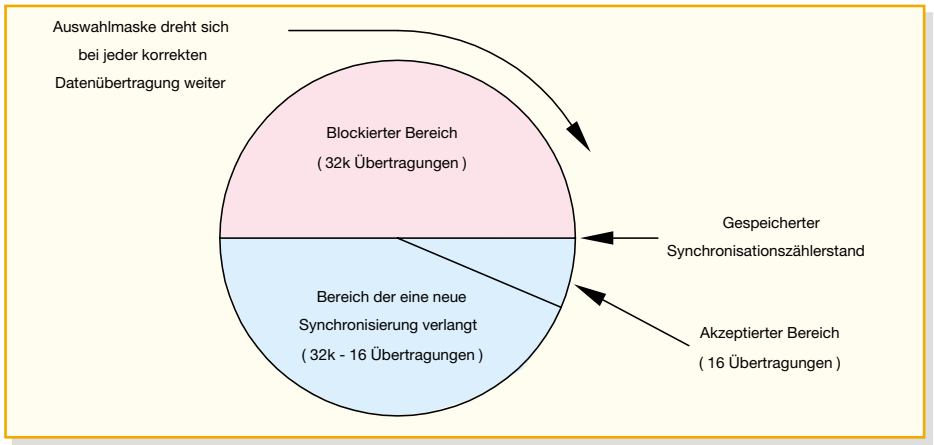


Bild 4: Überprüfung des Synchronisationszählers

Aus den Augen, aber nicht aus dem Sinn – wie sich Empfänger und Sender immer „wiederfinden“

Das bedeutet in der Praxis, dass der Handsender bis zu 15-mal außerhalb der Reichweite des Empfängers betätigt werden kann und bei der 16. Betätigung, dann innerhalb der Reichweite des Empfängers, sofort einen Schaltvorgang auslösen kann. Sollte der Handsender öfter als 15-mal außerhalb der Reichweite des Empfängers betätigt worden sein, liegt der dann von ihm übertragene Synchronisationszählerstand in einem Bereich, der eine neue Synchronisation erfordert. Diese neue Synchronisation erfolgt fast unmerklich für den Anwender, denn sie erfordert nur zwei gültige Übertragungen mit zwei aufeinander folgenden Synchronisationszählerständen, die im Bereich liegen, der eine neue Synchronisation erfordert. Empfängt der Decoder eine Übertragung mit einem Zählerstand aus diesem Bereich, wird der Schaltbefehl zunächst noch nicht ausgeführt. Erst wenn die zweite Übertragung mit dem folgenden Zählerstand eintrifft, erfolgt eine Ausführung des Schaltbefehls, und der Zähler ist wieder synchronisiert.

Der Anwender wird die Synchronisation kaum bemerken, da es in der Natur des Menschen liegt, die Taste des Handsen-

ders ein zweites Mal zu drücken, wenn beim ersten Mal nichts passiert.

Bedienung

Der in eine feste Netzspannungsverkabelung zu installierende Aufputzschalter ist nach dem Anschluss an die Netzspannung sofort betriebsbereit.

Direktbedienung am Empfänger

Mit den Tasten für Kanal 1 und Kanal 2 lassen sich die gleichen Schaltvorgänge wie mit den Tasten des Handsenders auslösen, das heißt z. B., ein Kanal kann durch kurzes Betätigen der Ein- oder der Aus-Taste gezielt ein- und ausgeschaltet werden. Dieses Verfahren ist im Übrigen beim Einsatz des Handsenders von Vorteil, wenn kein direkter Sichtkontakt zum Schaltereignis besteht (wie z. B. beim Scharfschalten einer Alarmanlage).

Mit dem Taster für Kanal 2 kann dieser Kanal bei jedem Tastendruck umgeschaltet werden, d. h., je nachdem in welchem Zustand sich der Schaltkontakt gerade befindet, wird er beim Betätigen des Tasters entweder ein- oder ausgeschaltet. Die Leuchtdioden über den Tastern zeigen die Schaltzustände der beiden Kanäle an. Sie leuchten, wenn der zugehörige Schaltkontakt geschlossen ist.

Timer-Betrieb

Mit der Taste „Ein/Aus/Timer“ ist auch die Timerfunktion für Kanal 2 programmierbar. Wird die Taste länger als 4 Sekunden gedrückt, beginnt die LED von Kanal 2 in kurzen Abständen aufzublitzen und der Schaltkontakt von Kanal 2 wechselt in die Ruheposition, falls er vorher eingeschaltet war. Wird nun innerhalb der nächsten 4 Sekunden die Taste losgelassen, erfolgt der Start der Zeitmessung. Dies wird dadurch angezeigt, dass die LED für Kanal 2 nun im 0,5-Sekunden-Abstand blinkt und der Schaltkontakt für Kanal 2 schließt. Durch ein weiteres kurzes Betätigen der Taste wird die Zeitmessung beendet und die Zeit gespeichert, der Schaltkontakt wechselt wieder in den Ruhezustand, und die LED erlischt. Die Einschaltdauer lässt sich in einem Bereich von 0,5 Sekunden bis 9 Stunden einstellen. Beendet man die Zeitmessung nicht manuell vor Ablauf der 9 Stunden, speichert das Gerät die 9 Stunden als Einschaltdauer.

Zur Deaktivierung der Timerfunktion ist die Taste „Ein/Aus/Timer“ mehr als 8 Sekunden gedrückt zu halten. Nach 4 Sekunden beginnt wieder die Leuchtdiode von Kanal 2 kurz aufzublitzen, und nach weiteren 4 Sekunden erlischt die LED, jetzt kann die Taste losgelassen werden, und die Timerfunktion ist deaktiviert.

Betreibt man Kanal 2 mit der Timerfunktion, so kann der Schaltkontakt bei laufender Zeit durch kurzes Betätigen der Taste „Ein/Aus/Timer“ oder der Taste für Kanal 2 am Handsender in den Ruhezustand gebracht werden. Ein weiteres Drücken der Taste schaltet den Kontakt erneut für die programmierte Einschaltdauer ein.

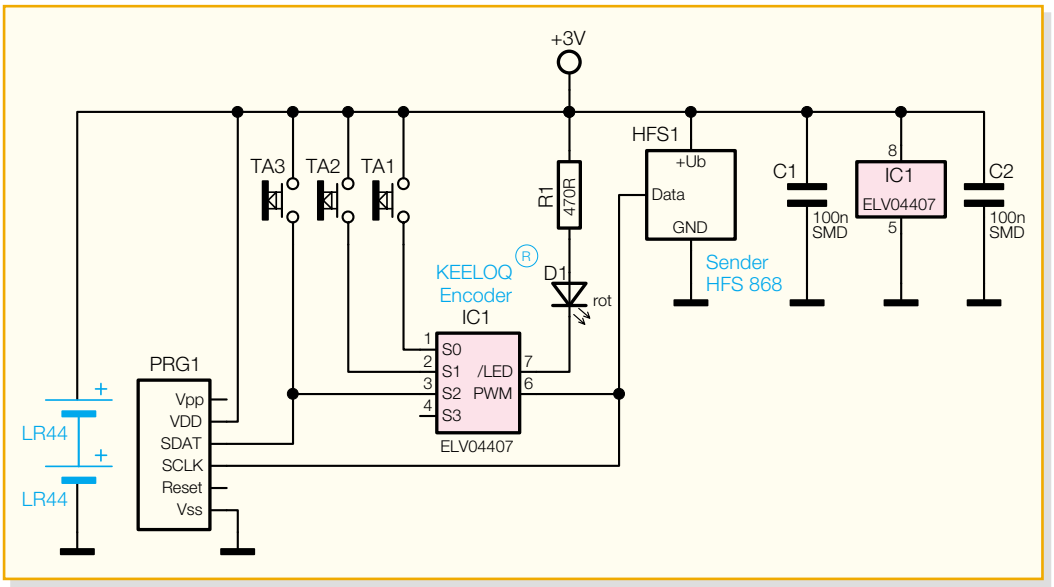


Bild 5: Schaltbild des Rolling-Code-Handsenders RCS100 S32

Handsender: Anlernen und Bedienung

Die Tasten des Handsenders haben die gleichen Schaltfunktionen wie die Tasten am Aufputzschalter, die Einschaltdauer des Timers ist allerdings nicht mit dem Handsender programmierbar.

Bevor man allerdings den Handsender einsetzen kann, muss dieser am Aufputzschalter angelernt werden.

Um diesen Vorgang einzuleiten, ist zunächst die Taste „Anlernen“ am Aufputzschalter kurz zu drücken. Die Leuchtdiode über der Taste leuchtet jetzt dauerhaft. Betätigt man nun innerhalb einer halben Minute eine Taste des Handsenders, erlischt die LED, nach dem nochmaligen Betätigen derselben Taste am Handsender innerhalb von einer halben Minute zeigt die LED durch 5 Sekunden langes Blinken einen erfolgreichen oder durch Aufleuchten für eine Sekunde einen fehlgeschlagenen Anlernvorgang an.

Wird in einer der 30 Sekunden dauernden Warteschleifen kein gültiges Funksignal vom Handsender empfangen, so bricht der Empfänger den Anlernvorgang ab.

Auf diese Weise lassen sich bis zu sechs unterschiedliche Handsender am Funk-Aufputzschalter anlernen. Hierbei ist zu beachten, dass bei Anlernen eines siebten Handsenders die Daten des ersten Handsenders überschrieben werden und dieser dann nicht mehr den Empfänger ansteuern kann.

Gespeicherte Sender löschen

Drückt man die Taste „Anlernen“ für ca. 10 Sekunden, bis die LED über der Taste wieder erlischt, werden alle bisher angelernten Handsender aus dem Speicher des Aufputzschalters gelöscht, d. h., das System reagiert jetzt auf keine empfangenen Schaltbefehle mehr.

Betrieb

Im Normalbetrieb zeigt die LED „Anlernen“ durch schnelles Blinken den Empfang von Schaltbefehlen an, dies geschieht unabhängig davon, ob der Sender dem System bekannt ist und der empfangene Befehl ausgeführt wird oder ob es sich um einen unbekannten Sender handelt und der Schaltbefehl ignoriert wird.

Die Leuchtdiode am Handsender zeigt beim Betätigen einer Taste das Senden des Schaltbefehls durch dauerhaftes Leuchten an, solange die Taste gedrückt wird. Nimmt die Batteriespannung des Handsenders ab, blinkt die LED bei gedrückter Taste, dies ist ein Zeichen dafür, dass die Batterien bald erneuert werden müssen.

Um die Batterien zu schonen, wird die Sendefunktion abgebrochen, wenn eine Taste länger als 25 Sekunden gedrückt wird – dies könnte z. B. passieren, wenn der Handsender, in einer Tasche getragen, versehentlich betätigt wird.

Schaltung

Zur besseren Übersichtlichkeit sind die Schaltbilder für Sender und Empfänger getrennt dargestellt.

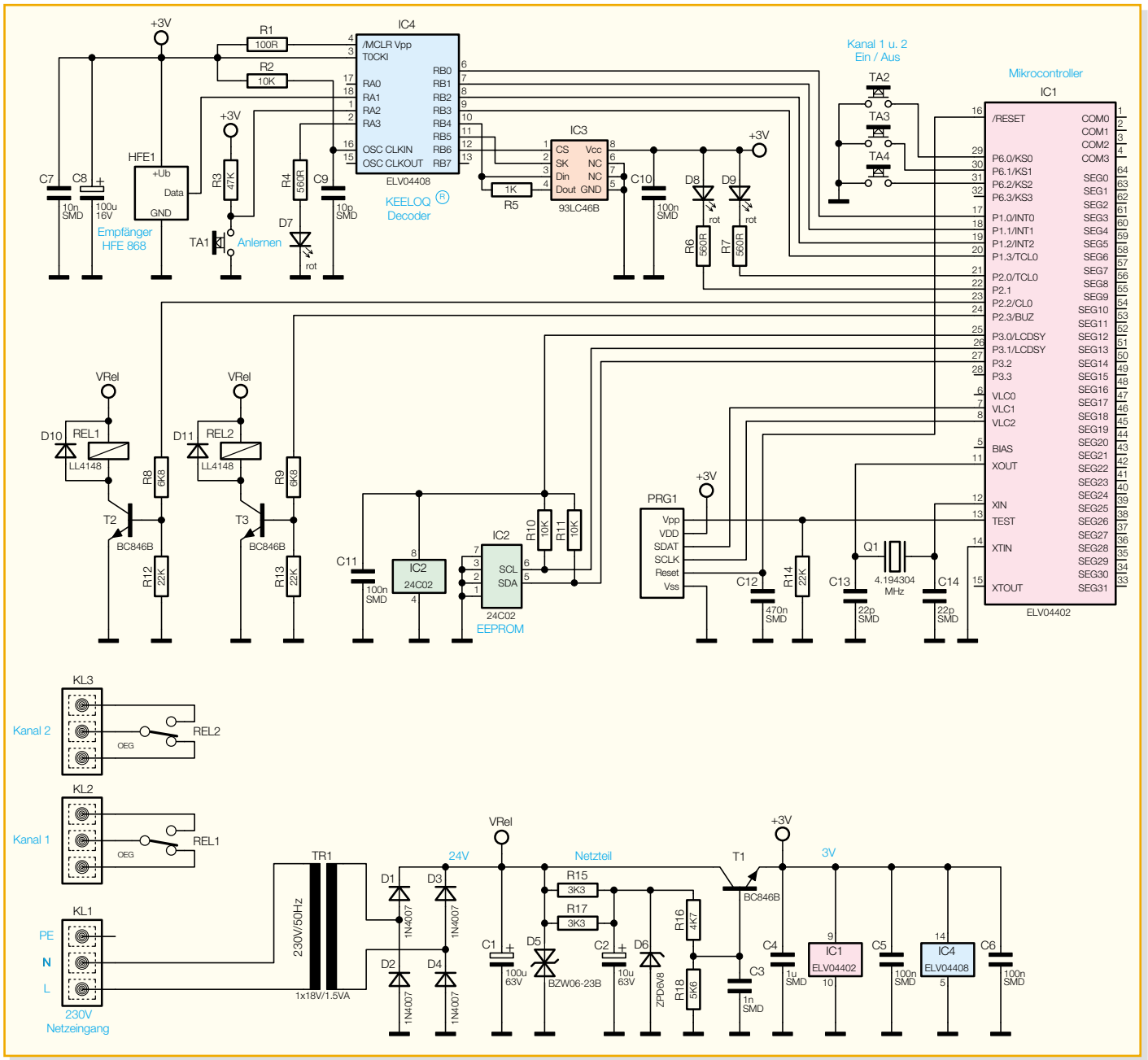


Bild 6: Schaltbild des Rolling-Code-Funk-Aufputzschalters RCS100 SA2

Rolling-Code-Handsender RCS100 S32

Das Herzstück des Handsenders (Abbildung 5) ist IC 1. Hierbei handelt es sich um einen bereits programmierten KEELOQ® Code Hopping Encoder HCS 300, der sowohl die Abfrage der Taster TA 1 bis TA 3 als auch die Ansteuerung der LED D 1 sowie die Ausgabe des PWM-Signals an das 868-MHz-Sendemodul HFS 1 übernimmt. Der Programmieradapter PRG 1 dient nur der Programmierung des HCS 300 während der Produktion. Die Spannungsversorgung des Handsenders erfolgt über zwei Knopfzellen des Typs LR 44.

Rolling-Code-Funk-Aufputzschalter RCS100 SA2

Das Schaltbild des Funk-Aufputzschalters ist in Abbildung 6 dargestellt.

Die Spannungsversorgung erfolgt über den kurzschlussfesten Transformator TR 1. Da der Transformator unterhalb seines Nennstromes betrieben wird, stellt sich nach Gleichrichtung (D 1 bis D 4) und Siebung (C 1) eine Spannung V_{Rel} von etwa 24 V ein. Diese ungeregelte Spannung wird für die Versorgung der Relaisschaltstufen benötigt. Die Transil-Schutzdiode D 5 verhindert, dass die Schaltung durch Überspannungsimpulse auf der Netzleitung beeinträchtigt wird.

Für die Mikrocontrollerschaltung stellt die Regelschaltung mit T 1 und Peripherie eine stabile Spannung von 3 V zur Verfügung.

Die Decodierung und Auswertung der empfangenen Schaltbefehle erfolgt in IC 4, einem als KEELOQ®-Decoder programmierten PIC-Mikrocontroller. Die Daten der angelernten Handsender werden im seriellen EEPROM IC 3 gespeichert. Die Abfrage der Taste „Anlernen“ TA 1 und die Ansteuerung der LED D 7 erfolgen ebenfalls durch dieses IC.

Der Mikrocontroller IC 1 übernimmt die Abfrage der Schaltausgänge von IC 4 und der Taster TA 2 bis TA 4. Wenn ein Schaltbefehl vom Decoder ausgewertet oder eine der drei Tasten am Funk-Aufputzschalter gedrückt wurde, erfolgt ein Schalten der Relais REL 1 und REL 2 über die Transistoren T 2 und T 3. Gleichzeitig werden die LEDs D 8 und D 9 entsprechend den Zuständen der Schaltkontakte geschaltet.

Im „ELVjournal“ 4/2004 beschreiben wir den Nachbau mit Gehäusemontage und Installation dieses interessanten Rolling-Code-Schaltsystems.