

Guerilla Infrarot Hacking

fd0@koeln.ccc.de

Easterhegg 2008
Köln

Themenübersicht

1. Einführung
2. Infrarot-Steuerungstechnik
3. Codierungsverfahren
4. Fernbedienungs-Protokolle
5. Informationsgewinnung
6. Hardware: “unzap”
7. Geräte-Penetrationstests
8. Ausblick

Einführung: Warum Infrarot?

- Weit verbreitet:
 - TV, Anlage, Unterhaltungselektronik
 - Autotürschloss
 - Alarmanlagen (MediaMarkt, Saturn)
 - Navigation, Weichenstellung (ÖPNV)
 - Abrechnung (Hotels)
- Gut nutzbar zur Steuerung
 - Reflektiert fast überall
 - Sichtverbindung nicht nötig
 - Ausbreitung beschränkt
- Aber: Meist security-by-obscurity









BUSHOFSANIERUNG MIT SONNENLICHT



BAUHERR:

ASEAG
AACHENER STRASSENBAHN UND
ENERGIEVERSORGUNGSGES.
NEUKÜLLER STRASSE 1
52068 AACHEN

ARCHITEKT:



architekturbüro
Wolfgang
Graf

Königsplatz 103
52070 AACHEN
Tel.: 0241 / 988-11
Fax: 0241 / 988-10
www.architekturbüro.de

Dipl.-Ing. Udo Fink
Planung und Ausführung
von Solaranlagen
Industriestraße 1
52068 AACHEN
Tel.: 0241 / 4611-0
Fax: 0241 / 4611-10

Born-Solar GmbH
Planung und Ausführung
von Solaranlagen
Industriestraße 1
52068 AACHEN
Tel.: 0241 / 4611-0
Fax: 0241 / 4611-10
www.born-solar.de

Elektro Fingst
(Elektro - Beleuchtung)
Industriestraße 1
52068 AACHEN
Tel.: 0241 / 4703470
Fax: 0241 / 47034728

Möller Hagers GmbH
(Modul-Lieferanten)
Georgstraße 14
52223 Badberg
Tel.: 02402 / 82500
Fax: 02402 / 24672

SMV
(Automatisierung und
Beleuchtungssysteme)
Schulze von Bunde Str. 41
52134 Herzogenrath
Tel.: 0241 / 97970
www.smv-automation.de

r & p Bau GmbH
(Rohbauarbeiten)
Im den Ackerbenden 29
52068 AACHEN
Tel.: 0241 / 1881129
Fax: 0241 / 9888887

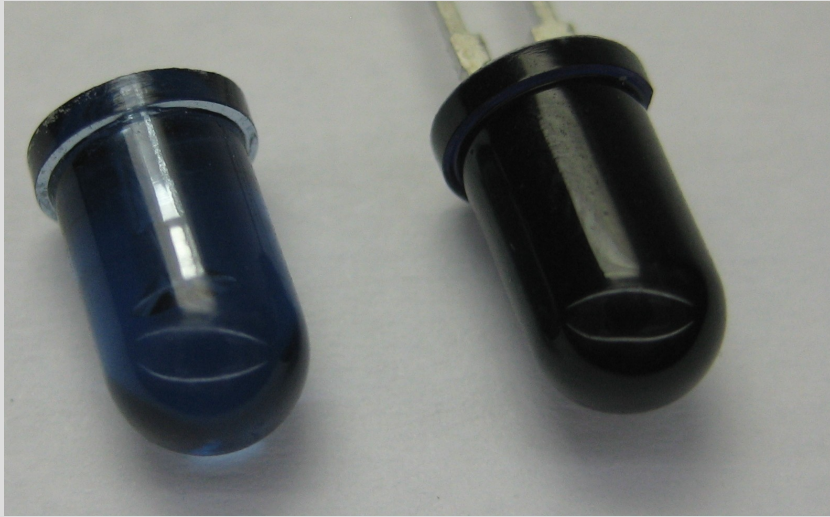
53

212

Mercedes-Benz



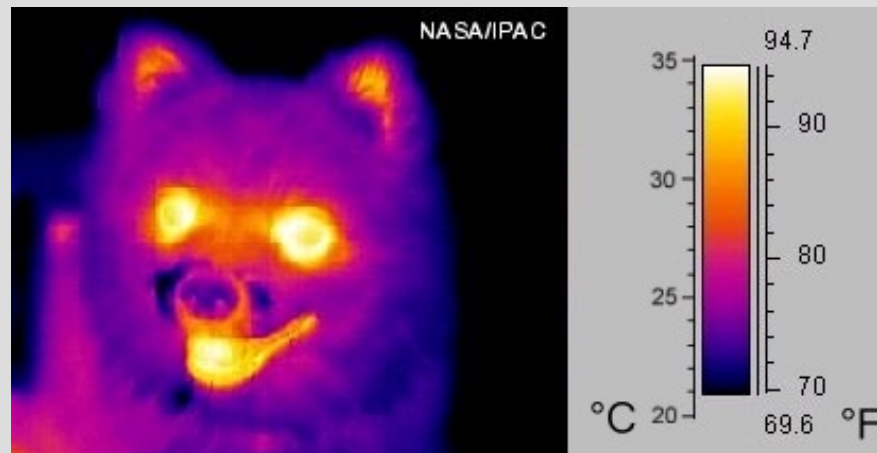
Infrarot-Steuerungstechnik



- Licht im infraroten Spektralbereich
- Wellenlänge: $\sim 950\text{nm}$
- Typisch: LEDs

Infrarot – Probleme

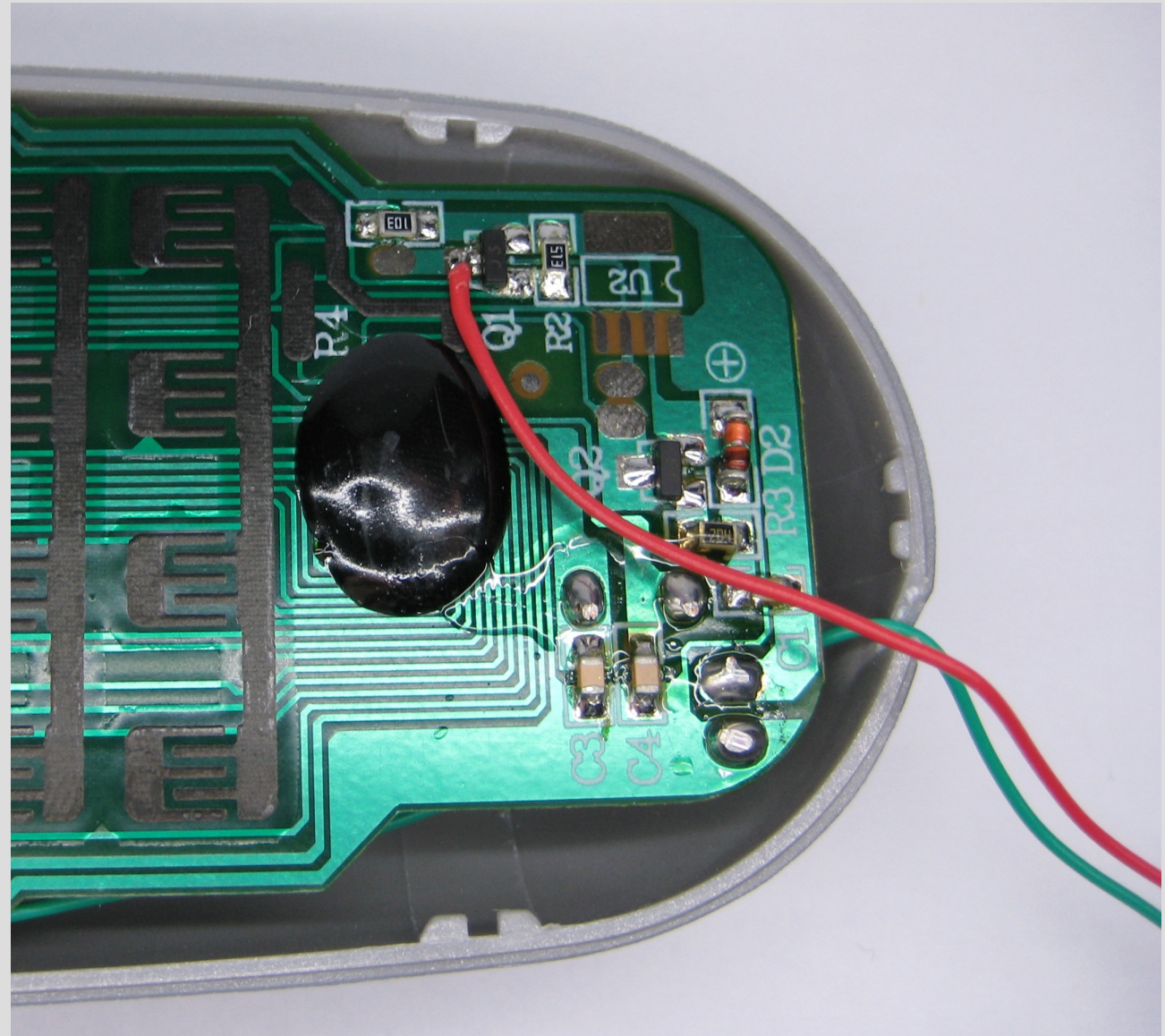
- Andere Infrarotlichtquellen:
 - Sonne
 - Heizung
 - Lebewesen
- Unterscheidung vom Nutzsignal?



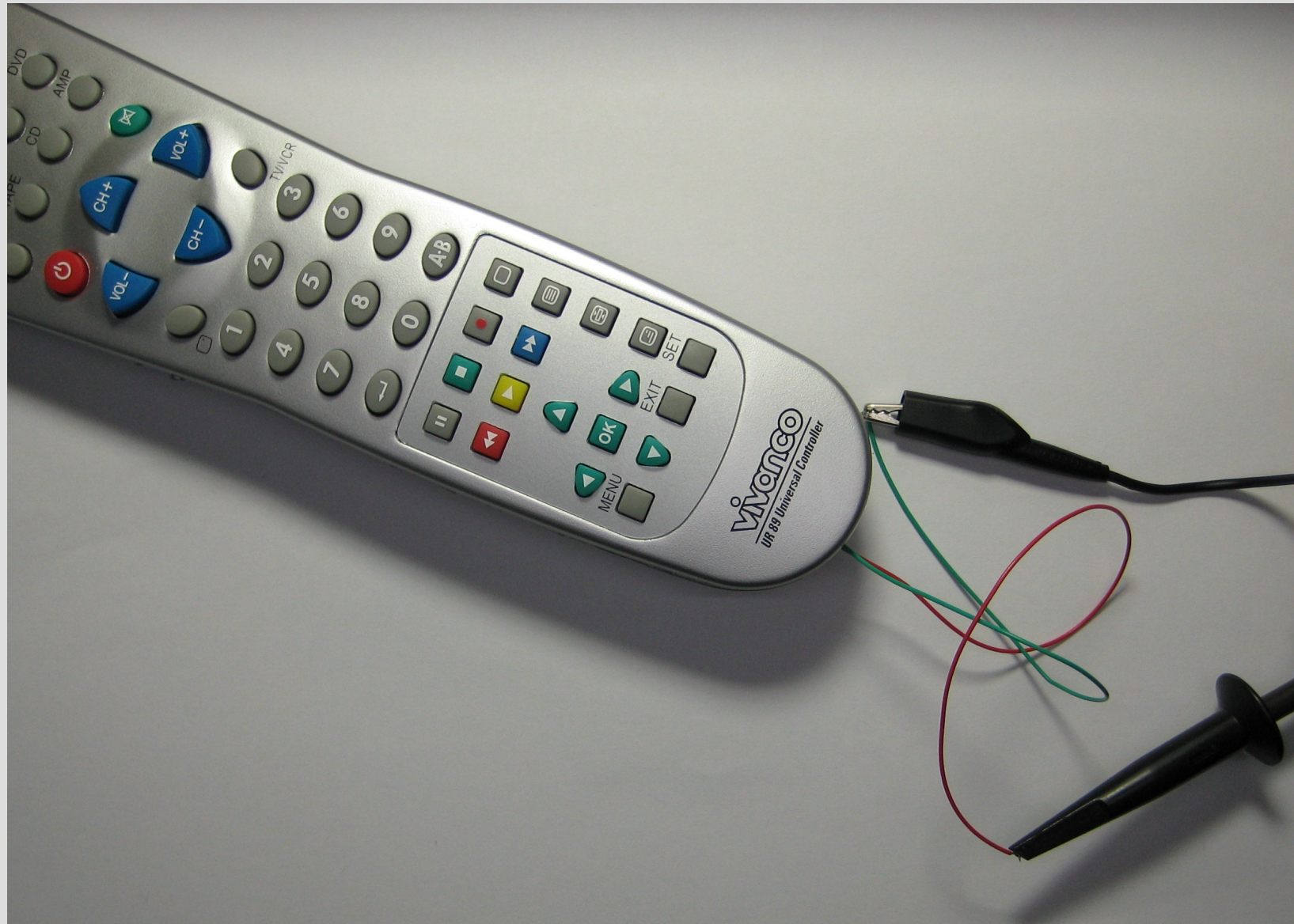
Modulation mittels Trägerfrequenz

- LED gepulst
- Trägerfrequenz:
 - Meist 30-60 kHz
 - Ausnahme: 445 kHz (Bang&Olufsson, ...)
- Vorteile:
 - Gut von Hintergrundlicht zu unterscheiden
 - Energiesparender
 - Gut zu senden
 - Leicht zu dekodieren

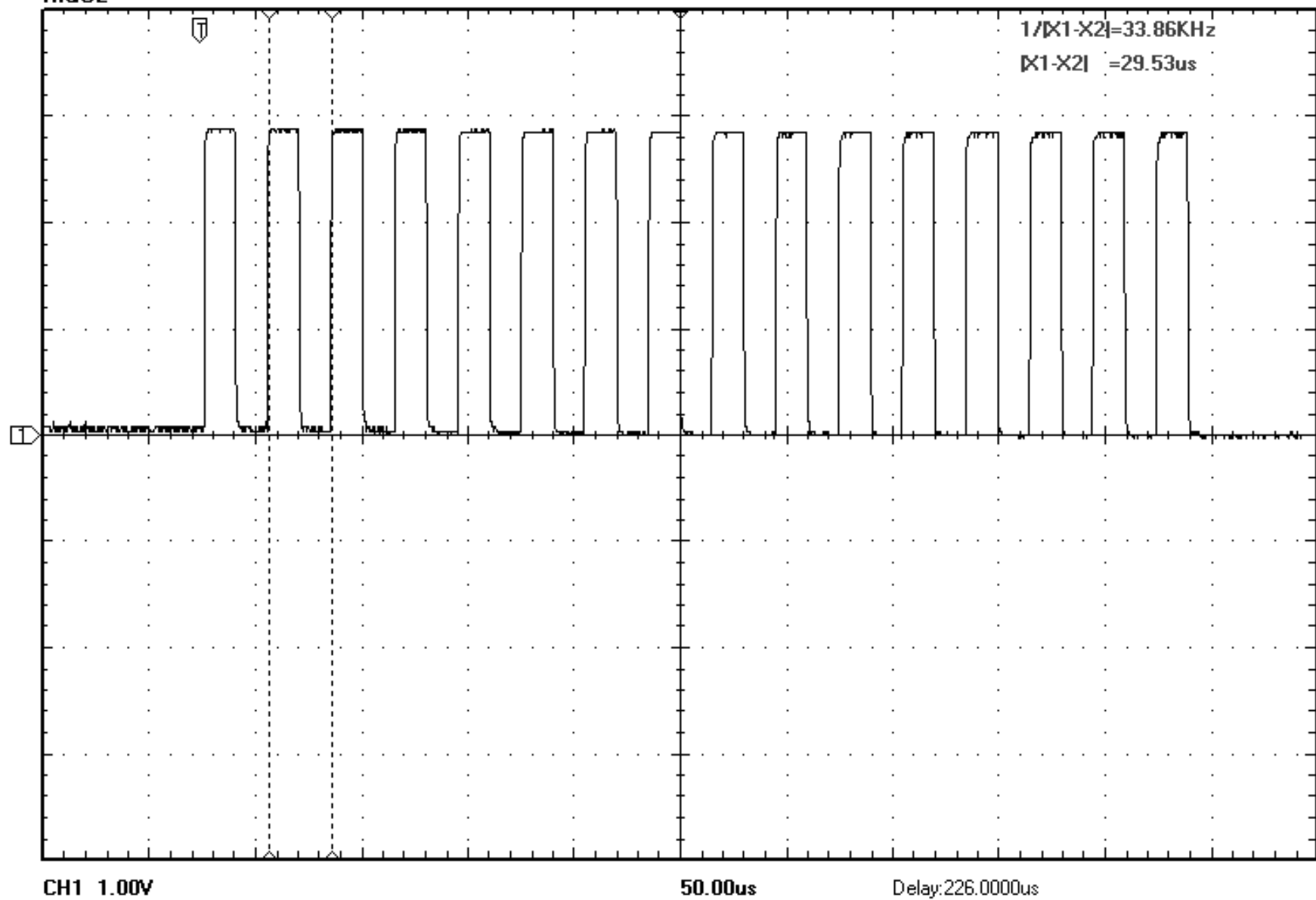
Messaufbau



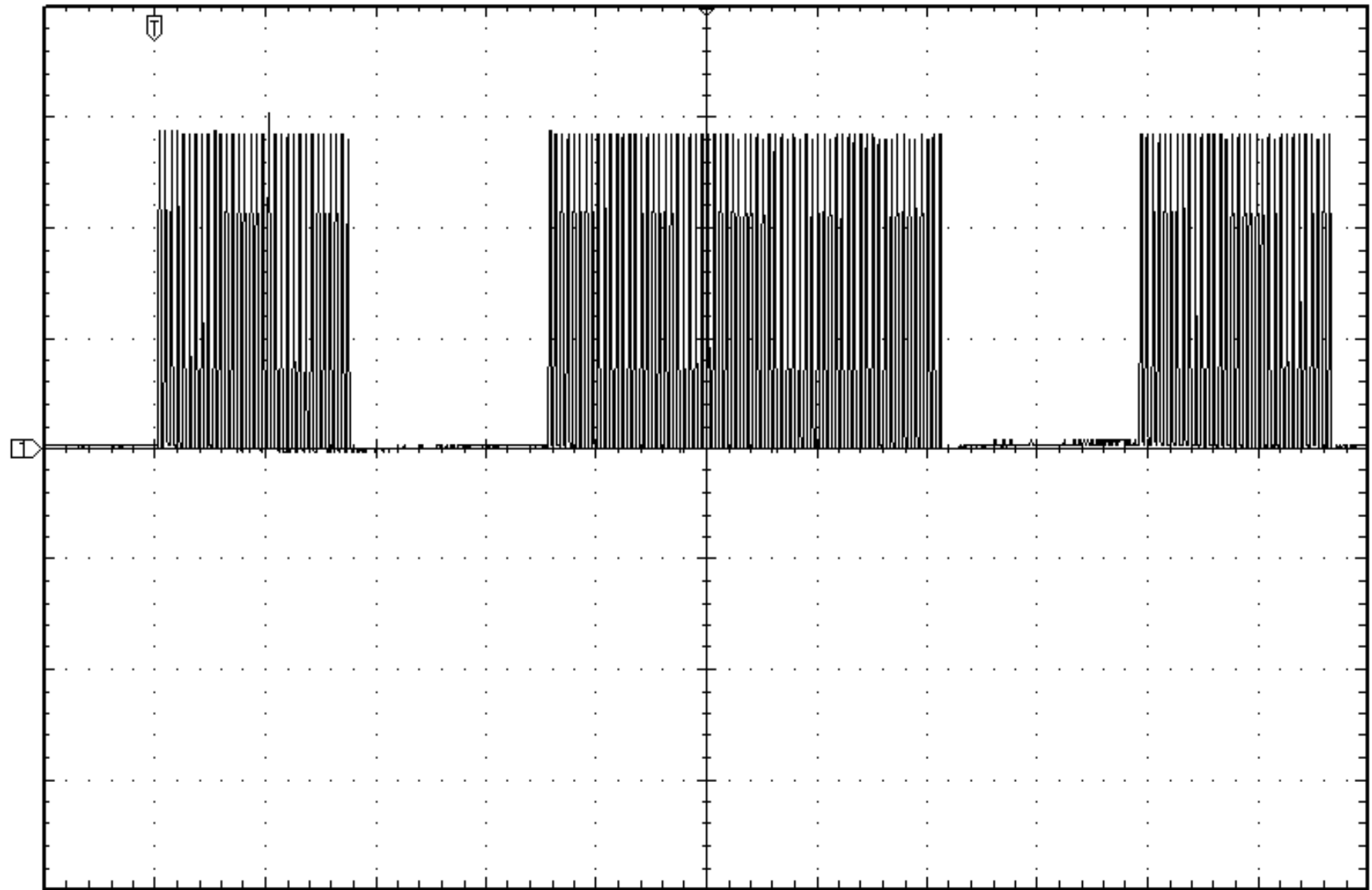
Messaufbau



RIGOL



RIGOL



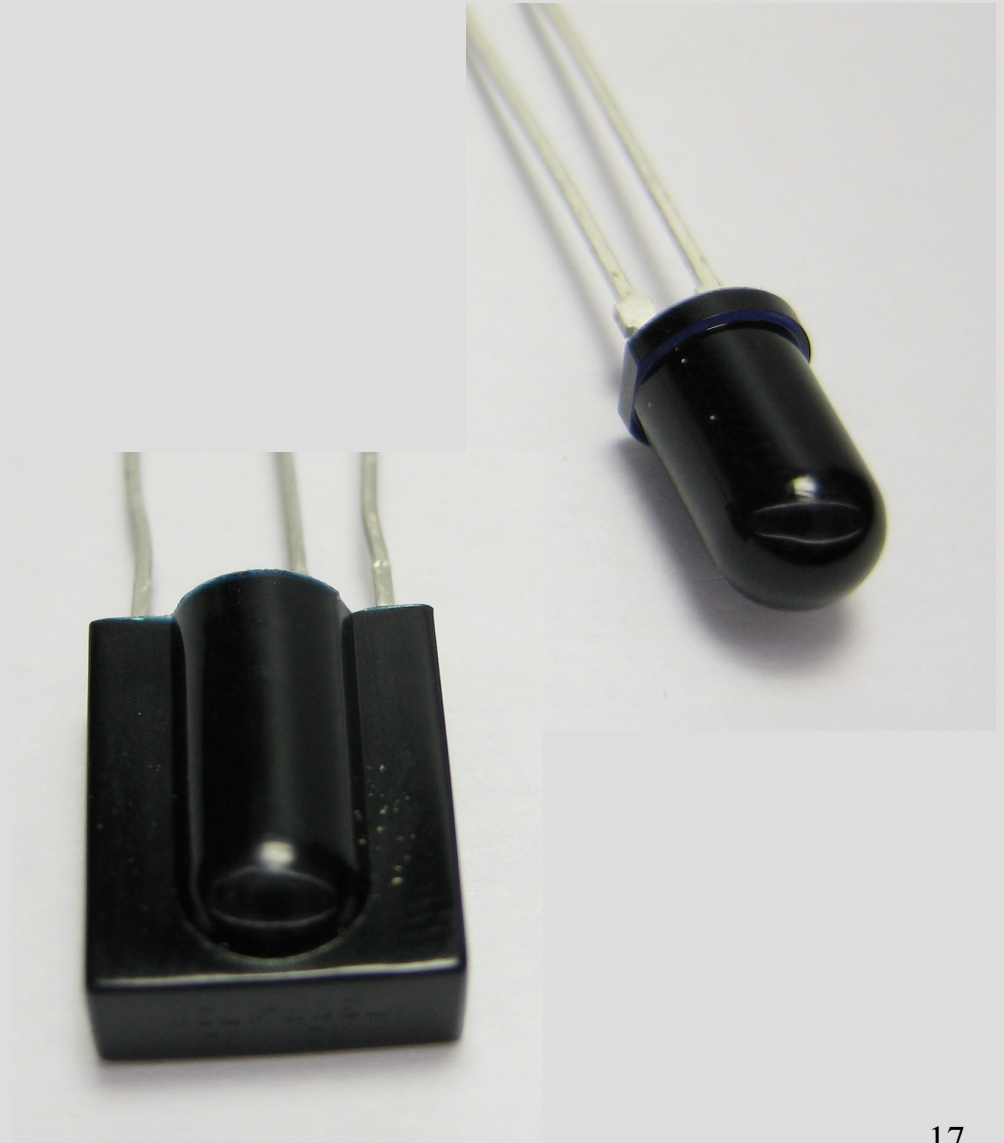
CH1 1.00V

500.0us

Delay: 2.500000ms

Infrarot-Emfänger

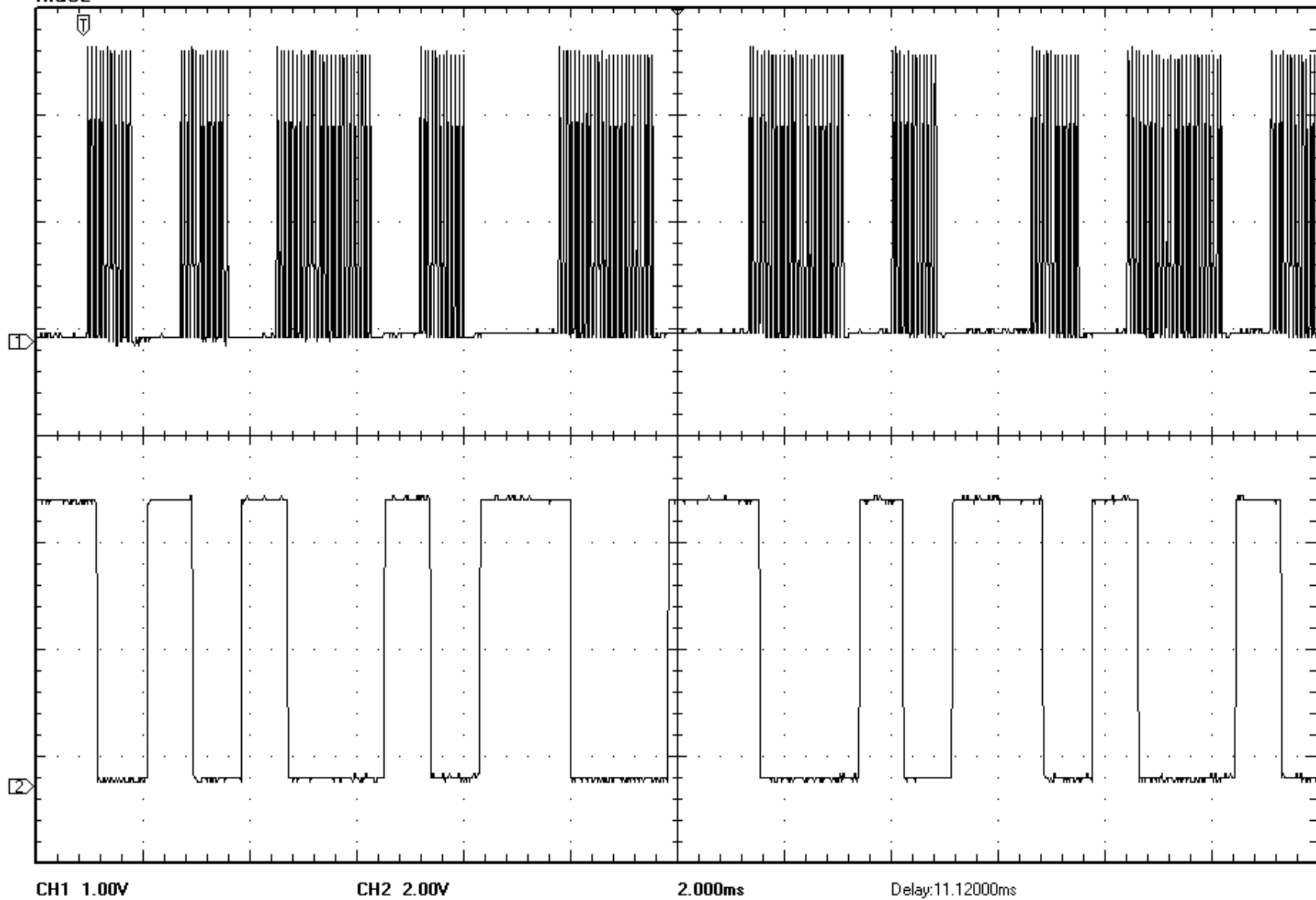
- Infrarot-Fototransistor
- Vishay TSOP17xx
 - Fototransistor
 - Bandpass
 - Demodulator
 - Ausgang invertiert



Beispiel: TSOP1738



RIGOL

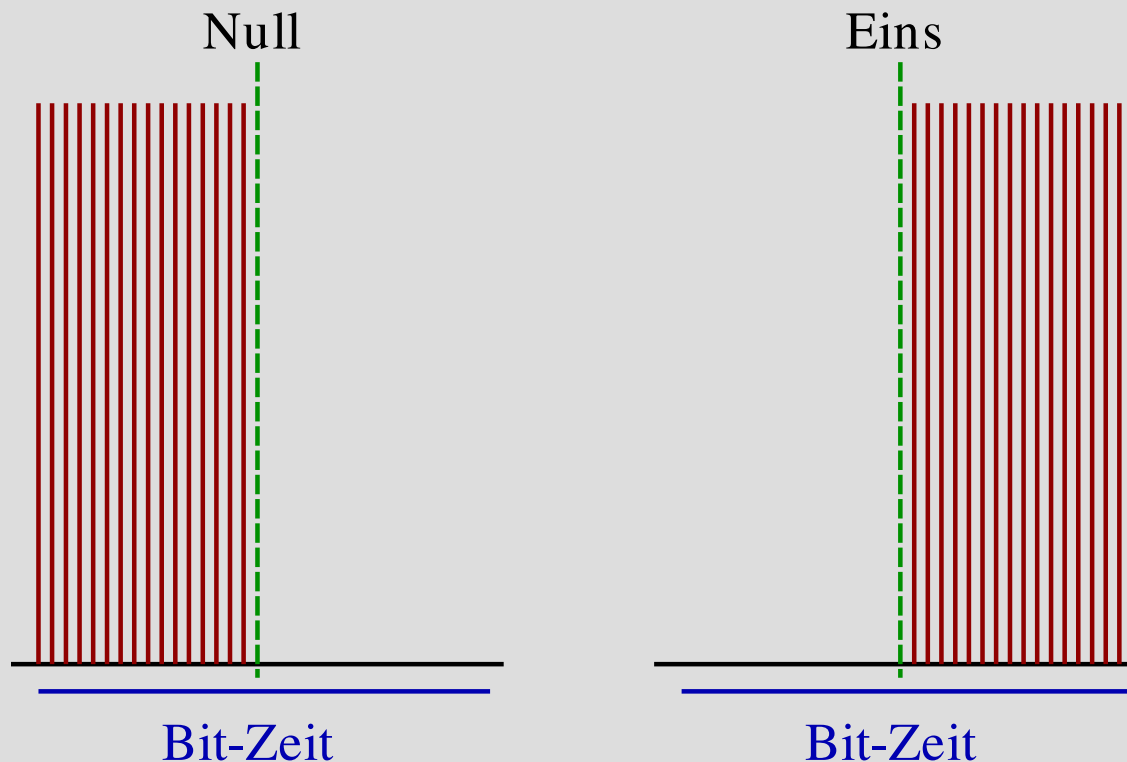


Codierungsverfahren

- Verbindung von Träger und Daten
- Nicht sehr viele Möglichkeiten
- Verbreitet:
 - Manchester-Code
 - Pulsdistanzmodulation
 - Pulsbreitenmodulation

Manchester-Code

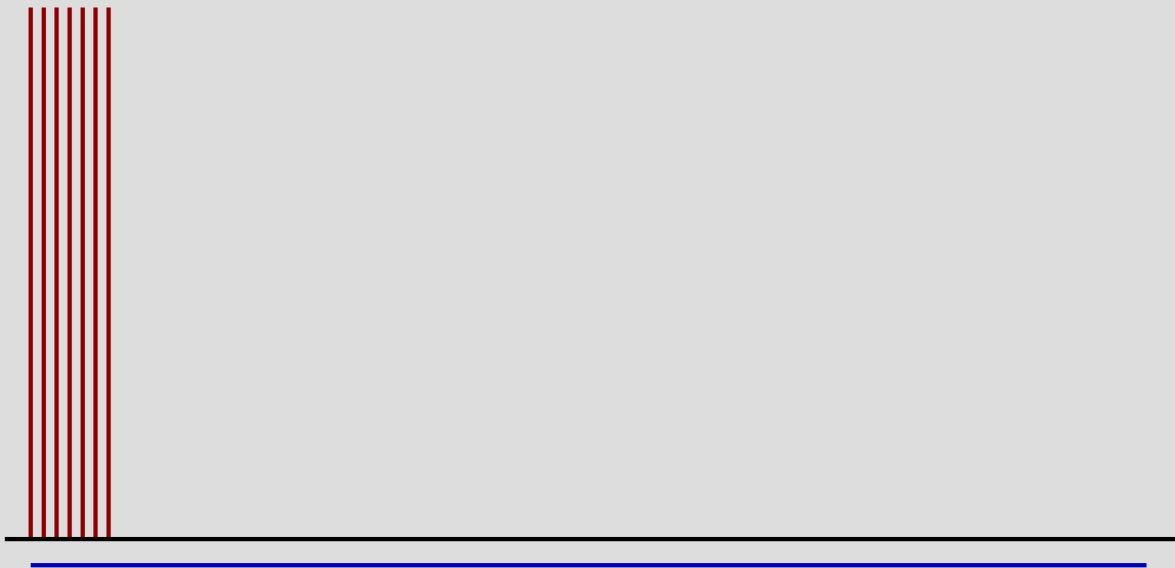
- Jedes Bit konstante Übertragungszeit
- Träger nur in halber Bit-Zeit aktiv
 - Eins: Träger in der ersten Hälfte
 - Null: Träger in der zweiten Hälfte



Pulsdistanzmodulation

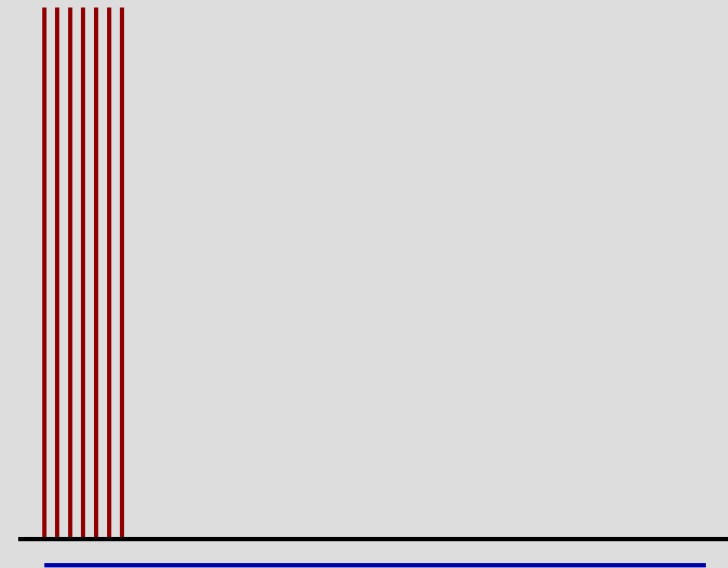
- Jedes Bit beginnt mit einem Träger konstanter Länge
- Eins wird als lange Pause kodiert
- Null wird als kurze Pause kodiert

Eins



Bit-Zeit

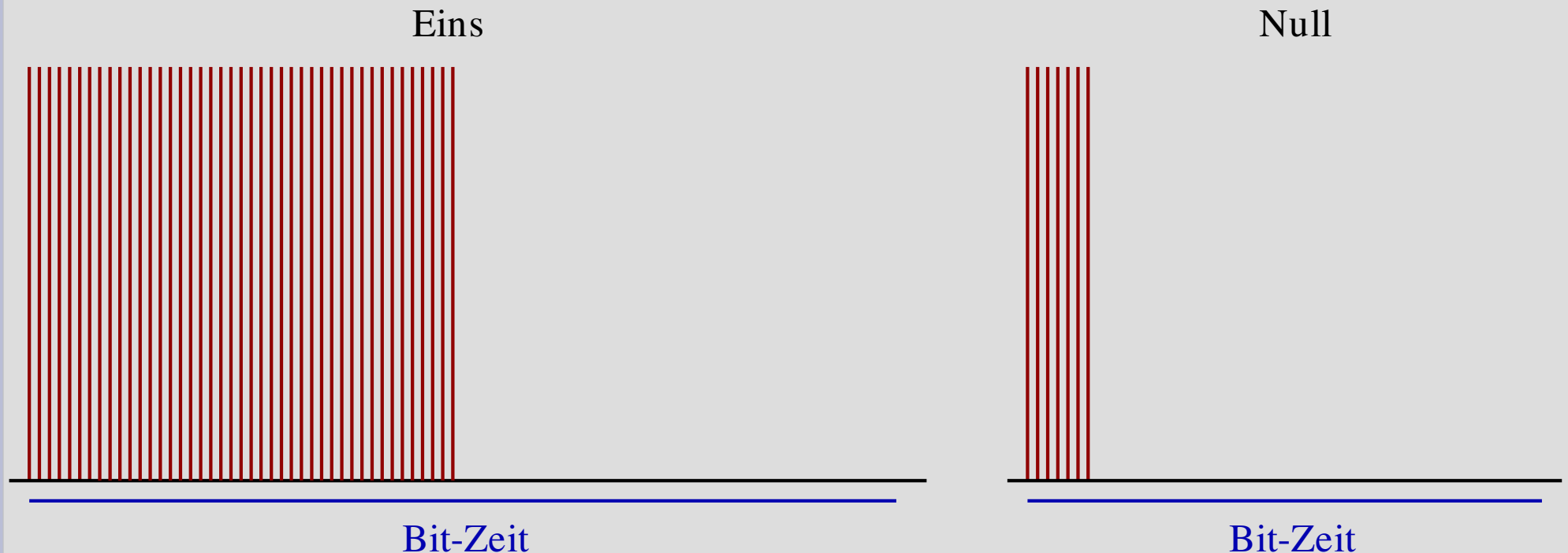
Null



Bit-Zeit

Pulsbreitenmodulation

- Eins beginnt mit einem langen Puls
- Null beginnt mit einem kurzen Puls
- Danach folgt jeweils eine Pause



IR-Protokolle

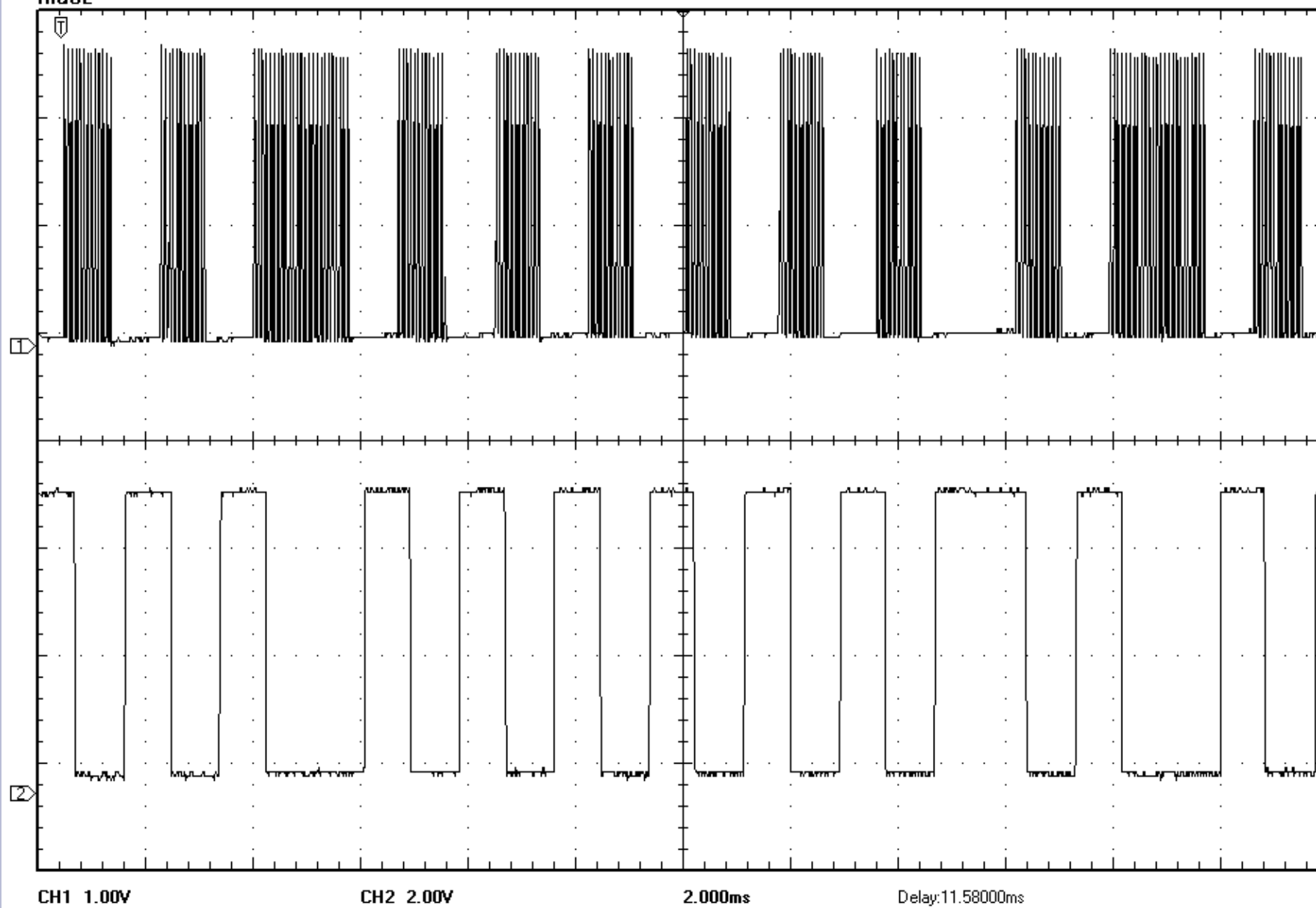
- Verbreitet zum Steuern von Geräten:
- RC5
- NEC
- SIRC

Quelle: [1]

RC5

- Codierung: Manchester
- Spezifikation: Philips
- Träger: 36 kHz
- Bitzeit: 1.7ms
- Daten
 - 2 Startbits (konstant 1)
 - 1 Togglebit
 - 5 Bit Adresse
 - 6 Bit Kommando
 - => 14 Bit

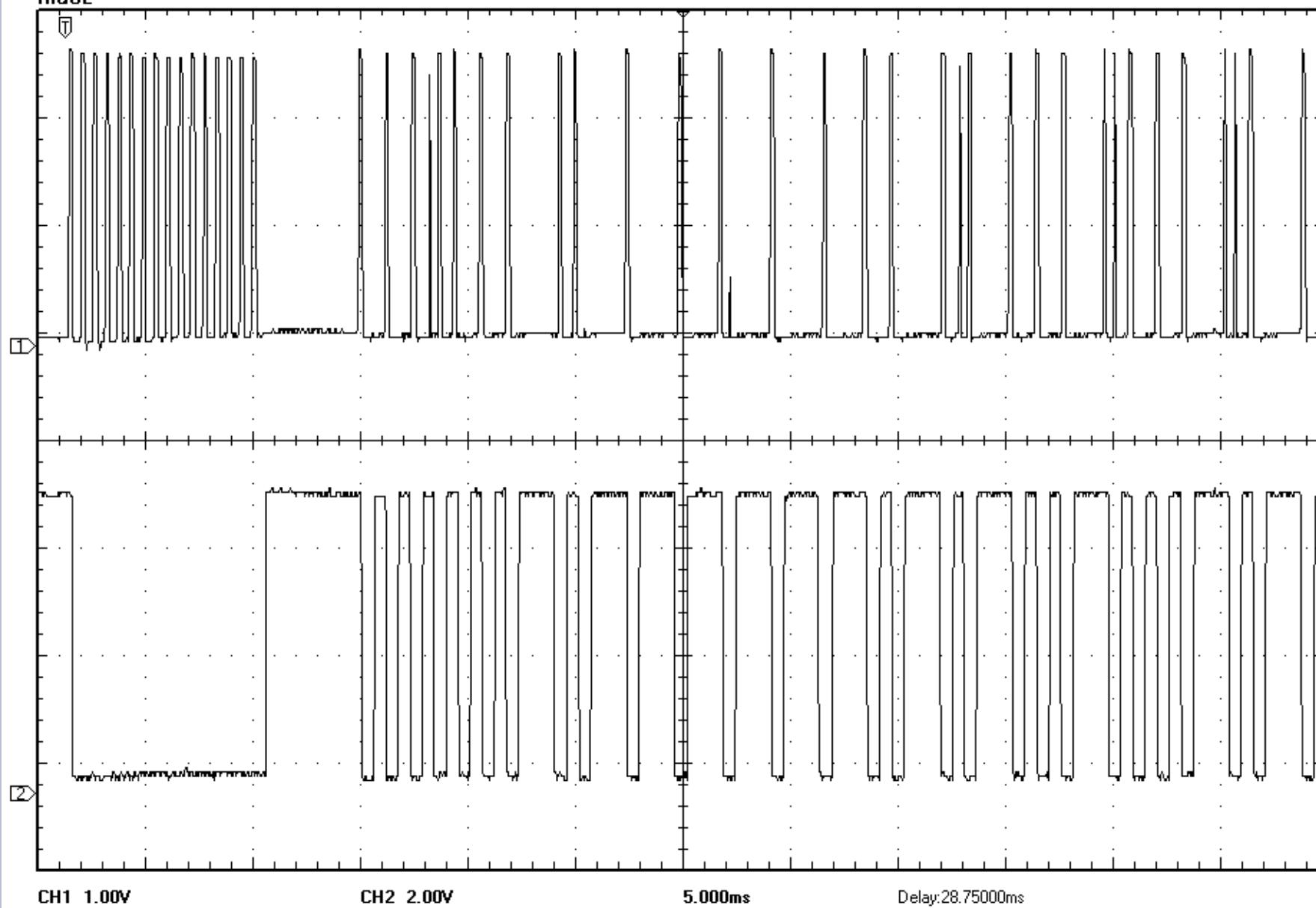
RIGOL



NEC

- Codierung: Pulsdistanzmodulation
- Spezifikation: Unklar, vermutlich NEC
- Trägerfrequenz: 38 kHz
- Header: 9ms Puls, 4.5ms Pause
- Daten
 - 8 Bit Adresse, 8 Bit inverse Adresse
 - 8 Bit Kommando, 8 Bit inverses Kommando
 - => 32 Bit
- Eins: 0.5ms Puls, 1.7ms Pause
- Null: 0.5ms Puls, 0.5ms Pause

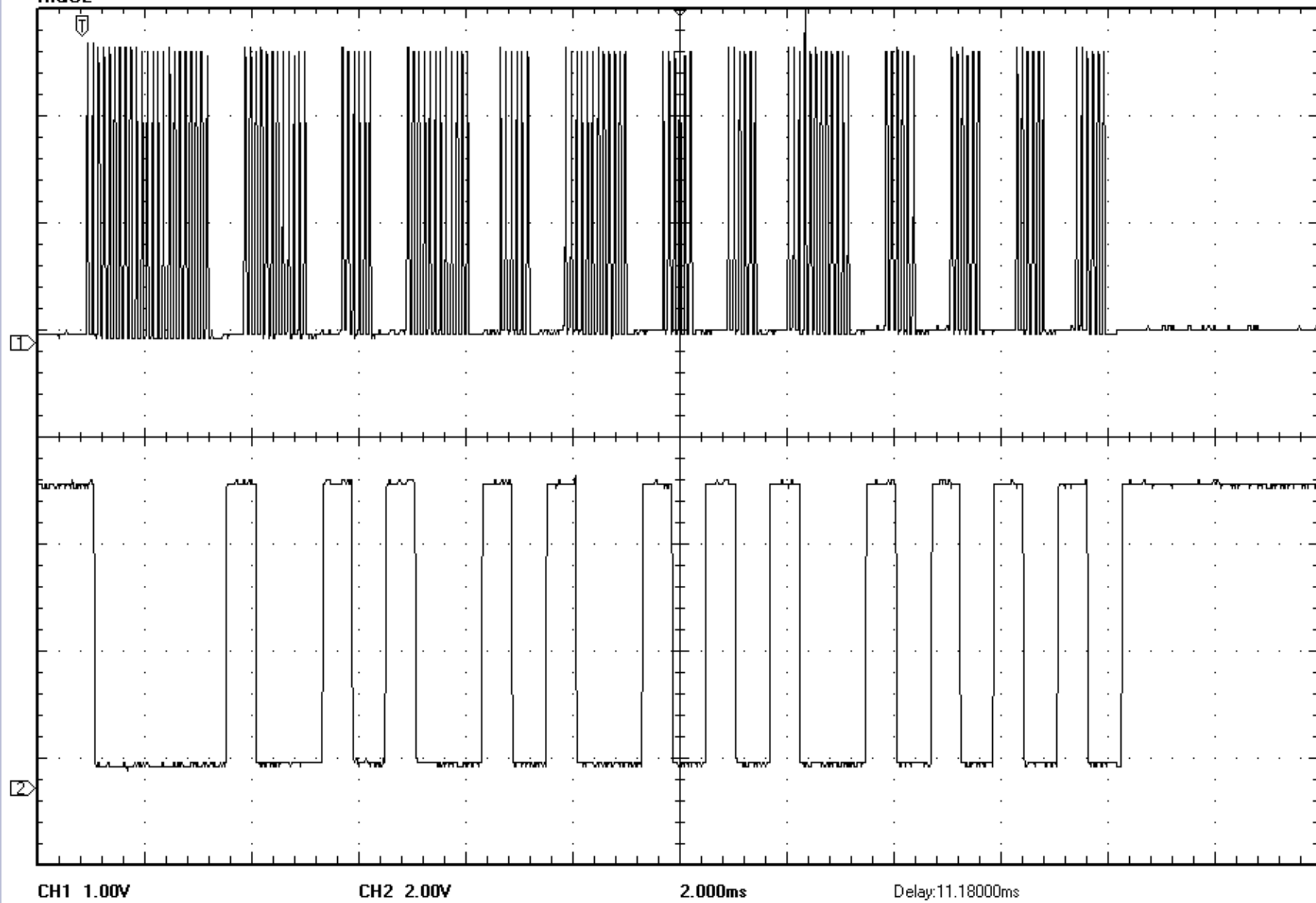
RIGOL



SIRC

- Codierung: Pulsbreitenmodulation
- Spezifikation: Unklar, vermutlich Sony
- Trägerfrequenz: 40 kHz
- Header: 2.4ms Puls, 0.6ms Pause
- Daten: 12, 15, 20 Bit, Verteilung unklar
- Eins: 1.5ms Puls, 0.6ms Pause
- Null: 0.6ms Puls, 0.6ms Pause

RIGOL



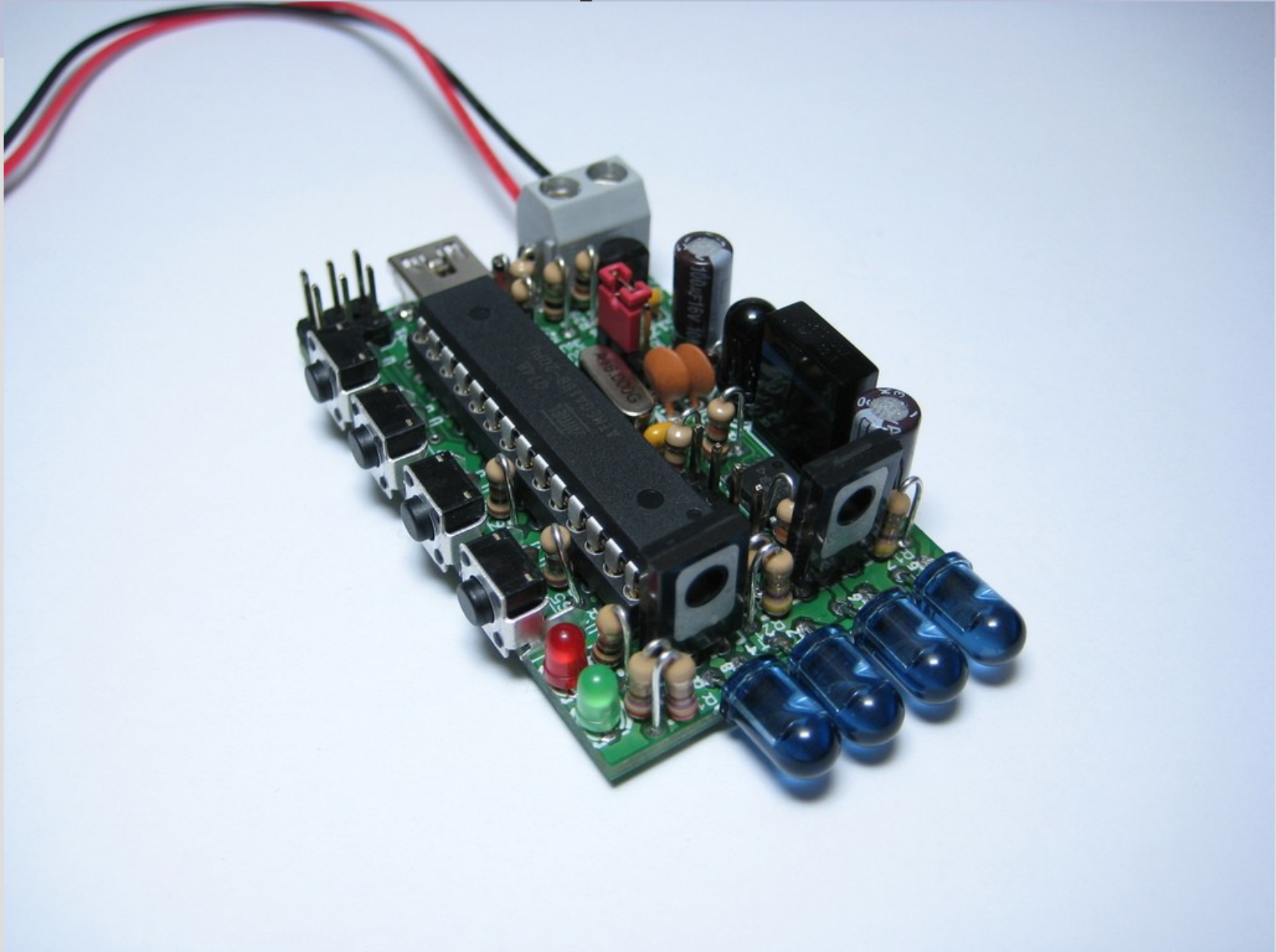
Informationsgewinnung

- Sehr wenig Dokumentation verfügbar
- Eigentlich nur RC5 richtig spezifiziert
- Gute Quellen:
 - Universalfernbedienungen
 - Datenblätter vom Empfängern
 - TV-B-Gone Projekt ([2], [3])
 - Ausprobieren

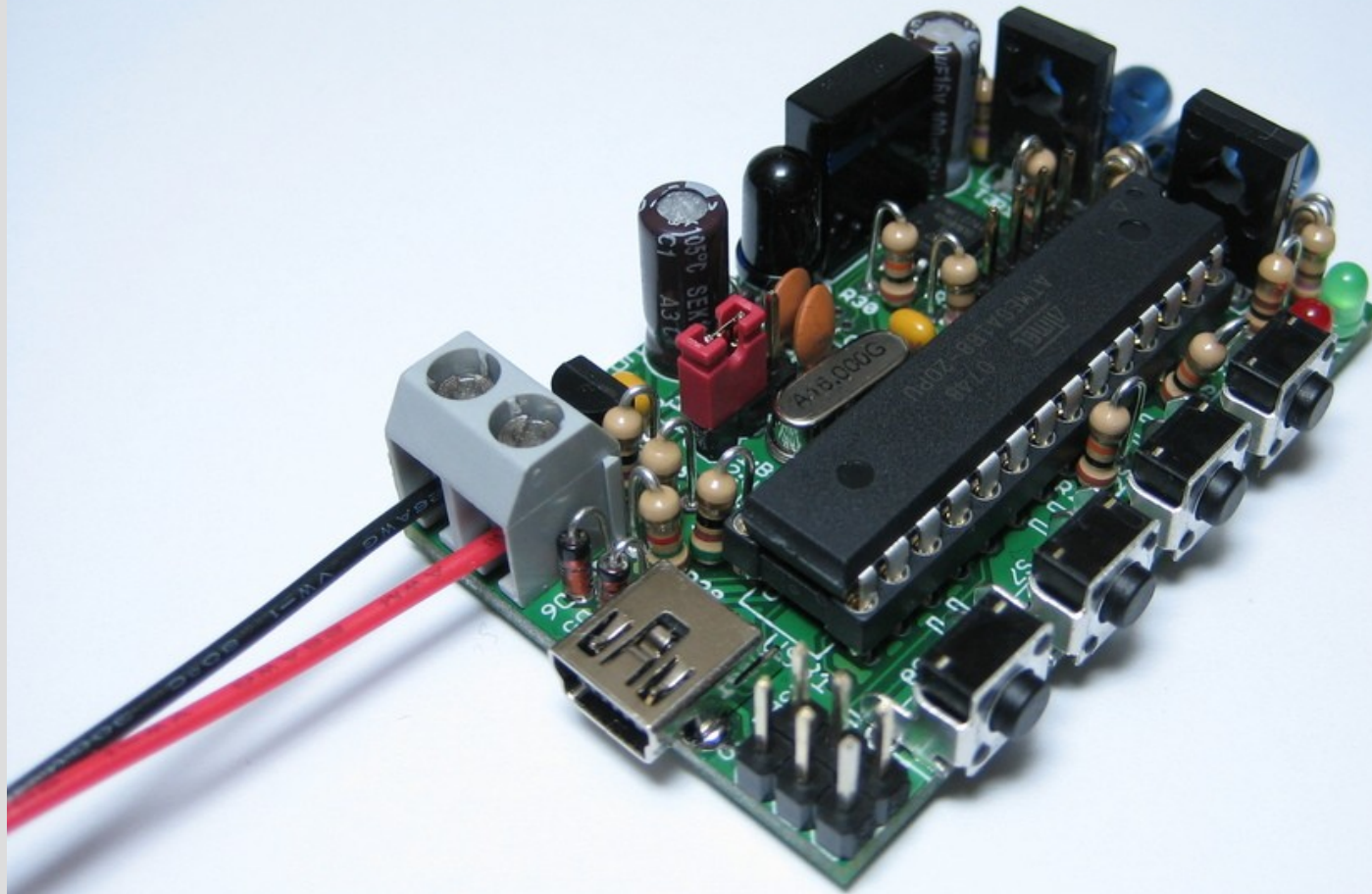
Hardware “unzap”

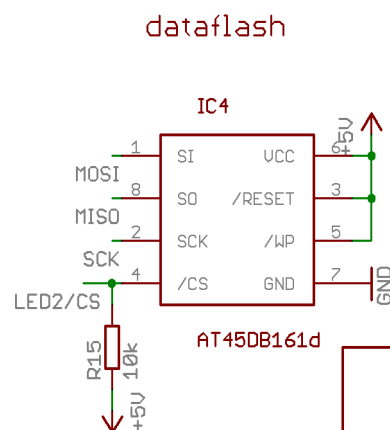
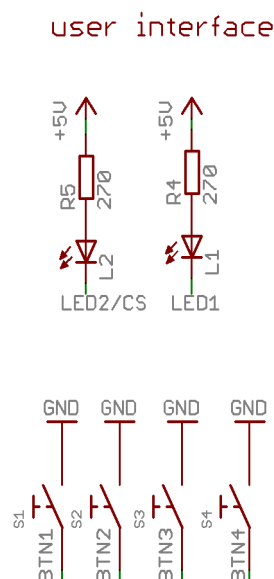
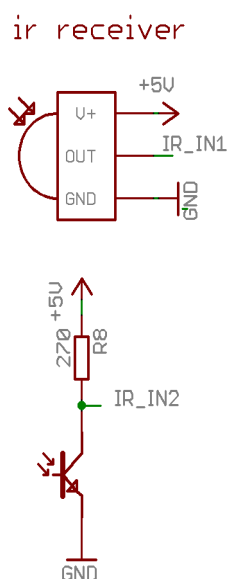
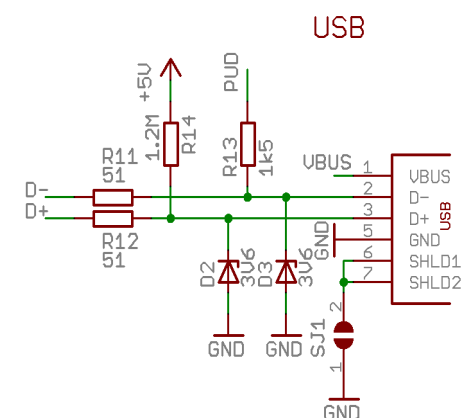
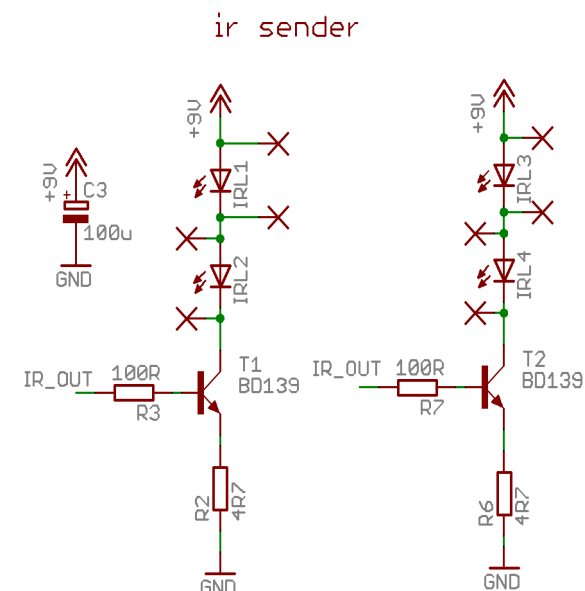
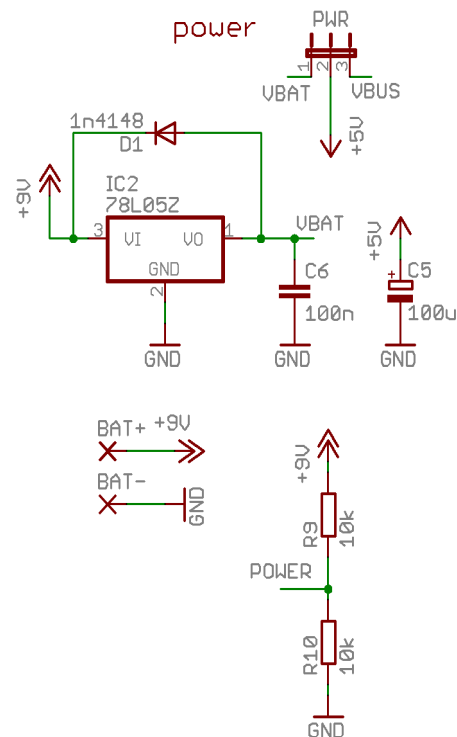
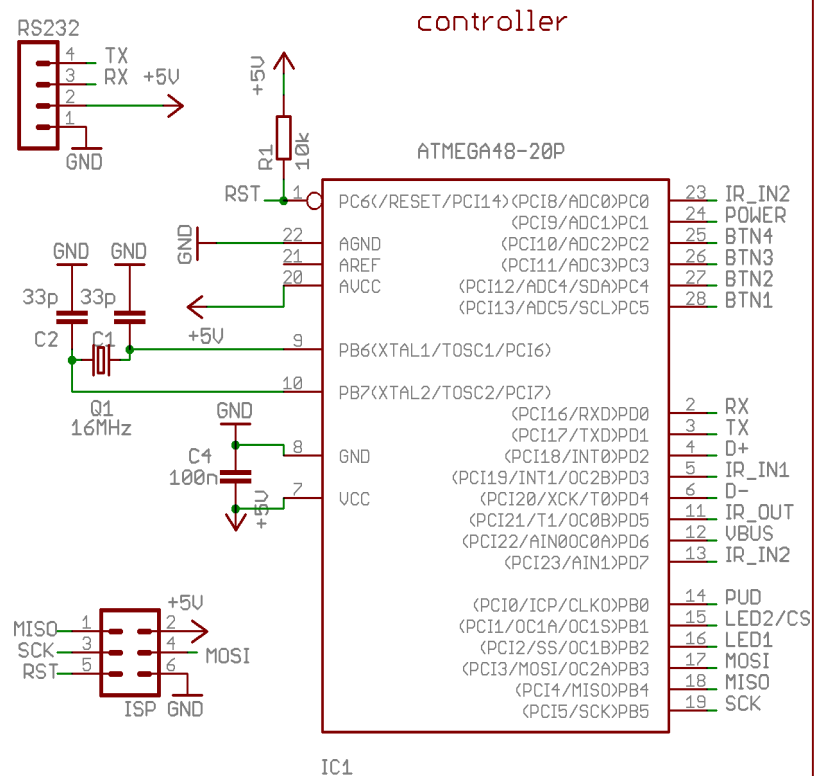
- Idee: Entwicklung eigener Hardware
- Eckdaten:
 - Klein, günstig
 - Lernfunktion für Codes
 - Code und Trägerfrequenz lernen
 - Viel Speicher (2MB)
 - Dadurch Langzeitaufnahmefähigkeit
 - Geringer Stromverbrauch (<10mA, 9V)
 - Einfache Schnittstelle (USB)
 - IR-Sender und Empfänger über USB ansteuern
 - Firmware-Upgrade über USB
 - TV-B-Gone Emulation
 - Bausatz

“unzap” Bilder



“unzap” Bilder





Lernfunktion

- Alle Protokolle lassen sich als Sequenz von Puls-Pausenzeiten darstellen
- Dadurch ist selbst Lernen von unbekannten Codes möglich
- RAM: 1024 Byte
 - 700 Byte für Lernfunktion
 - 350 16Bit Integer
 - 175 Puls/Pausenzeiten
 - Fazit: Reicht zum lernen sehr vieler Codes!

Penetrationstests

- DVD-Player regionfree schalten
- Fernseher bei MediaMarkt/Saturn ausschalten -> Social Engineering
- Steuern von Gleisanlagen [5]
- Abrechnungssysteme in Hotels laufen meist über das Fernseh-Infrarotsystem, Vortrag von MajorMalfunction [4]

Ergebnisse

- Windows-Desktop vom Backend-Server
- Raumstatus (sauber, verdreckt)
- Minibar-Abrechnung
- “Adult” Freischaltung
- Andere Gäste beim Surfen beobachten
- ...

Finden von versteckten Codes

- 1) Fernbedienungsprotokoll herausfinden
- 2) Code mit gut sichtbarem Effekt (Power) suchen
- 3) Bits einzeln durchgehen und umkippen
 - Code funktioniert -> Bit ist unwichtig
 - Code funktioniert nicht -> Bit ist wichtig
- 4) Nicht belegte Codes testen, unwichtige Bits weglassen

Weitere Ideen

- MediaMarkt/Saturn Alarmanlage bei Handy-/Digitalkameraauslagen lernen
- Was überträgt die ASEAG mit ihren Infrarotbaken?
- Infrarotkommunikation “hörbar” machen?

Ausblick

- Hardware wird nie wirklich “fertig”
- Steuern Sender/Empfänger über USB
- Hardware als Bausatz
- Open Source – Jeder kann mitbauen!
- Infrarot omnipräsent -> spannend!

Danke fürs Zuhören!

<http://www.lochraster.org/unzap>

Quellen

- [1]: [IR Knowledgebase](#)
- [2]: [TV-B-Gone](#)
- [3]: [TV-B-Gone Sourcecode und Schaltung](#)
- [4]: [22c3: MajorMalfunction: Infrared Hacking](#)
- [5]: [Heise: Fernbedienung lässt Züge entgleisen](#)