

16. Elektronik-Stammtisch: Logic Analyzer

Axel

Attraktor e.V.

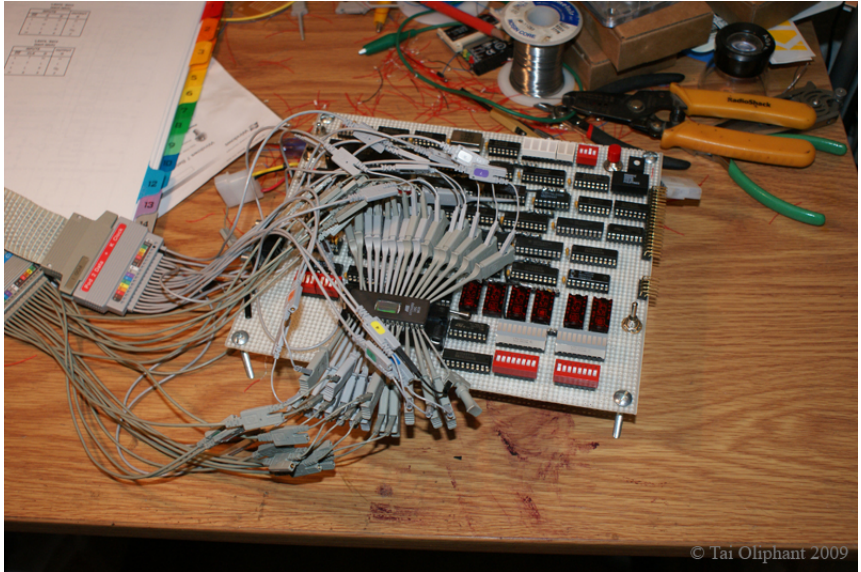
6. Mai 2013

Was ist ein Logic Analyzer

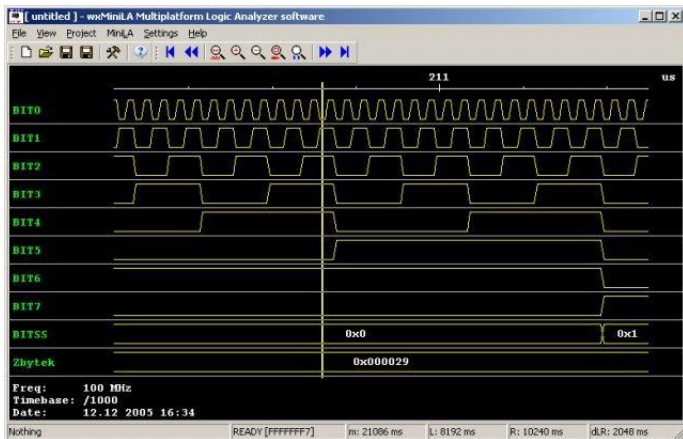
- Messgerät für digitale Signale
- Spannungsverläufe werden an Eingängen digital interpretiert
- Digitale Signale werden so gemessen, aufgezeichnet und analysiert
- Viele Eingänge die gleichzeitig genutzt werden
- Besonders für parallele Bus-Systeme geeignet
- Digitaler Verwandter des Oszilloskop



Übersicht: Verwendung eines Logic Analyzers



Übersicht: Verwendung eines Logic Analyzers



Warnhinweis: Die Aussagen in diesem Vortrag sind bis ca. 50 MHz zugelassen!

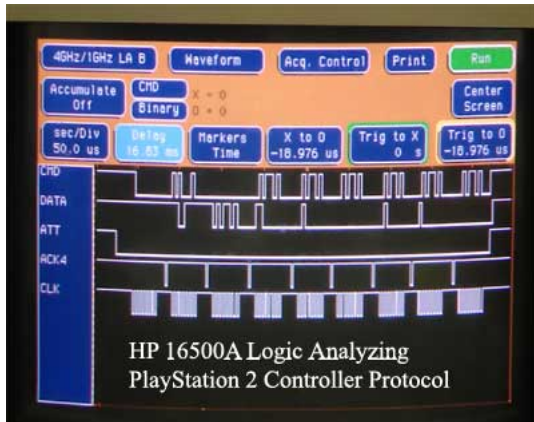


Wofür setzt man Logic Analyzer ein? (I)

- Prüfen der digitalen Kommunikation zwischen zwei Chips oder Geräten. (Daten-/Adress-Bus, SPI/I²C)
- Entwicklung von Low-Level Bibliotheken zur Chip-Ansteuerung
- Verifikation von Verhalten
- Debugging von Code- oder Logik-Fehlern
- Debugging von Firmwares und Programmcode
- Reverse Engineering(!)

Wofür setzt man Logic Analyzer ein? (II)

- Reverse Engineering von Protokollen, Schnittstellen und Geräten!
- Device Hacking!



Wofür setzt man Logic Analyzer ein? (III)

- Chip-Entwicklung (ASICs)
- Entwicklung von Speicher-Controllern und -Bussen
- FPGA-Entwicklung

**Diese Anwendungsfelder kommen im Hobby-Bereich eher selten vor.
Logik-Analyzer die hierfür tauglich sind, sind außerhalb eines
Hobby-Budgets!**

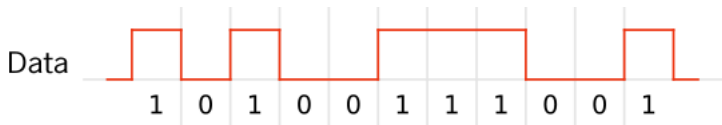
Wofür setzt man Logic Analyzer eher nicht ein?

- Eher nicht zur Analyse von Übertragungsfehlern
- Timing-Probleme
- Eingestrahlte Störungen
- Bandbreitenbegrenzung/Dämpfung
- Spannungs-Level

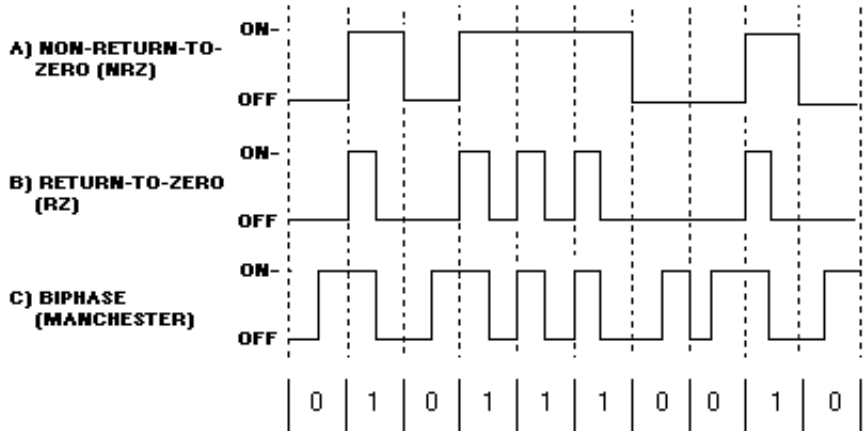
**Um mit einem Logic-Analyzer halbwegs frustfrei zu arbeiten sollten auf der analogen Ebene möglichst keine Probleme bestehen!
Bei Fehlersuche ggf. vorher/gleichzeitig zum Oszilloskop greifen!**

Wie funktioniert digitale Übertragung?

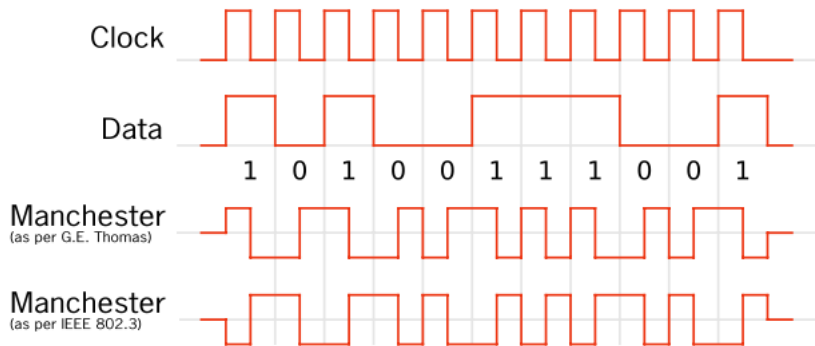
- Eine Spannung wechselt über die Zeit zwischen zwei Werten: **High** und **Low**
- **Low**: Meistens 0 Volt, kann aber auch darüber oder darunter liegen
- **High**: Oft 5 Volt oder 3,3 Volt; Höher als Low
- **High** und **Low** können, müssen aber **nicht** den Binärwerten 0 und 1 entsprechen¹. Dies hängt von der Codierung ab!
- Sender legt Spannungen an, Empfänger interpretiert, was er sieht



Wie funktioniert digitale Übertragung?



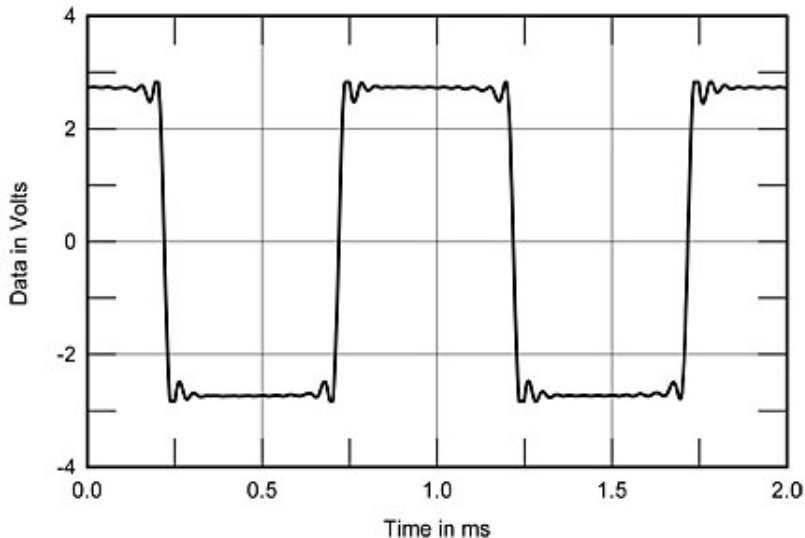
Wie funktioniert digitale Übertragung? (II)



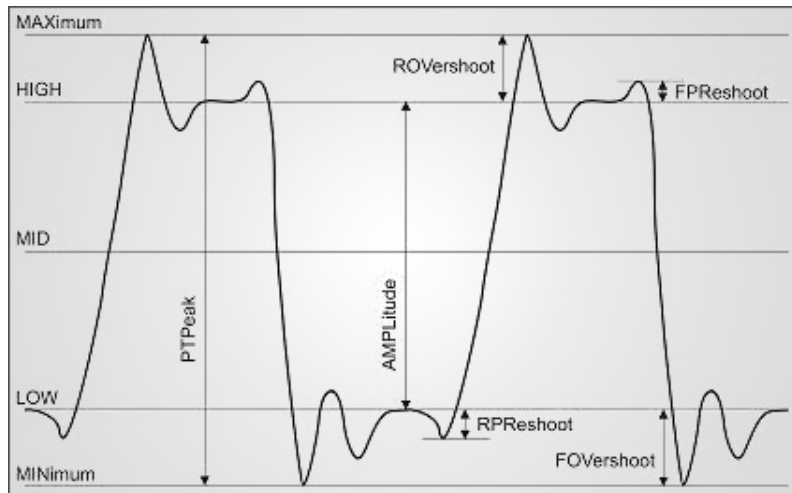
Digitale Formate mit mehr als zwei Spannungswerten können für Logik Analyzer ein Problem darstellen.

Empfang von digitalen Signalen

Medien sind nicht perfekt, ihre Bandbreite ist immer begrenzt. Perfekte Rechteck-Wellenformen würden eine unendliche Bandbreite erfordern.



Empfang von digitalen Signalen

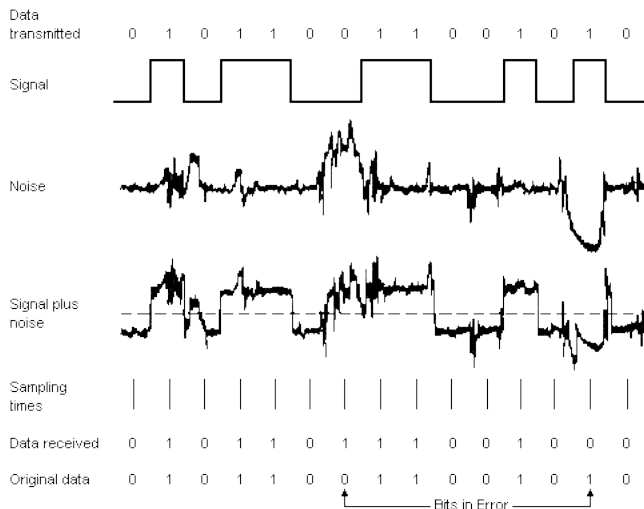


Empfang von digitalen Signalen

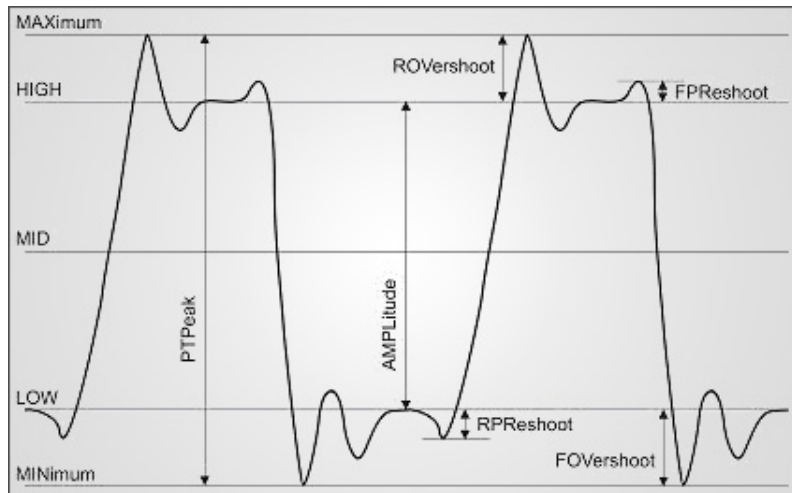
In der Praxis treten sehr viele weitere Probleme auf!

- Eingestrahlte Störungen (Platine oder von extern, z.B. Schaltnetzteile, Leuchtstoffröhren)
- Unsauberkeiten des Senders
- Messfehler beim Empfänger
- Probleme mit Kontakten/Lötstellen (insb. bei Experimentierplatinen)

Empfang von digitalen Signalen



Interpretation durch den Logic Analyzer oder Empfänger



Interpretation durch den Logic Analyzer

- Definition einer Schwellwertspannung
- Alles, was darüber liegt ist **High**, alles darunter ist **Low**
- Definition, **wann** der Zustand der Leitungen interpretiert wird
- Angeschlossene Leitungen werden nach Start der Aufzeichnung kontinuierlich gelesen und so eine Bit-Folge erzeugt.

Vergleich zwischen Logic Analyzer und Oszilloskop

Logic Analyzer und Oszilloskop haben viele Gemeinsamkeiten, aber auch viele Unterschiede.

Logic Analyzer	Oszilloskop
eher ein Spezial-Gerät	Standard-Gerät
interpretiert digital	interpretiert analog
bis zu hunderte von Eingängen	2 oder 4 Eingänge
immer digital	analog oder digital
speichert immer	speichert, wenn digital
meist sehr komplexe Trigger	eher einfache Trigger
verdeckt große Teile des Signals	zeigt das ganze Signal
aufzeichnung einzelner Bitfolgen	häufig für periodische Signale
sehr billig bis extrem teuer	teuer bis absurd teuer

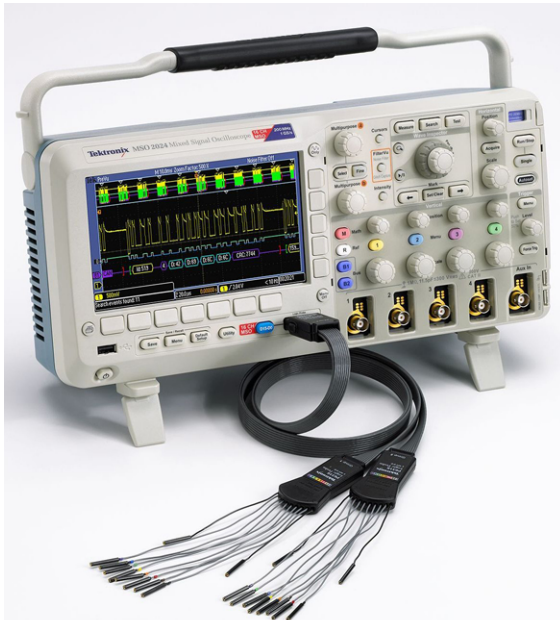
Typen von Logic-Analysern: klassische Stand-Alone Geräte



Typen von Logic-Analysern: PC-basierte



Typen von Logic-Analyzern: Mixed-Signal Oszilloskop



Kenndaten eines Logic Analyzers

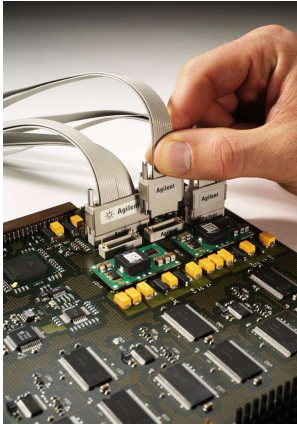
- Maximale Abtastrate in MHz? (je Modus)
- Speichergrösse
- Anzahl der Eingänge
- Trigger-Arten
- Protokolle und Decoding-Möglichkeiten

Verwendung eines Logic Analyzers

- Masse (GND) verbinden
- Clock (CLK) verbinden (falls benötigt/vorhanden)
- Weitere Datenleitungen verbinden (freie aus dem Weg räumen oder erden)
- Verkabelung im Logic Analyzer abbilden
- Trigger konfigurieren
- Starten!



Alternativen zu Einzel-Sonden



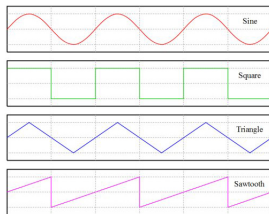
Kenndaten eines Logic Analyzers

- Maximale Abtastrate?
 - ▶ In welchem Modus? Mit wievielen Eingängen?
- Anzahl der Eingänge
- Speichertiefe
 - ▶ Bei welcher Geschwindigkeit? Kompression?
- Trigger
 - ▶ Welche Arten? Einfach/Komplex? Kombinierbar?
- Protokoll-Dekotierung
- Spannungs-Level

und viele weitere, die hauptsächlich bei höheren Frequenzen relevant werden..

Spannungsniveaus und Sampling

- Zu jedem Sampling-Zeitpunkt werden alle Eingänge gelesen und deren digitaler Wert bestimmt. Störungen
- Alle Eingänge werden rein Digital gelesen, Gefahr eines Blindflug
- Spannungsniveau hängt von der Logik-Familie ab
- TTL (0V/5Volt): Schwellwert: 1,4 Volt
- CMOS (0V/3,3Volt oder 5Volt): $V_{CC}/2$: 2,5V oder 1,5Volt
- In der Praxis sind 1,5 Volt meist ok.



Analyse Methoden

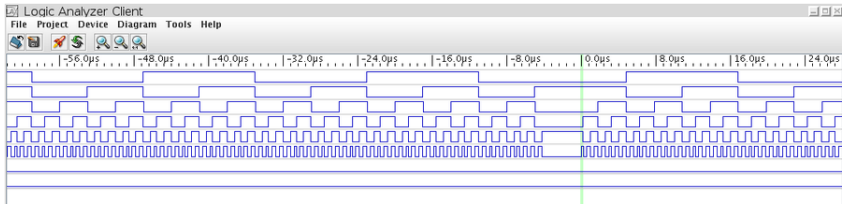
- Zeit-Analyse (Time Analysis)
 - ▶ Leitungen werden in festen Zeit-Abständen gemäss interner Uhr gelesen
 - ▶ Hohe Abtastrate
- Zustands-Analyse (State Analysis)
 - ▶ Leitungen werden auf Grund externer Ereignisse gelesen
 - ▶ Stark Reduzierte Abtastrate (Hälfte und weniger)
 - ▶ ähnlich einem Trigger

Man verwendet meistens Zeit-Analyse

- Speicherung der Analysedaten
 - ▶ Speicherung in Speicher-Worten
 - ▶ Optional Speicher-Kompression

Triggering

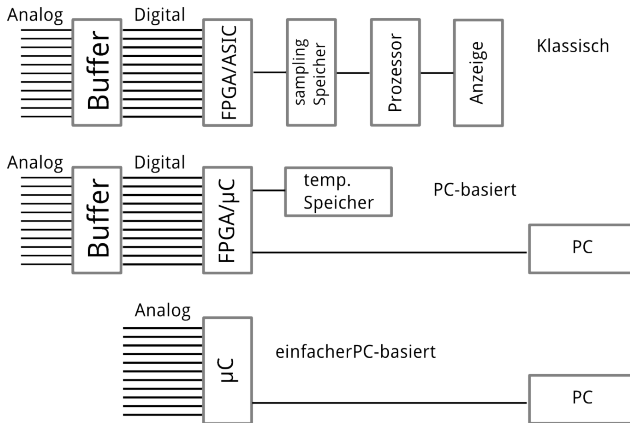
- Arming, Trigger, Aufzeichnen, Ende
- Arming: Abhören der Leitungen und warten auf den Trigger
- Trigger: Bedingung, die die Aufzeichnung auslöst
- Aufzeichnungs-Fenster: Vor und/oder nach dem Fenster
- Aufzeichnung daher schon während der Arming-Phase
- Aufzeichnungs-Zeitraum ist fest, Position des Triggers darin ist wählbar



Interner Aufbau eines Logic Analyzers

- Eher einfach aufgebaut
- Analoger Teil
 - ▶ Sonden
- Digitaler Buffer oder A/D-Wandler
- Digitaler Teil
 - ▶ Sampling-Speicher
 - ▶ Trigger-Logik
- Speicherung/Anzeige

Interner Aufbau eines Logic Analyzers (II)

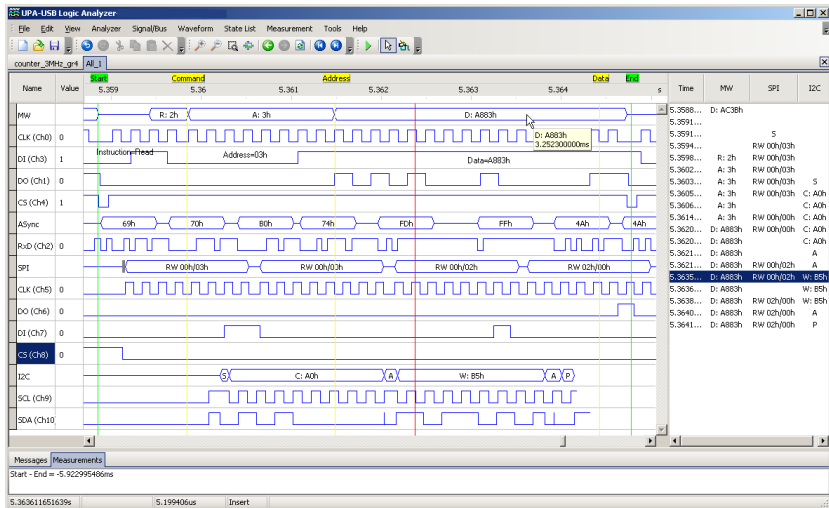


Protokoll-Decoding

Viele Logic-Analyzer unterstützen Protokoll-Dekodierung.

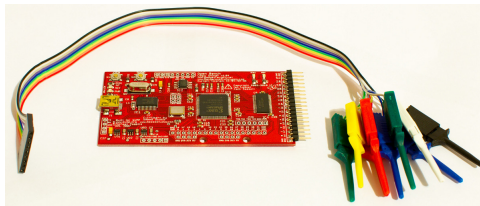
- Leitungen werden Rollen in einem Protokoll zugewiesen (z.B. Clock, Data, Chip Select)
- Serielle Protokolle: SPI, I2C, UART, USB
- Parallel: Adresss- und Speicherbusse (Adress- und Inhalts-Dekodierung)
- Wird als weitere, virtuelle Leitungen eingeblendet
- Bei Dekodierung nach der Aufzeichnung nur für die Anzeige
- Bei Dekodierung in Echtzeit können diese für Trigger verwendet werden
 - ▶ Triggering auf bestimmte Werte/Befehle
 - ▶ Triggering auf Protokoll-Fehler
- Echtzeit-Decoding meist nur bei teureren Geräten

Protokoll-Decoding (II)

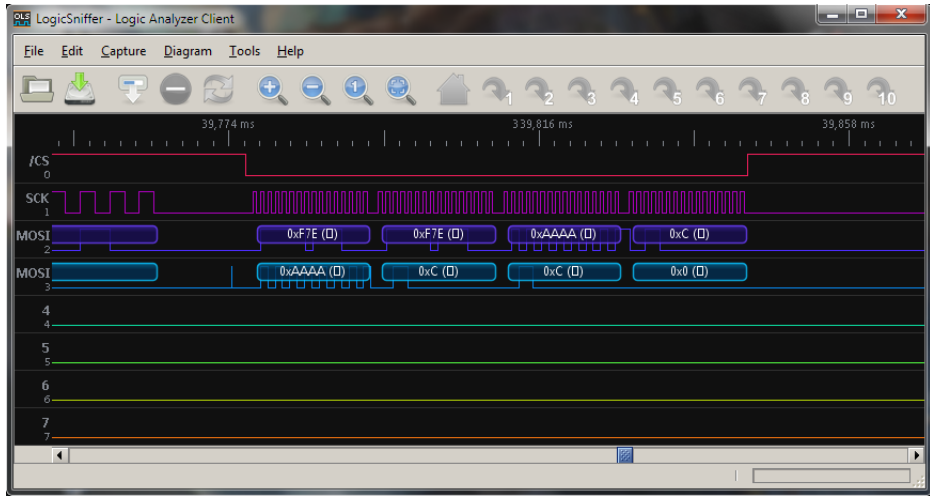


Open Bench Logic Sniffer

- Open Hardware von dangerousprototypes.com (etwa 45Euro)
- 100MHz sampling bei 16 Eingängen (oder 32Eingänge@50MHz)
- Verschiedene Clients (OLS <http://www.lxtreme.nl/ols/>), Erweiterbar da Open Source! Sehr gut für Protokoll-Decoder! Java
- 216K RAM (24kS@8channel, 12kS@16channel, 6kS@32channel)

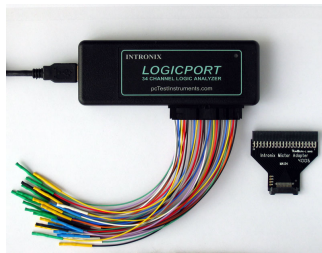


Open Bench Logic Sniffer (II)

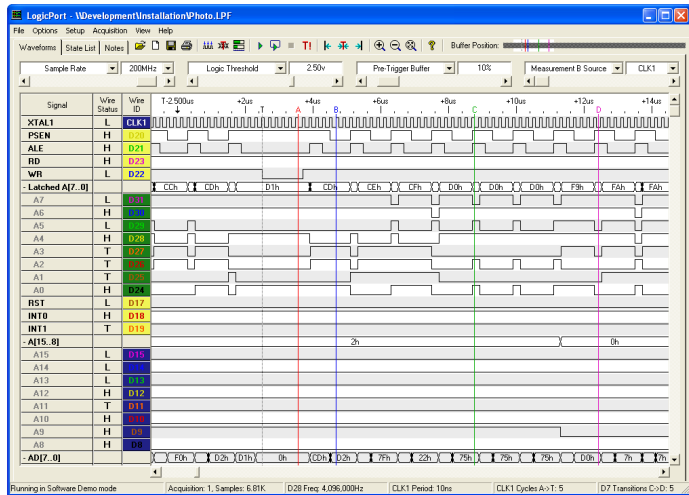


Intronix Logicport

- Kommerzieller, PC-basierter Logic-Analyzer (etwa 350Euro)
- 34 Eingänge
- 500MHz sampling bei zeitbasierter Aufzeichnung
- 200MHz sampling bei zustandsbasierter Aufzeichnung
- 34 x 2048 samples (unterstützt Sample Compression)
- Einstellbare Spannungs-Schwellwerte
- Decoding diverser, serieller Protokolle



Intronix Logicport (II)



Hewlett Packard 1663C

- Kommerzieller, klassischer Logic-Analyzer (ca 15 Jahre alt, “war mal sehr teuer”)
- 34 Eingänge
- 500MHz sampling zeitbasiert, 100MHz sampling zustandsbasiert
- 4k samples (8k bei Hälfte der Channels)
- Einstellbare Spannungs-Schwellwerte
- Sehr(!) umfangreiche und komplexe Mehrstufen-Trigger möglich!
- paralleles Decoding (Zahlen, ASCII, leider keine Protokolle)
- interne Festplatte :)

Hewlett Packard 1663C



Zusammenfassung:

- Logic Analyzer sind eine sehr nützliche Sache!
- Sie sind relativ einfach einzusetzen (bei geringen Frequenzen)...
- ... so lange man weiss, was schief gehen kann und wo Grenzen sind.
- Insbesondere zum Reverse Engineering digitaler Schnittstellen sind sie sehr nützlich



Spock Approves

There is much logic in this