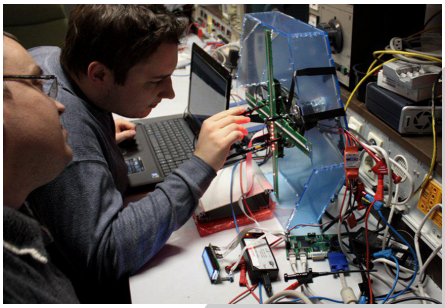
Borg Ventilator



M. Sauren (links) und P. Deppenwiese

Author: Michael Sauren
Projektbeginn: Anfang 2008
in der Öffentlichkeit: 27.12.2011 (27er Chaos Congress)

Ziel des Projektes ist es ein Videosignal auf einem Ventilator darzustellen. Dazu besitzt der Ventilator insgesamt 244 RGB LEDs verteilt auf vier Flügel. Als Datenquelle wird ein Standard VGA Anschluss verwenden. Dieses VGA Signal wird digitalisiert, aufbereitet und auf dem Ventilator dargestellt. Dabei werden Datenraten von 60 bis 150MB/s erreicht. Für normale Oszilloskope ist hier einfach kein Platz.

Datenübertragung

Demonstration 27C3

Die Daten werden induktiv und somit berührungslos übertragen. Hierfür passende Spulen lassen sich zum Beispiel in der Kopftrommel von alten Videorekordern finden. Für die induktive Übertragung der Daten, das dem Prinzip eines Trafos nicht unähnlich ist, ist es notwendig das Signal gleichspannungsfrei zu halten. Das Taktsignal des ersten FPGAs wird mit Hilfe der Datenübertragung für den zweiten FPGA, der z.B. für das Steuern der Helligkeit zuständig ist, zurückgewonnen. Dadurch ist es nicht notwendig zwei identische Taktsignale zu generieren. Damit dies funktioniert, wird der Leitungscode B8B10 verwendet. Die zu übertragenden Daten werden nicht, wie man annehmen könnte als Datenstrom übertragen, sondern paketweise gesendet. Ein Paket besteht aus 512 Byte Nutzdaten. Gefolgt von einer Synchronisationsnummer und zwei und einer Checksumme. Mit der Synchronisationsnummer kann der FPGA auf den Flügeln erkennen, ob er sich noch synchron zum Signal digitalisierendem FPGA befindet und sich im Fehlerfall wieder an den Ursprungstakt anpassen. Die Checksumme wird verwendet um Fehler in den Datenpaketen zu erkennen. Diese Fehler lassen sich Aufgrund der kontaktlosen Datenübertragung nicht vermeiden, werden aber erkannt und verworfen.

Seitenkanalangriffe und RFID Protokolle

Author: Markus Kasper
Vortrag: 15.12.2009

Author: Vincent
Vortrag: 23.02.2011

Bereits im Jahre 2009 wurde im Labor ein umfangreicher Vortrag von Markus Kasper über Seitenkanal Angriffe gehalten. Dieser Vortrag war für viele ein Einblick in "eine neue Welt", da auf einmal klar wurde, dass selbst wenn die Mathematik hinter einem kryptografischem Algorithmus fehlerfrei ist, dies nicht zwangsweise auch auf dessen Hardwareimplementierung zutreffen muss. Hierfür wird mit Hilfe der Simple Power Analysis (SPA) oder der Differentielle Power Analyse (DPA) versucht Informationen über einen verwendeten kryptografischen Schlüssel aus dem Chip zu extrahieren. Hierfür wird berechnendem derStromverbrauch des chips bei der Berechnung gemessen, Sicherheits- Im Labor gibt es die Möglichkeit digital gespeichert zu analysieren.Auch bei der Reverse undanalysiert. Funkprotokollen ist es unabdingbar die eigenen Chips und ihre Funktionen Engineering Analyse von Daten in digitaler Form zu haben.