Keep your tentacles off my bus: Introducing Die Datenkrake.

REcon 2013, Montréal

Dmitry Nedospasov, Thorsten Schröder

RECON

modzero

About us

Dmitry Nedospasov

- PhD Student TU Berlin

Thorsten Schröder

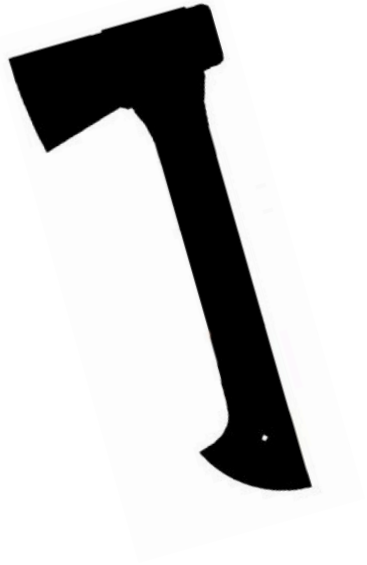
- Founder, modzero AG

Voiding Warranty

RECON

modzero

Tools



modzero

120,000€

1,100 €

LeCroy 7-Zi MSO Picoscope (4000)

Read-Only Devices

RECON

modzero

Source: Arduino Project

Arduino

Source: GoodFET Project

GoodFET

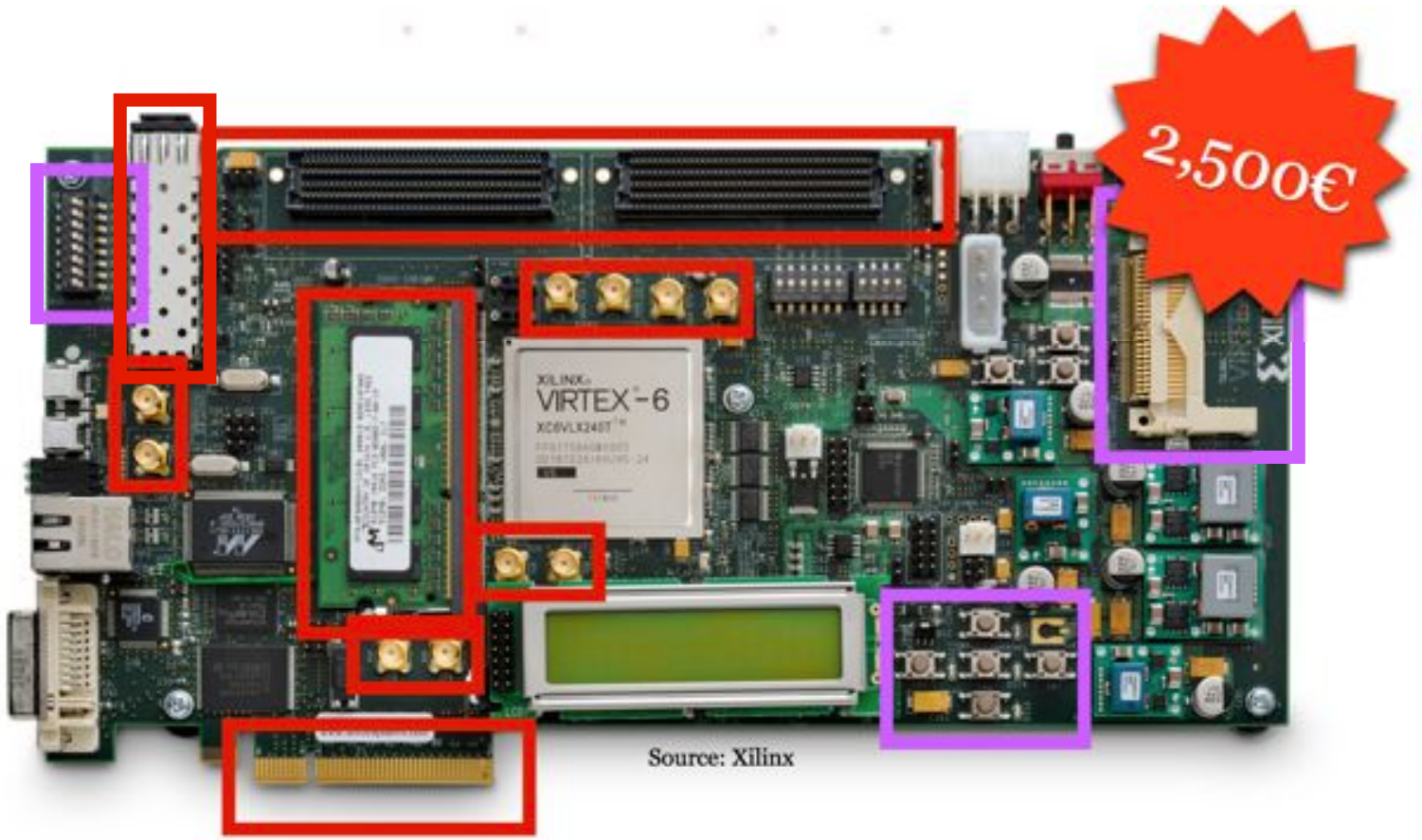
Source: http://en.wikipedia.org/wiki/File:Bus_pirate_v3a.jpg

BusPirate

µController

RECON

modzero



Feldprogrammierbare Gatteranordnungen

RECON

modzero

But wait… There are even more FPGA boards.

Source: http://commons.wikimedia.org/wiki/File:LEGO_Bits_Box_2.jpg

Source: Digilent

SASEBO

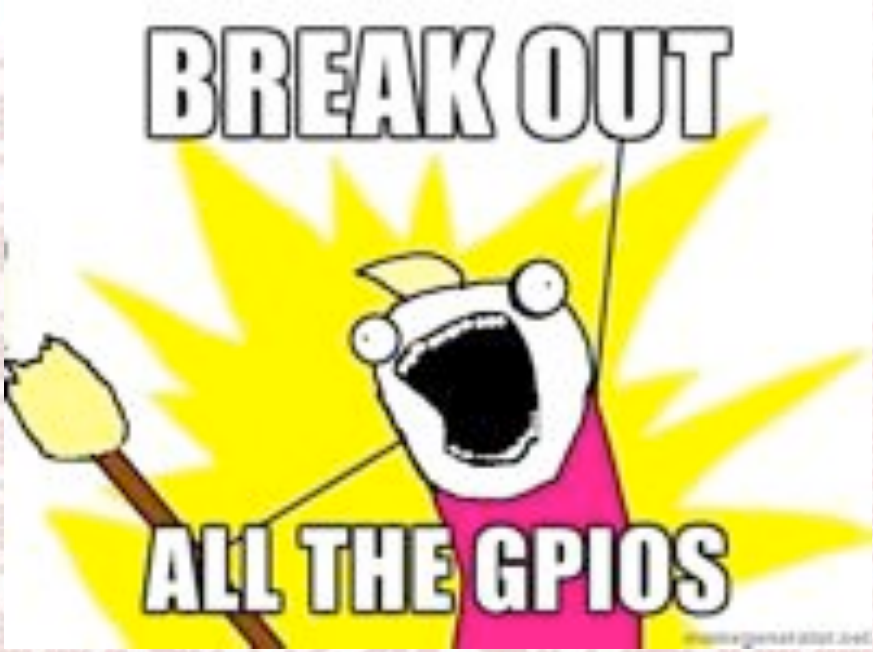
Source: Embedded Micro

Mojo

Feldprogrammierbare Gatteranordnungen

RECON

modzero



When in doubt...

Trigger-Warning

the following slide may contain traces of rainbows.

RECON

modzero

DDK Hardware

- Open-Source Hardware & Software
- User friendly interfaces and connectors
- Test pads, breakout of GPIO pins
  - Terminated & unterminated
  - Bread-boardable
- Firmware & bitstream updates via USB serial interface

DDK Hardware

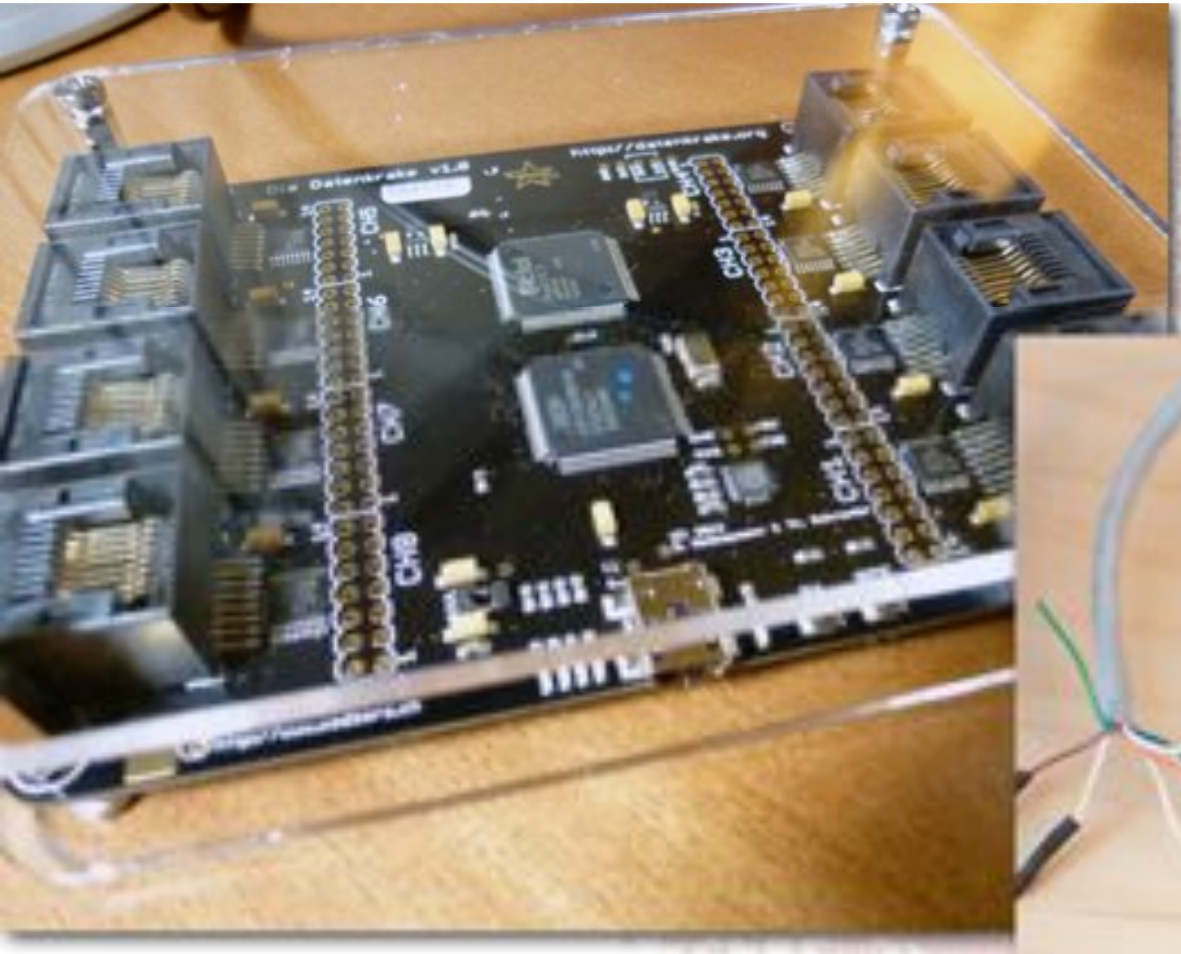
- NXP LPC1765 ARM Cortex-M3 microcontroller
  - 100 MHz, 256kB Flash ROM, 64kB RAM
- Microsemi Actel A3PN125 FPGA
  - 125k system gates, 36 kbit SRAM, 71 IO
- FTDI FT230X Serial-USB converter
  - 3Mbaud

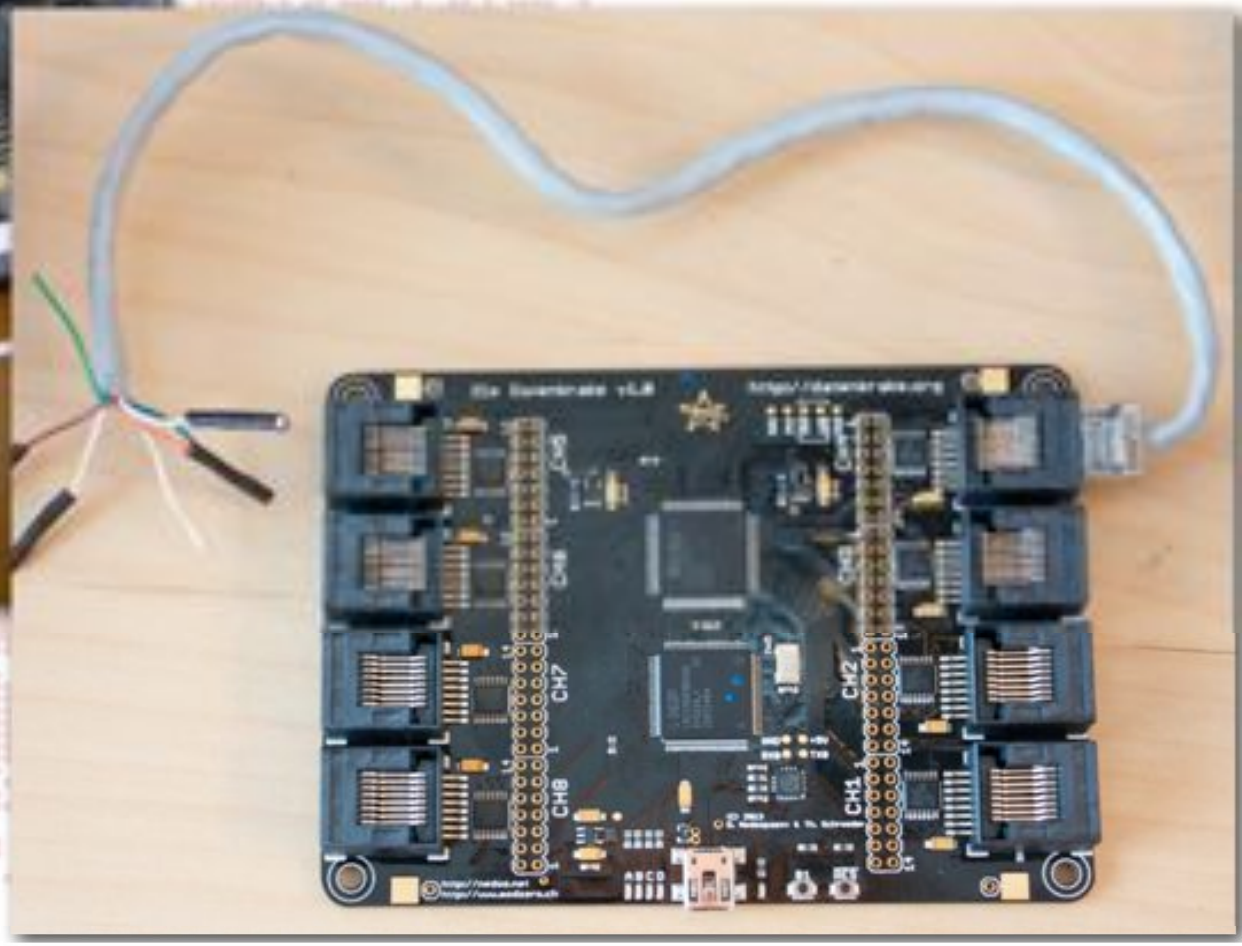
DDK Hardware

- µControler
  - Controls FPGA power and reset
  - Controls buffer power
  - Provides clock for FPGA
  - IEEE1532 ISP of FPGA

DDK Hardware

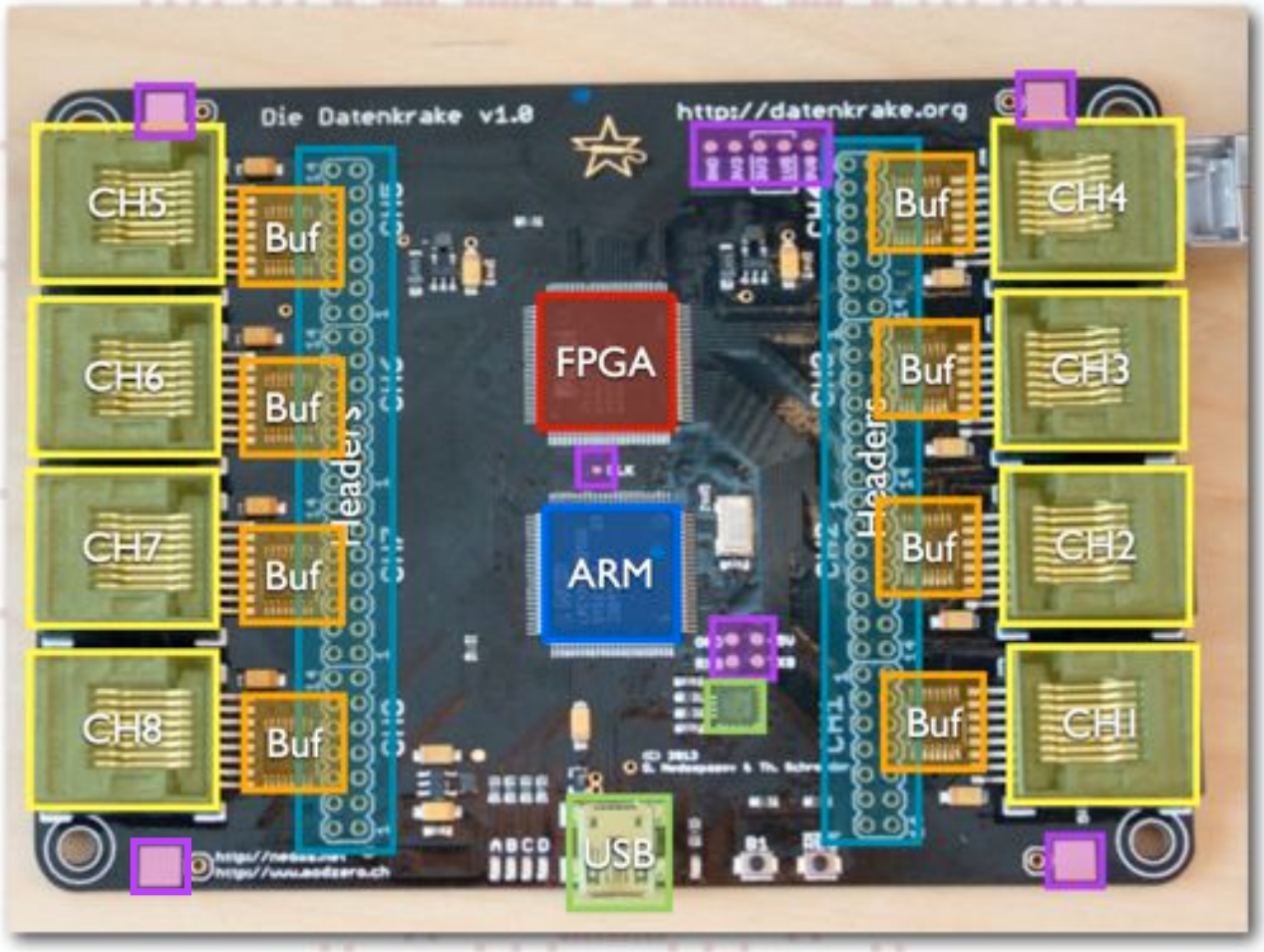
- FPGA
  - 3 UARTs / 6 GPIO interfacing the µC for data exchange
  - 16bit parallel bus interfacing the µC for data and command exchange
  - 56 general purpose 3.3/5V tolerant, terminated I/O for interfacing your targets





RECON

Die Datenkrake



RECON

modzero

DDK Software

- µController
- FreeRTOS Realtime Operating System
- Command Line Interface via USB

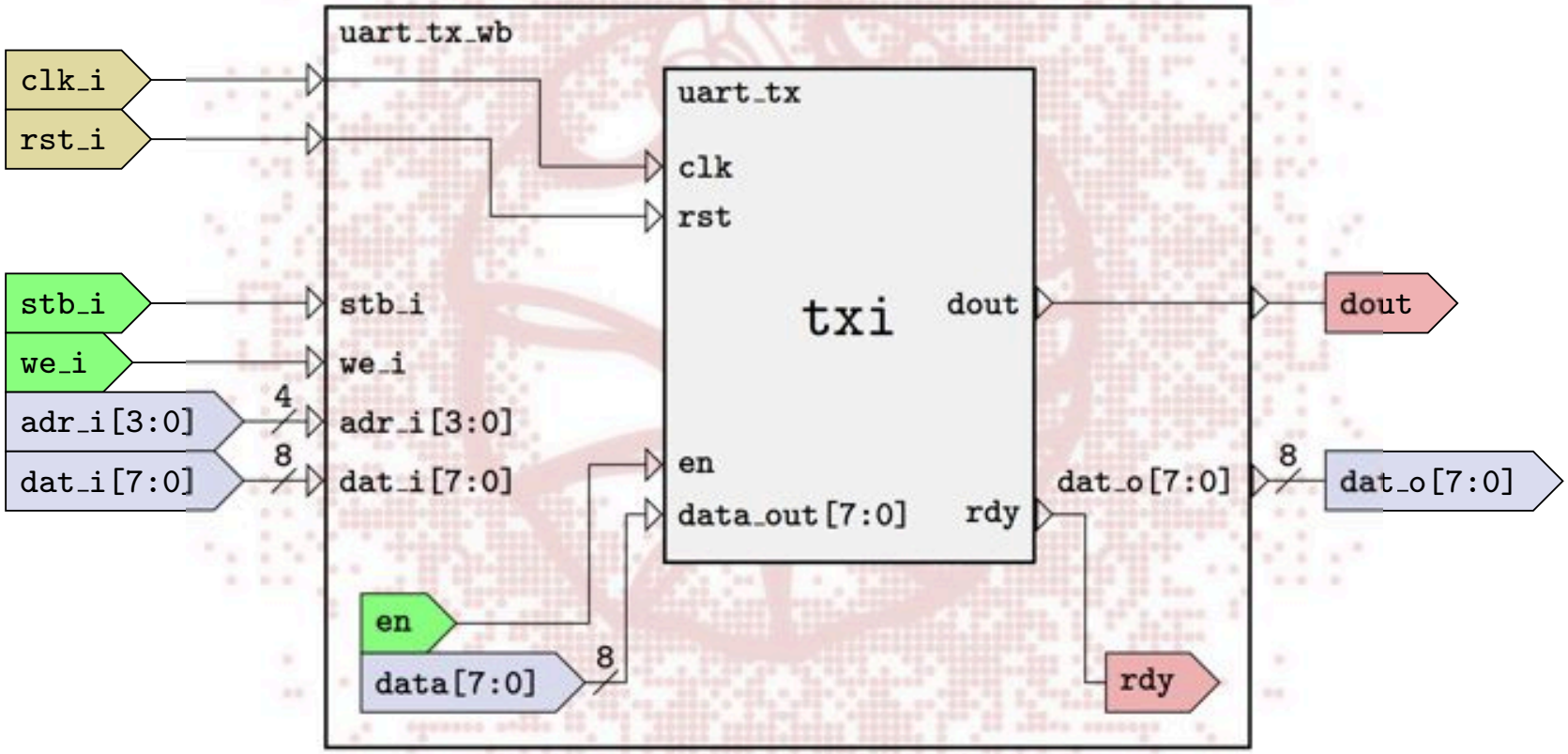
```
# help
mem      -- Various memory functions
led      -- LED control commands
fpga     -- FPGA control commands
buffer   -- Buffer/channel control commands
adv      -- Advanced commands
help     -- This help list
credits -- Display credits, greets & shoutz
reboot   -- Reset Datenkrake
R        -- FPGA reset
H        -- FPGA halt (reset high)
o        -- Power off FPGA
O        -- Power on FPGA
e        -- Buffer enable
d        -- Buffer disable
E        -- Buffer enable all
D        -- Buffer disable all
0        -- Advanced - FPGA erase flash ROM
t        -- Advanced - HW test
p        -- Advanced - Program FPGA flash ROM
l        -- LED control single
L        -- LED control all
w        -- Data write
r        -- Data read

Use '<command> ?' for details on parameters to command
#
```

DDK Logic

- Released / public version provides basic bit-banging and comm-modules
- Wishbone Bus to easily connect custom modules
- Compatible to most Wishbone compatible cores

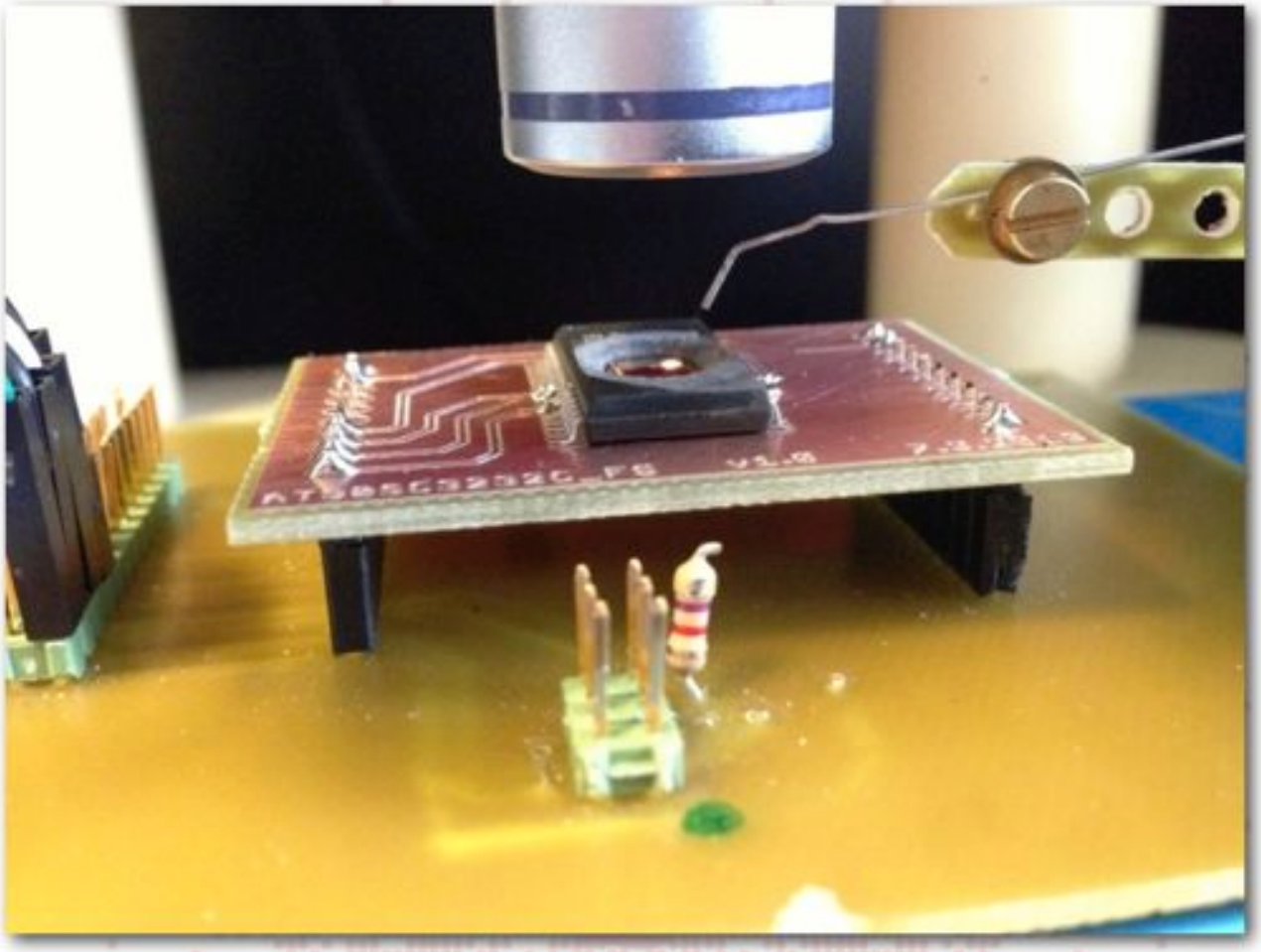
DDK Logic



Example: Connecting a UART TX module to the Wishbone

RECON

modzero



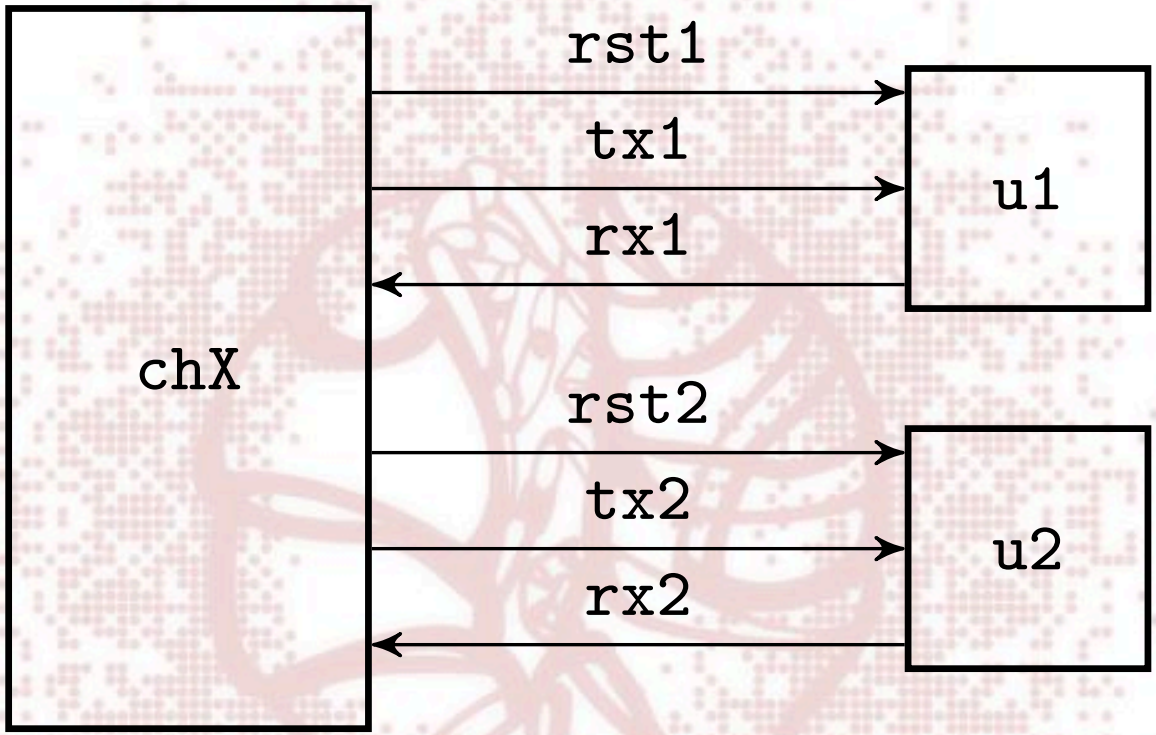
Targets

Hardware Fuzzing

- Fuzzing multiple hardware instances.
- Determine the current state of the target.
- Concurrent monitoring of embedded linux devices via serial interface
- Crash detection, target device reset and logging.
- Multiplexing signals to the device.

Odroid-U2

- Shout out **@miaubiz**
- 1.8V UART
- 5V/2A wall wart
- Single UART, multiplexed to all of the devices.
- Automatic crash detection.
- Background logging (FIFO memory).

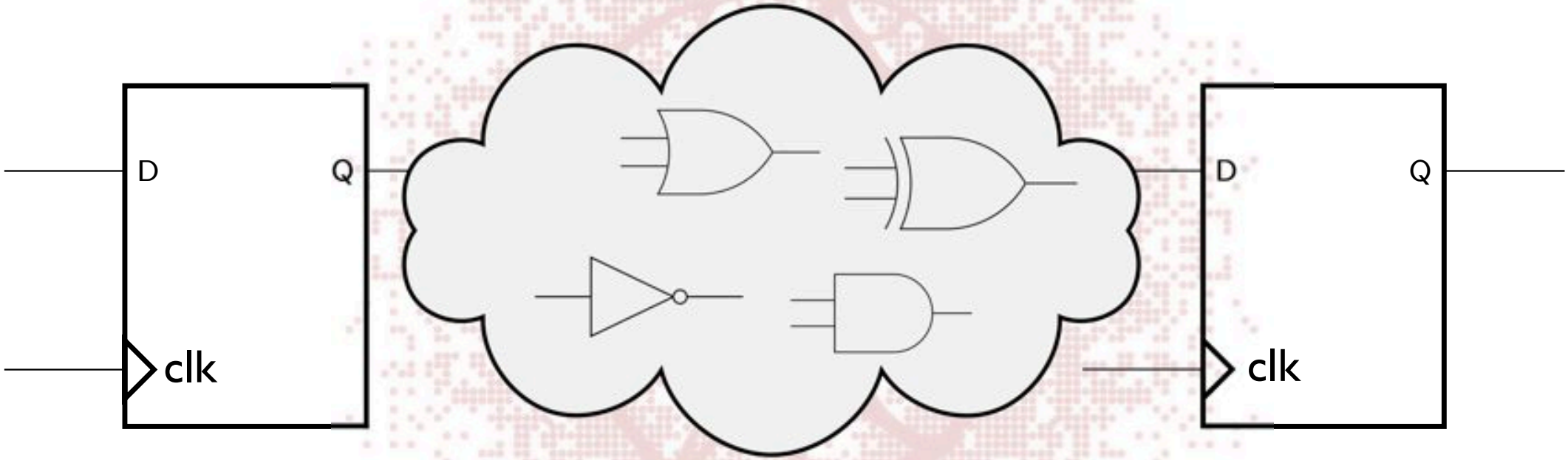


Hardware Fuzzing

Hardware Glitching

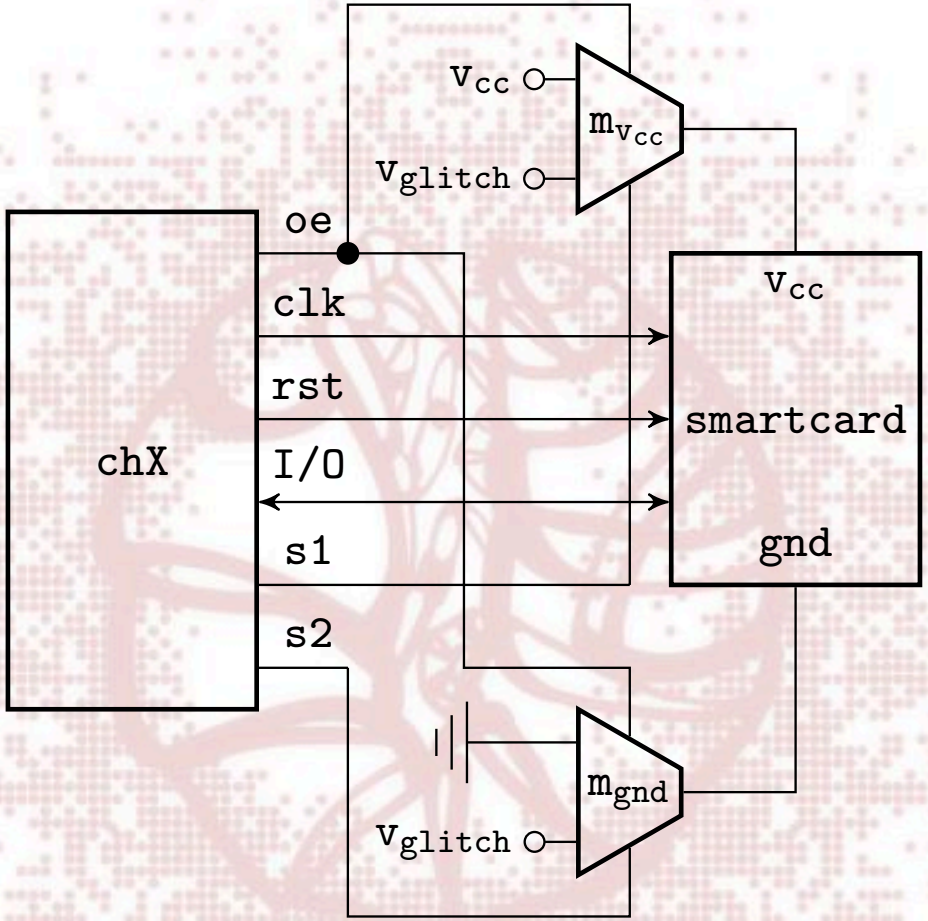
- Introducing transient, non-invasive faults (rise & hold-time violations).
- Attacks a single clock cycle. May cause "incorrect" values to be loaded into registers or memory locations.
- Require precise timing on the order of fractions of clock-cycles of the target.
- Two common forms: Voltage supply and clock glitching.

Register-Transfer Layer



Hardware Glitching

- Alter the clock period during execution resulting in incorrect intermediate values.
- Drop the voltage, corrupt read and write operations to memory.
- DDK includes PLLs, frequency dividers and multiple global clock signals.
- Multiple clock frequencies can be generated (i.e. 20ns, 10ns ...).
- FPGA I/O pins are directly accessible.



Hardwareglitschen

RECON

modzero

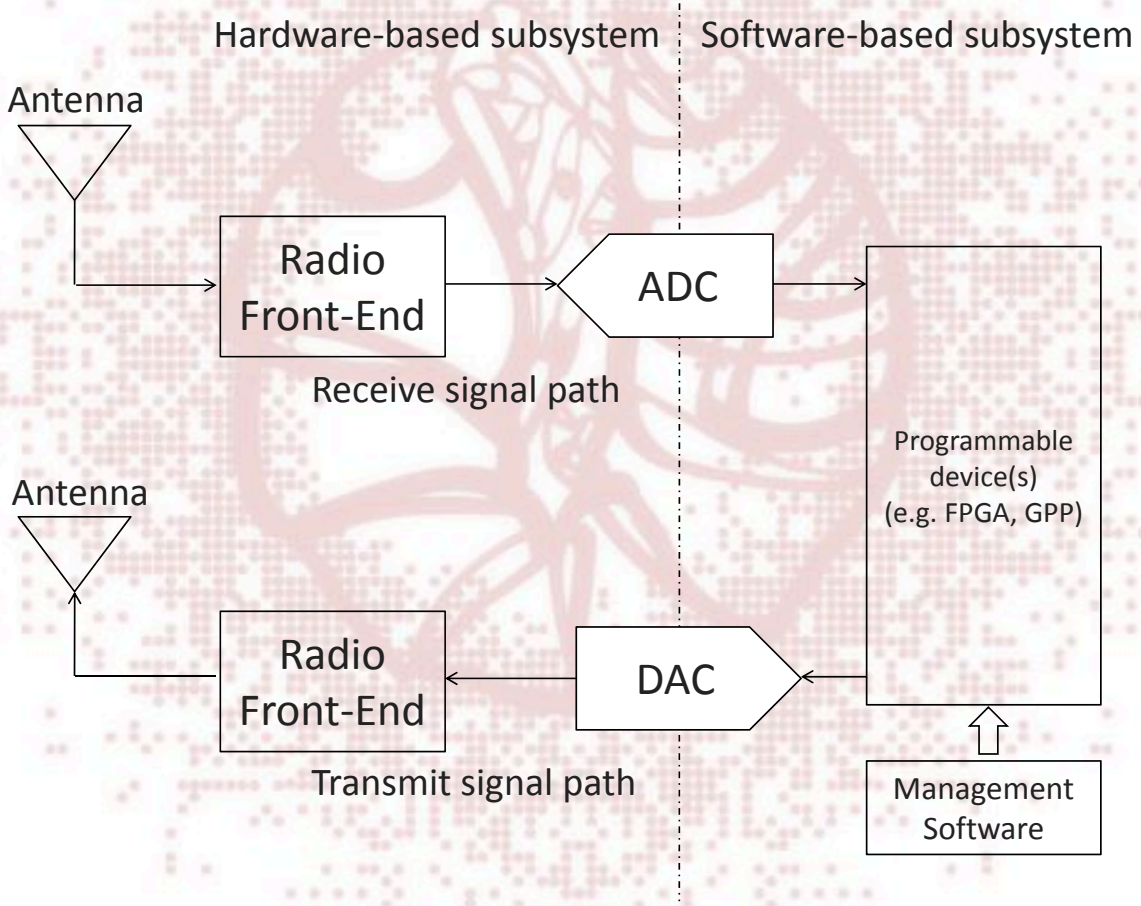
Software Defined Radio

- Utilize digital RF transceivers with a digital serial output of data.
- Multiple transceivers and multiple configurations can be monitored simultaneously.
- Only certain parts of the payload are of interest while others can be discarded.
- Protocol decoding must keep up with the data rate of the target.

Software Defined Radio

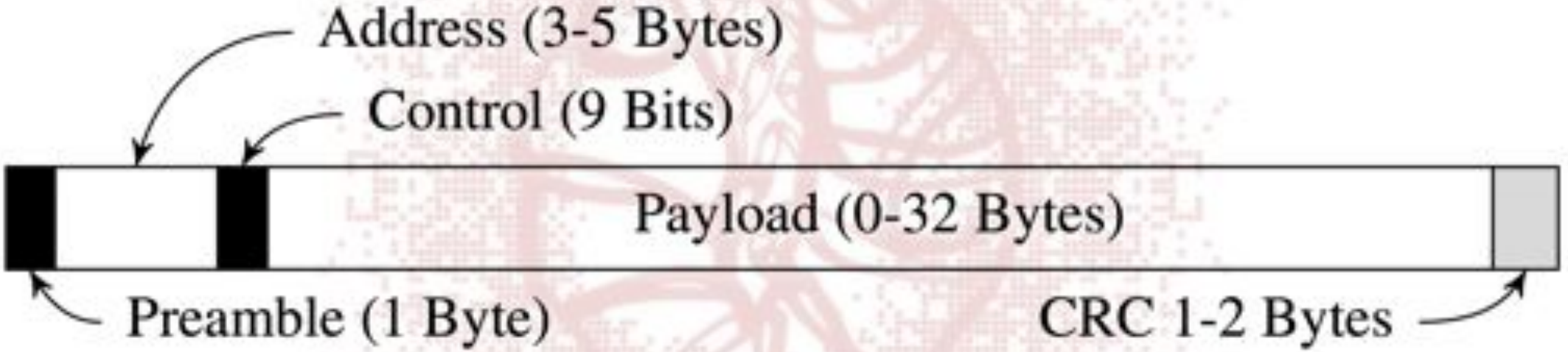
- Example: Keykeriki - Difficulties & challenges
- 2.4GHz Nordic Semiconductor NRF24 family
- Enhanced Shockburst protocol
- 2Mbit/s RF (2MHz = 500ns per bit)

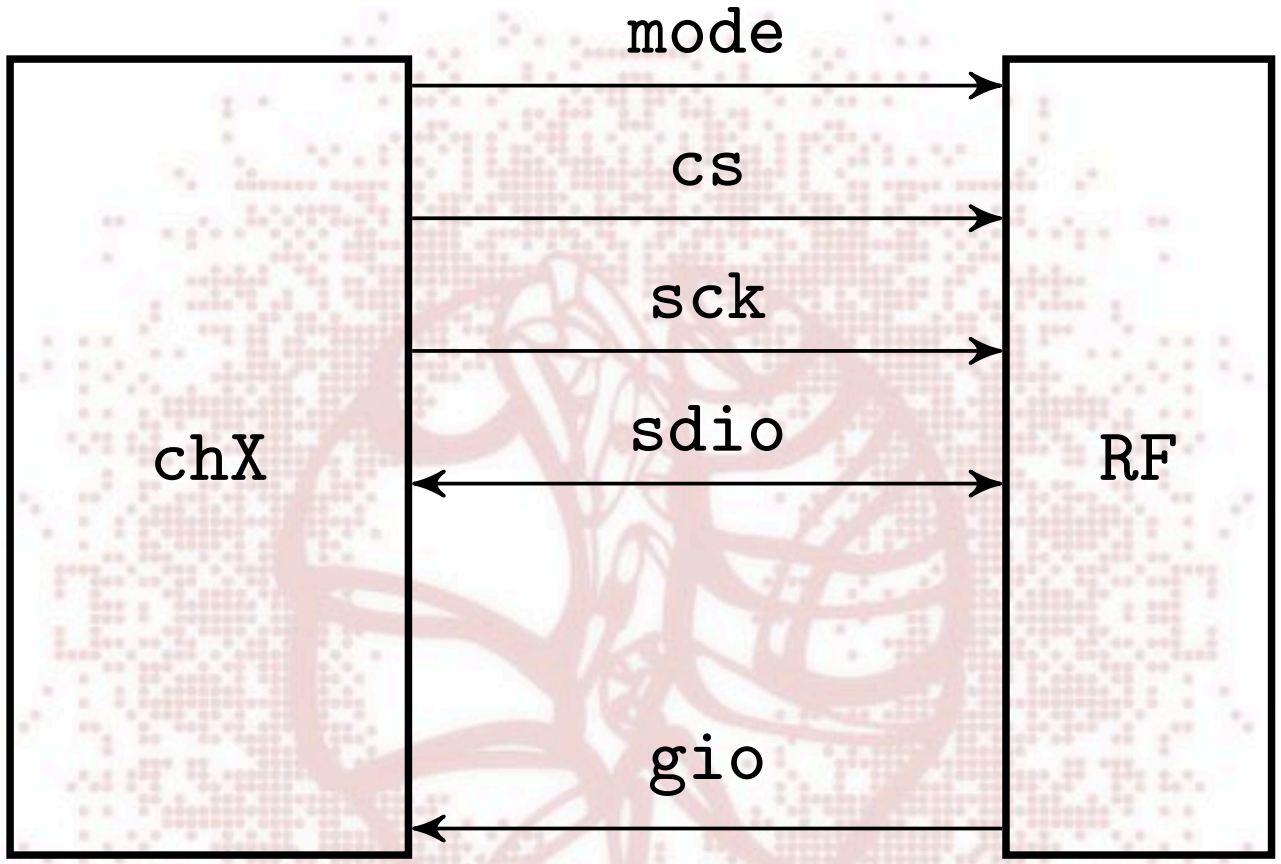
Typical SDR



Source: http://userver.ftw.at/~valerio/files/SDRreport.pdf

Example: Nordic Semi





Software Defined Radio

Die Datenkrake - Release

github.com/ddk

www.gnu.org/licenses/gpl-2.0.txt

Acknowledgements

- Daniel Mack , Joachim Steiger, Jonas Hilt, Felix von Leitner
- Hugo Fortier, Sam, Eric Preston and the REcon 2013 crew!
- Colleagues at SECT & modzero AG
- Microsemi Corporation - http://www.microsemi.com/

RECON

modzero

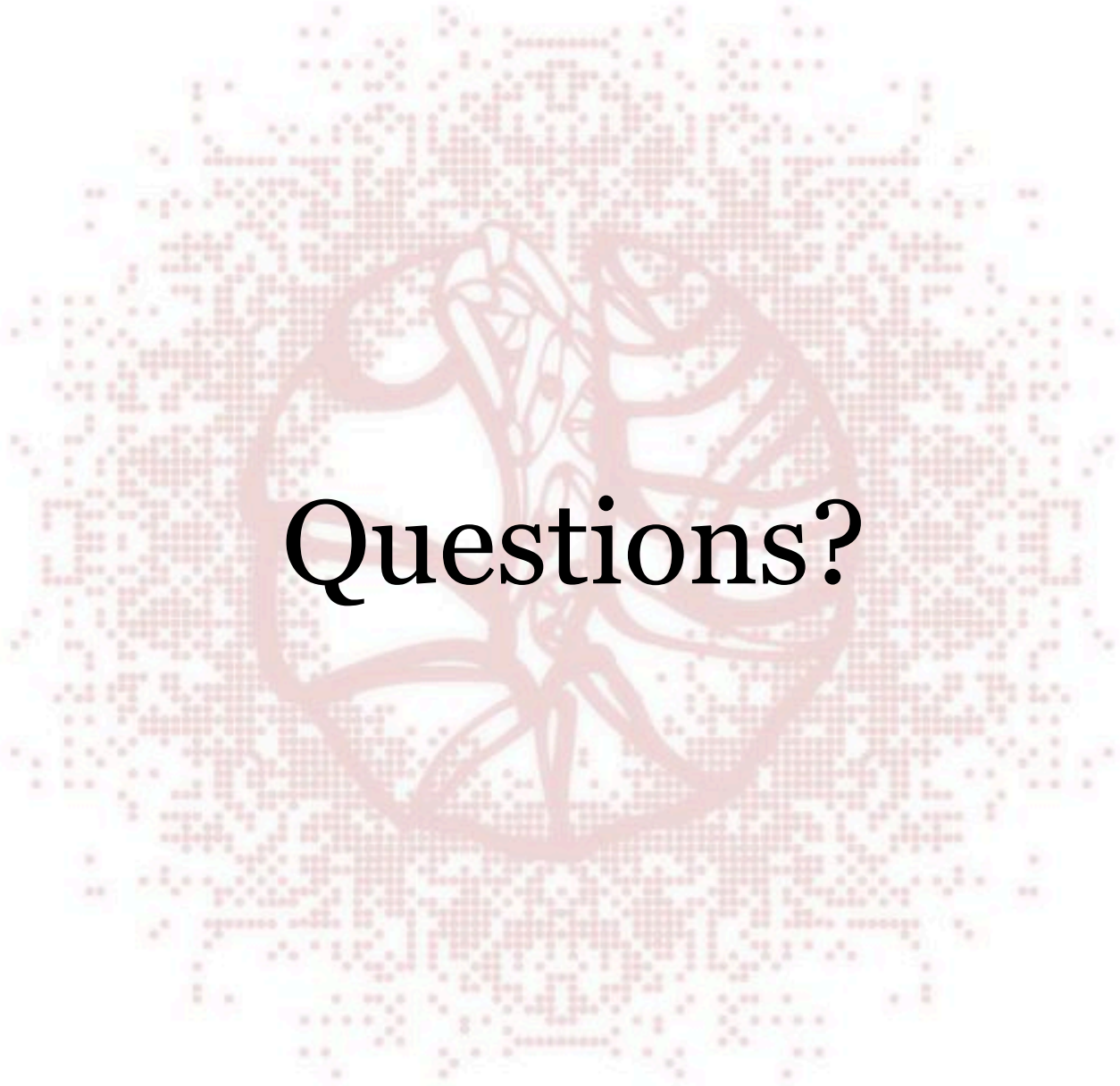
Get Schooled

- We had a Datenkraken Hardware-Hacking Training already:
  - pREcon 2013 (Berlin)
  - REcon 2013 (Montréal)
- There will be trainings:
  - RUXCON/Breakpoint 2013 (Melbourne)
  - On demand…

Logo Contest

RECON

modzero



Questions?

RECON

modzero

Thanks!

http://datenkrake.org

@diedatenkrake

Thorsten Schröder

http://modzero.ch

@br3t

Dmitry Nedospasov

http://nedos.net

@nedos

RECON

modzero