Hardware YOU Can

Trust

Benedikt Stockebrand
Stepladder IT Training+Consulting GmbH

March 18, 2015
Troopers 15
Heidelberg, Germany

Hardware YOU Can Audit and Then Trust

Benedikt Stockebrand
Stepladder IT Training+Consulting GmbH

March 18, 2015
Troopers 15
Heidelberg, Germany

About Me

- Diplom-Informatiker (Uni Dortmund)
- Specialized in IT operations, TCP/IP networks, Unix
- Even more specialized on IPv6 since mid 2003
- Co-author of an IPv6 related security study for the BSI (Federal Office for IT Security)
- Actively working on microcontrollers and hardware random number generators since 2012 (or so)

Part I

The Current Situation

So-called “IT Security”

So-called “IT Security”

- Do we have to prove IT systems to be insecure?

So-called “IT Security”

- Do we have to prove IT systems to be insecure?
- . . . or should the vendor demonstrate their security instead?

So-called “IT Security”

- Do we have to prove IT systems to be insecure?
- . . . or should the vendor demonstrate their security instead?
- For more on this:
  “The Limits of Cryptography”, EasterHegg 2014
  `http://www.youtube.com/watch?v=7bTaKSZQKhc`

“Secure Hardware”

- Do we blindly want to trust all the
  - designers/developers
  - vendors
  - manufacturers
  - component suppliers
  - logistics operators
  - distributors
  - dealers
  - customs authorities
  - investigative authorities
  - so-called “intelligence” agencies
  - standard issuing bodies
  - . . . and whoever else

  involved?

“Tamper Protection”?

- In some cases, this is imporant

“Tamper Protection”?

- In some cases, this is imporant
- But in other cases this is

“Tamper Protection”?

- In some cases, this is imporant
- But in other cases this is
  - unnecessary

“Tamper Protection”?

- In some cases, this is imporant
- But in other cases this is
  - unnecessary
  - exceedingly difficult

“Tamper Protection”?

- In some cases, this is imporant
- But in other cases this is
  - unnecessary
  - exceedingly difficult
  - or a convenient excuse to peddle snake oil.

Auditability I

- Can I audit a TPM module or the crypto features of a CPU...
- ... without destroying it?
- ... with affordable and available tools?
- ... with available know-how?
- ... and with a reasonable amount of effort?

Auditability II

- Is auditability possible?

Auditability II

- Is auditability possible?
- Not with attackers, who
  - have unlimited resources
  - have unlimited technical skills
  - have unlimited insider knowledge
  - have unlimited political and judicial backing
  - nonchalantly ignore applicable laws
    (not to talk about “decency”)
  - have support from the manufacturers
  - don’t make mistakes

Auditability II

- Is auditability possible?
- Not with attackers, who
  - have unlimited resources
  - have unlimited technical skills
  - have unlimited insider knowledge
  - have unlimited political and judicial backing
  - nonchalantly ignore applicable laws (not to talk about "decency")
  - have support from the manufacturers
  - don't make mistakes
- But what about real world attackers?

Risk Assessment of Attacks

- Risk of discovery
- Personal risk for attacker

Risk Assessment of Attacks

- Risk of discovery
- Personal risk for attacker

- Economic risk for attacker

Scope of Attacks

- Targeted attacks
- Untargeted, large scale attacks

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices
- Replacement of operational devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families
- Manipulation of standards and specifications

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families
- Manipulation of standards and specifications
- Attacks at the political level

Part II

Fighting Back

Defense Strategies I

- Technical

Defense Strategies I

- Technical
- Economic

Defense Strategies I

- Technical
- Economic
- Political

Defense Strategies II

- Diversity
- Auditability
- Modularity

Development Criteria

- Designs must be
  - easy to understand
  - easy to modify
  - easy to reproduce (and build yourself)
- Development tools must be
  - auditable
  - generally available
  - affordable
  - available in multiple implementations

Usable Hardware Components

Components should be

- cheap
- mass produced for multiple purposes
- available from multiple manufacturers
- simple (i.e. no highly integrated ICs if possible)
- widely available
- easily replaceable by similar components
- easy to use for custom builds

PCB Technology

- Through-hole (THT) only
- Surface mount (SMT) for home assembly
- Surface mount for industrial assembly

Part III

A Random Self-Experiment

Choosing the External Interface

- Raw analog output
- UART (5V)
- RS-232
- USB
- PCIe

Choosing the Microcontroller and Interface

- Atmel ATtiny2313 and FTDI FT232RL
- Various MSP430 and FTDI FT232RL
- PIC 16F 1454/1455/1459
- PIC 18F 13K50/14K50
- Various Atmel ATxmega with on-chip USB
- Various STM32

FTDIgate

- FT232's can be configured via USB interface
- In September 2014, FTDI released a driver update...

FTDIgate

- FT232's can be configured via USB interface
- In September 2014, FTDI released a driver update...
- ... which bricked fake FTDI chips
- (and no warning given)

FTDIgate

- FT232's can be configured via USB interface
- In September 2014, FTDI released a driver update...
- ... which bricked fake FTDI chips
- (and no warning given)

- That chip must go

Choosing the Noise Source

- Radioactive decay
- Radio static
- Noise from blackened CCD chip
- Thermal noise in a resistor
- Ring oscillator
- Microphone at Kindergarten playground
- ...

Choosing the Noise Source

- Radioactive decay
- Radio static
- Noise from blackened CCD chip
- Thermal noise in a resistor
- Ring oscillator
- Microphone at Kindergarten playground
- ...

- Avalanche effect in “Zener” diodes

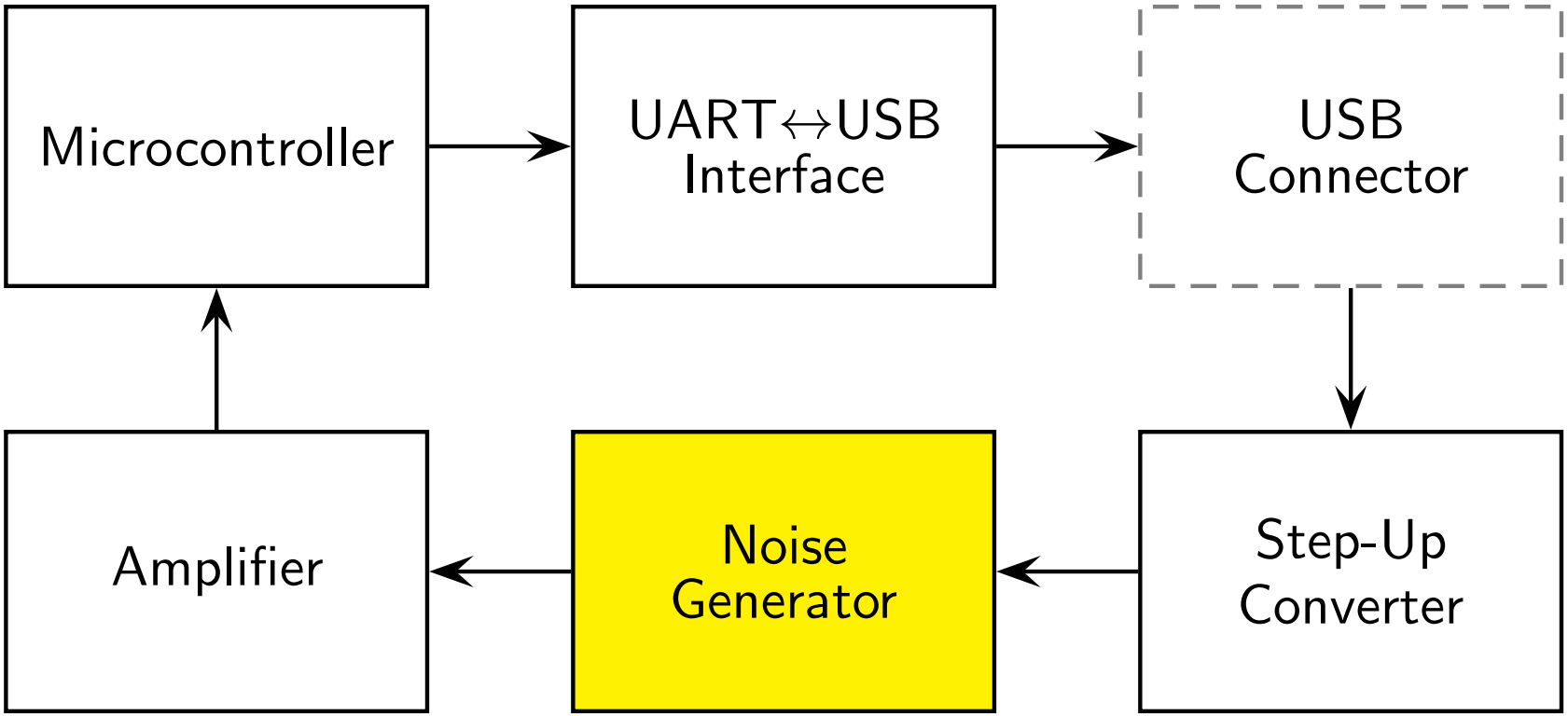
Generating 12V

- Fredrik Thulin's choice: Charge pump
  - Depends on input voltage
  - Doesn't need inductances

Generating 12V

- Fredrik Thulin's choice: Charge pump
  - Depends on input voltage
  - Doesn't need inductances
- My choice: Step-up converter (MC34063)
  - Needs inductances
  - Ultra cheap
  - Huge variety of vendors
  - Widely known
  - General purpose chip

Block Schematic



Noise Specifications

- Noise is undesirable...

Noise Specifications

- Noise is undesirable...
- ... and generally specified as upper limit only

Noise Specifications

- Noise is undesirable...
- ... and generally specified as upper limit only

- This is a fundamental problem.

“Magic Zener Diodes”

“Magic Zener Diodes”

Source: `http://www.conrad.de/ce/de/product/179001`

Getting Reliable Noise

- More magic?
- BE junction in bipolar junction transistors (BJTs)

Getting Reliable Noise

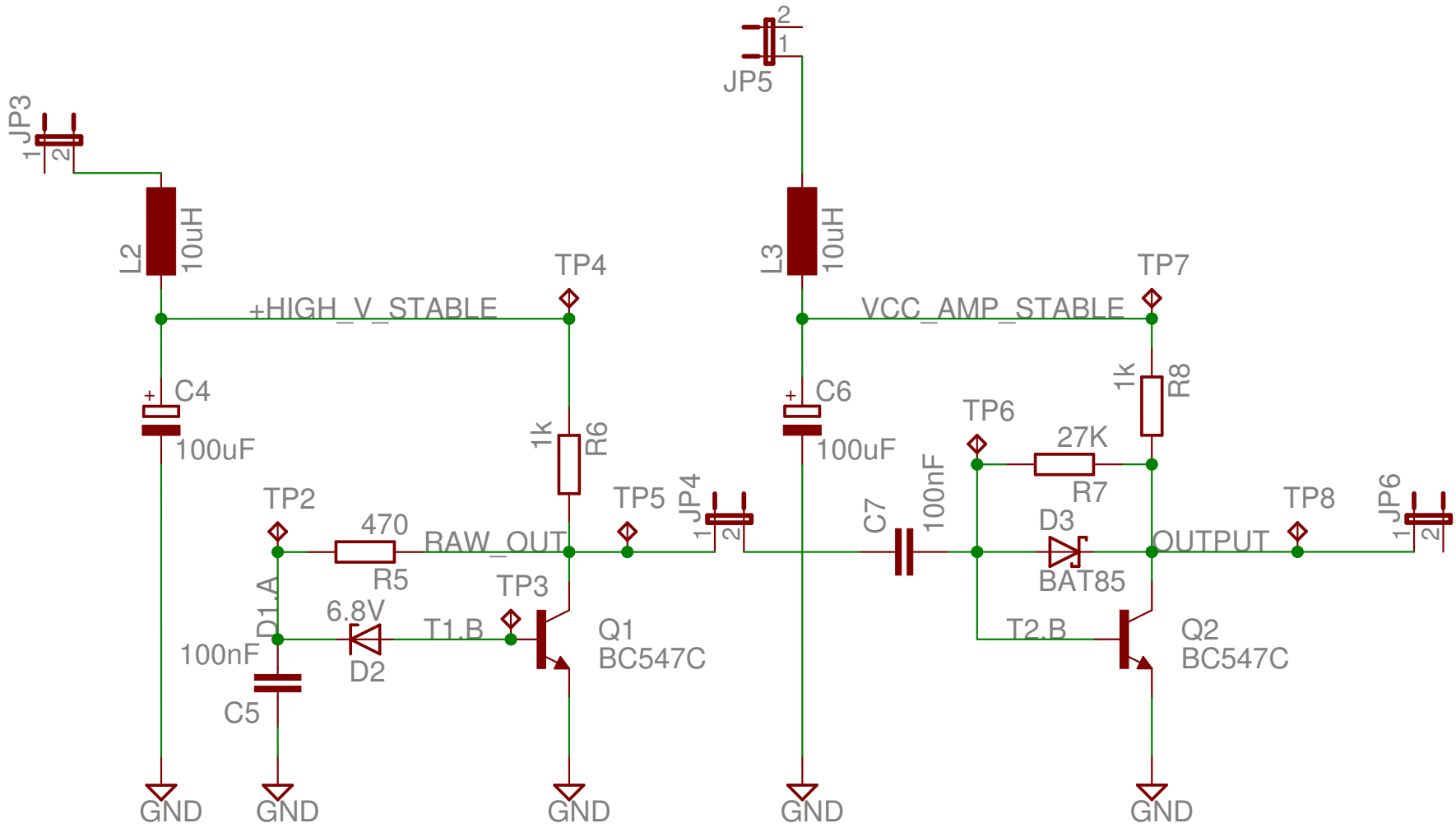
- More magic?
- BE junction in bipolar junction transistors (BJTs)

- This is still a fundamental problem.

Building for Auditability

- Minimized circuit design
- Test pins
- Auditable PCB layout
- DIY compatibility

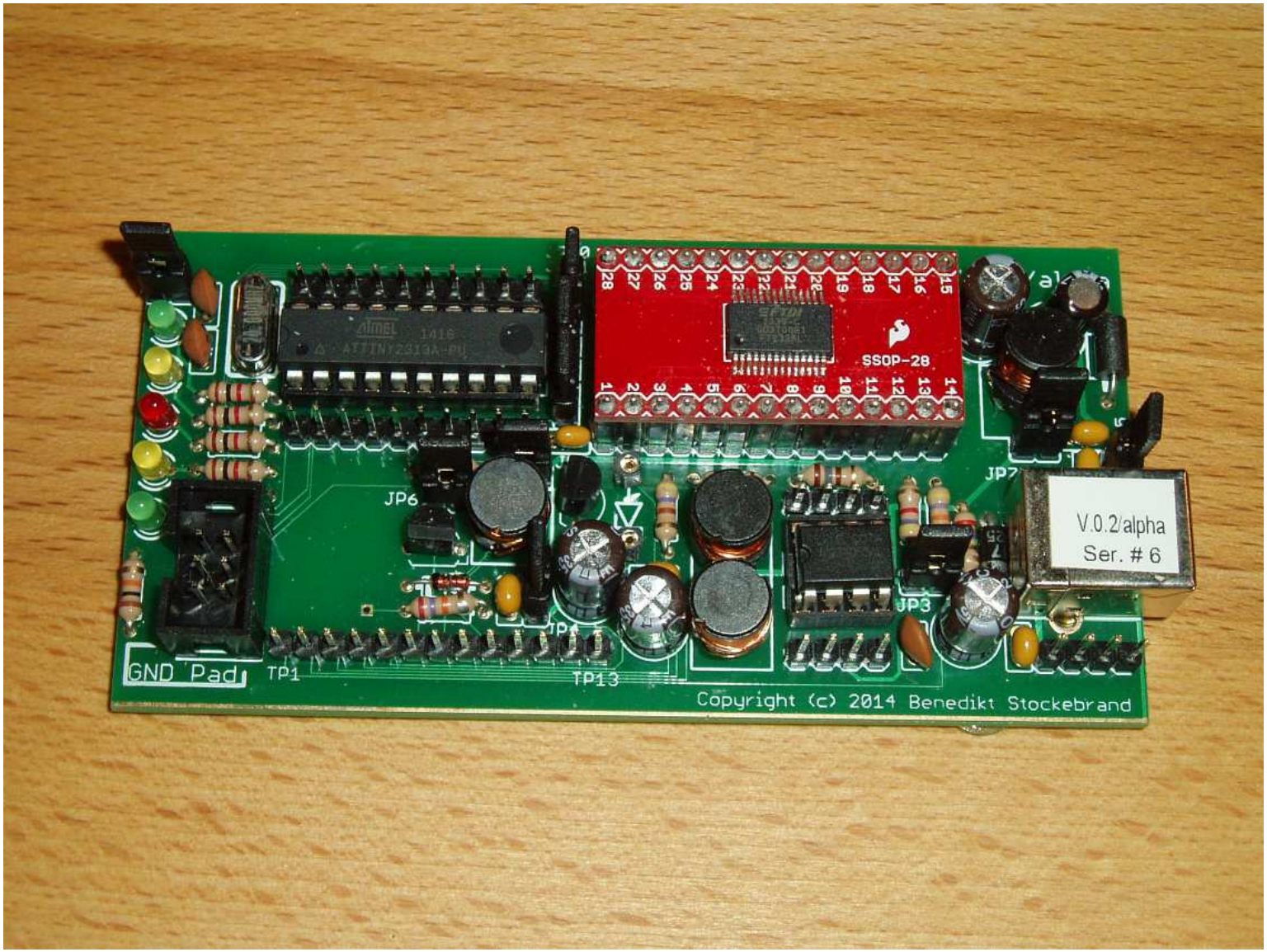
Minimizing the Circuit Design



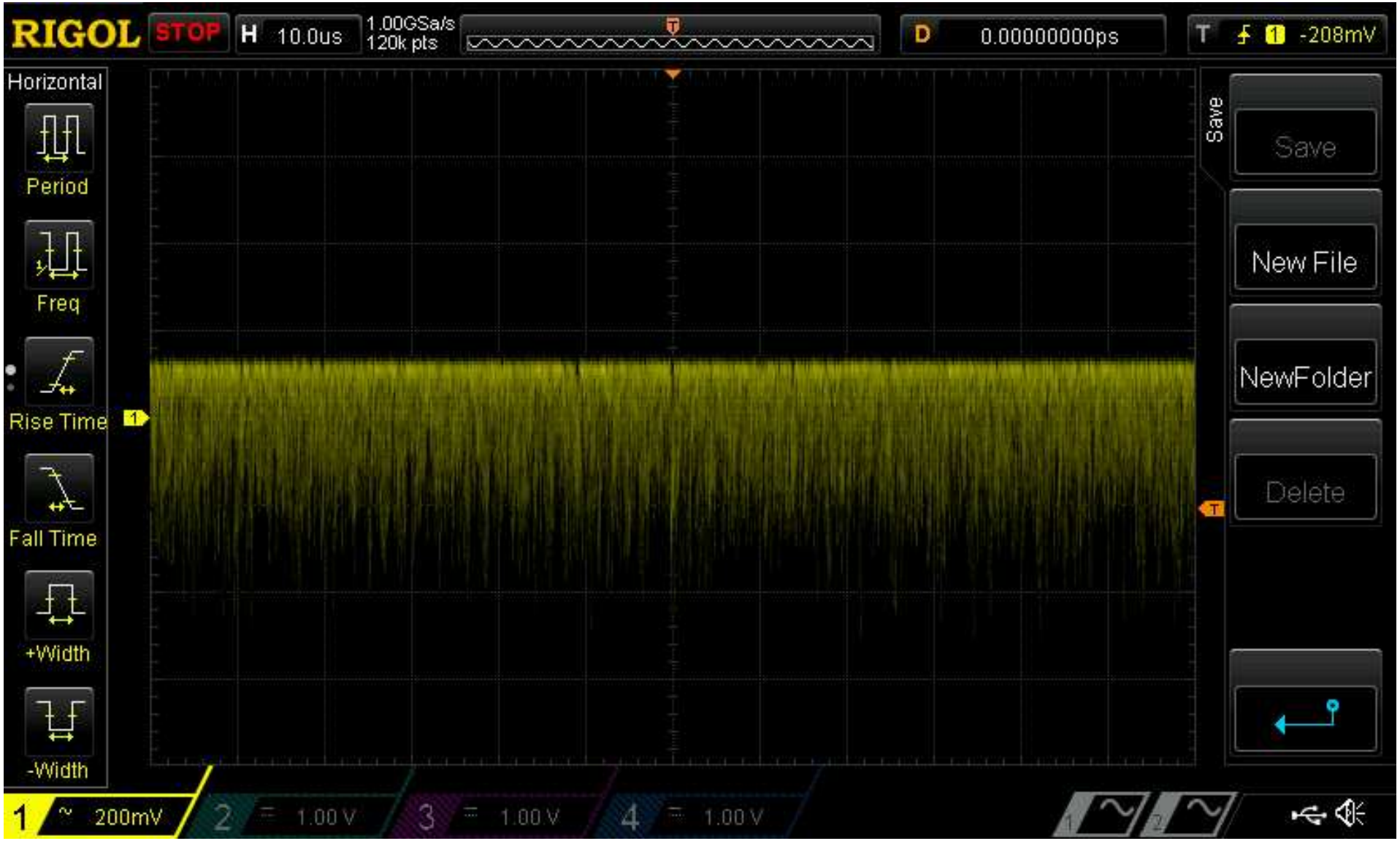
Generator Core

Amplifier Stage

My Very First Real PCB



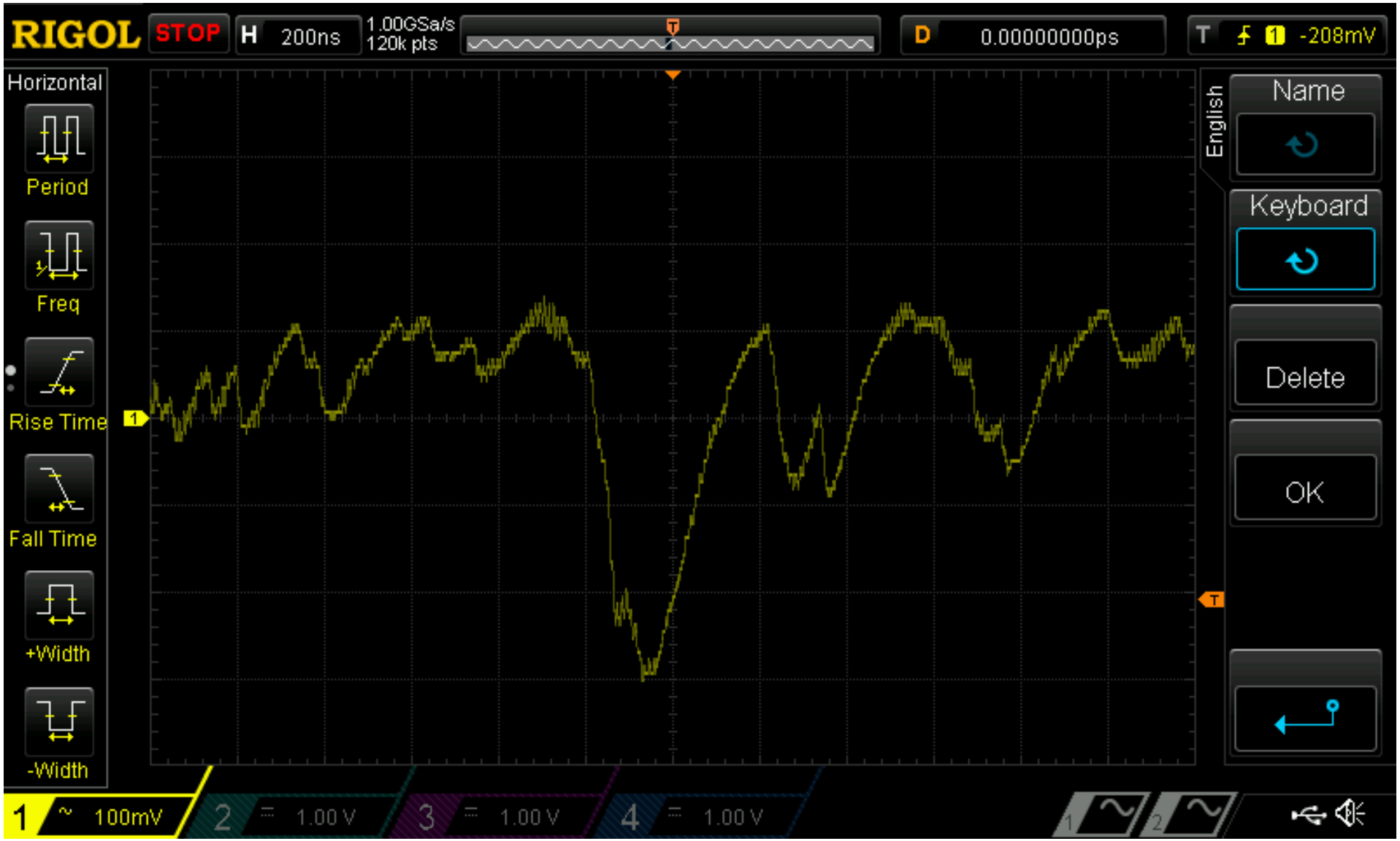
Analog Output I



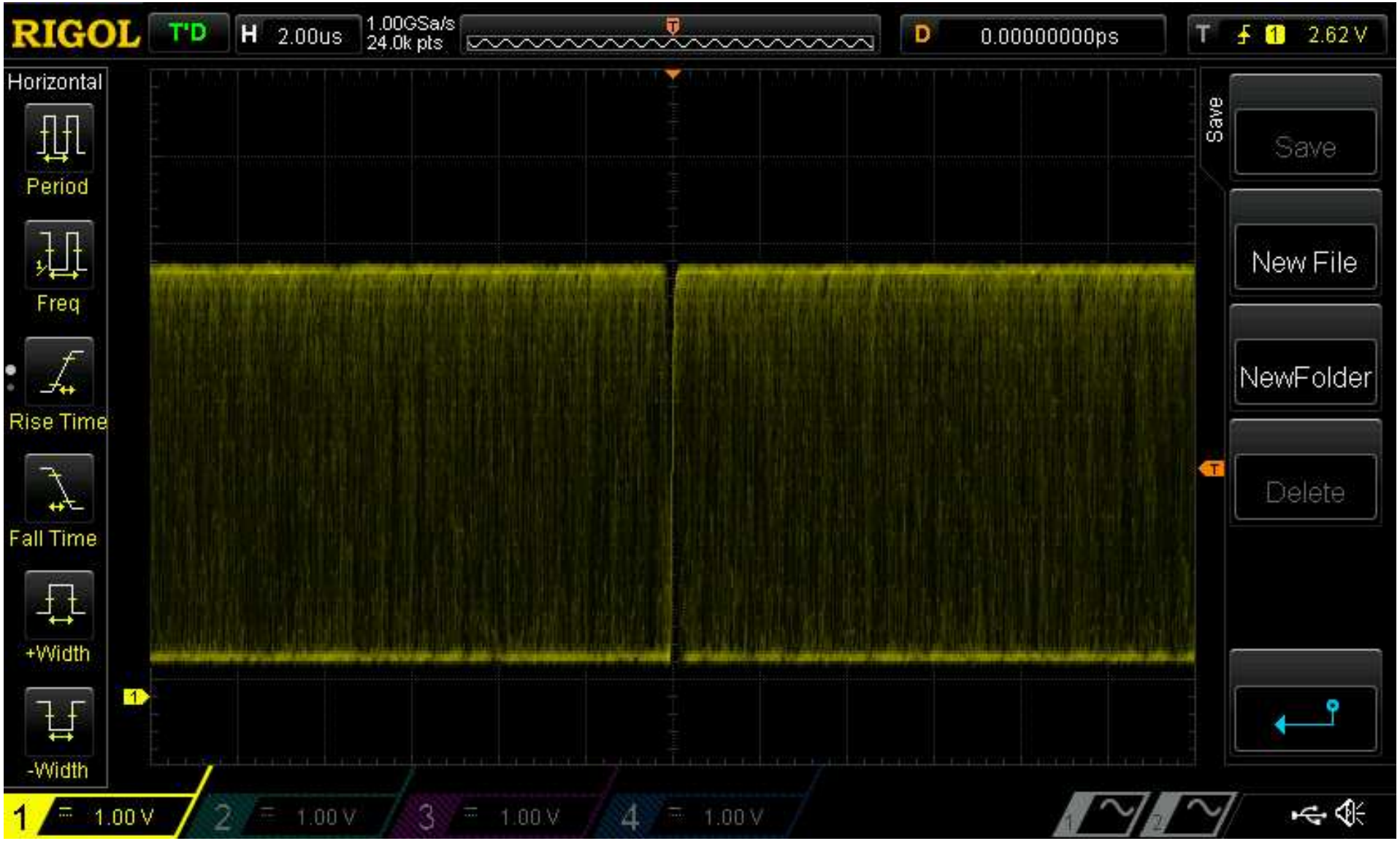
Analog Output II

Analog Output III

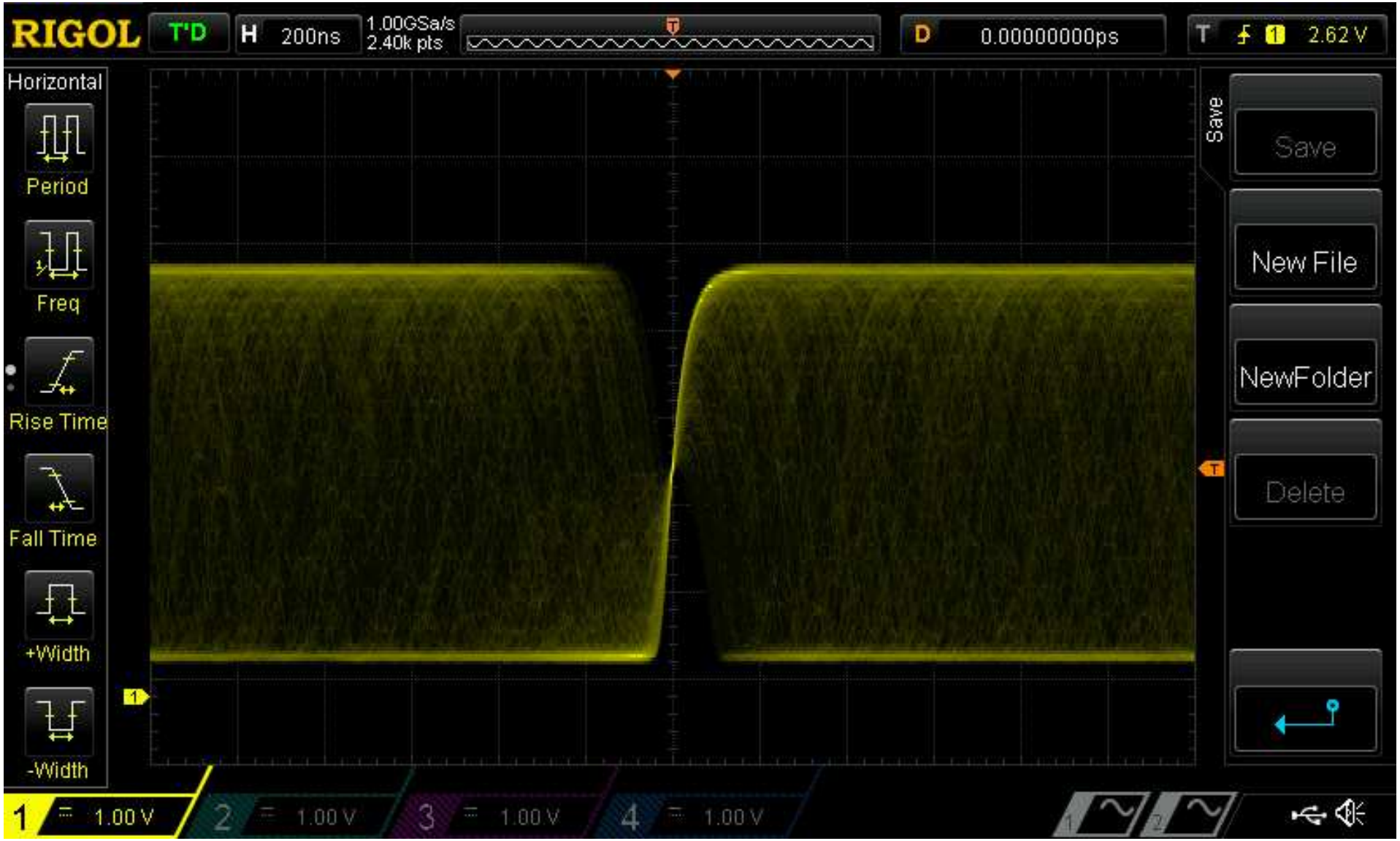
Analog Output IV



Amplified Output I



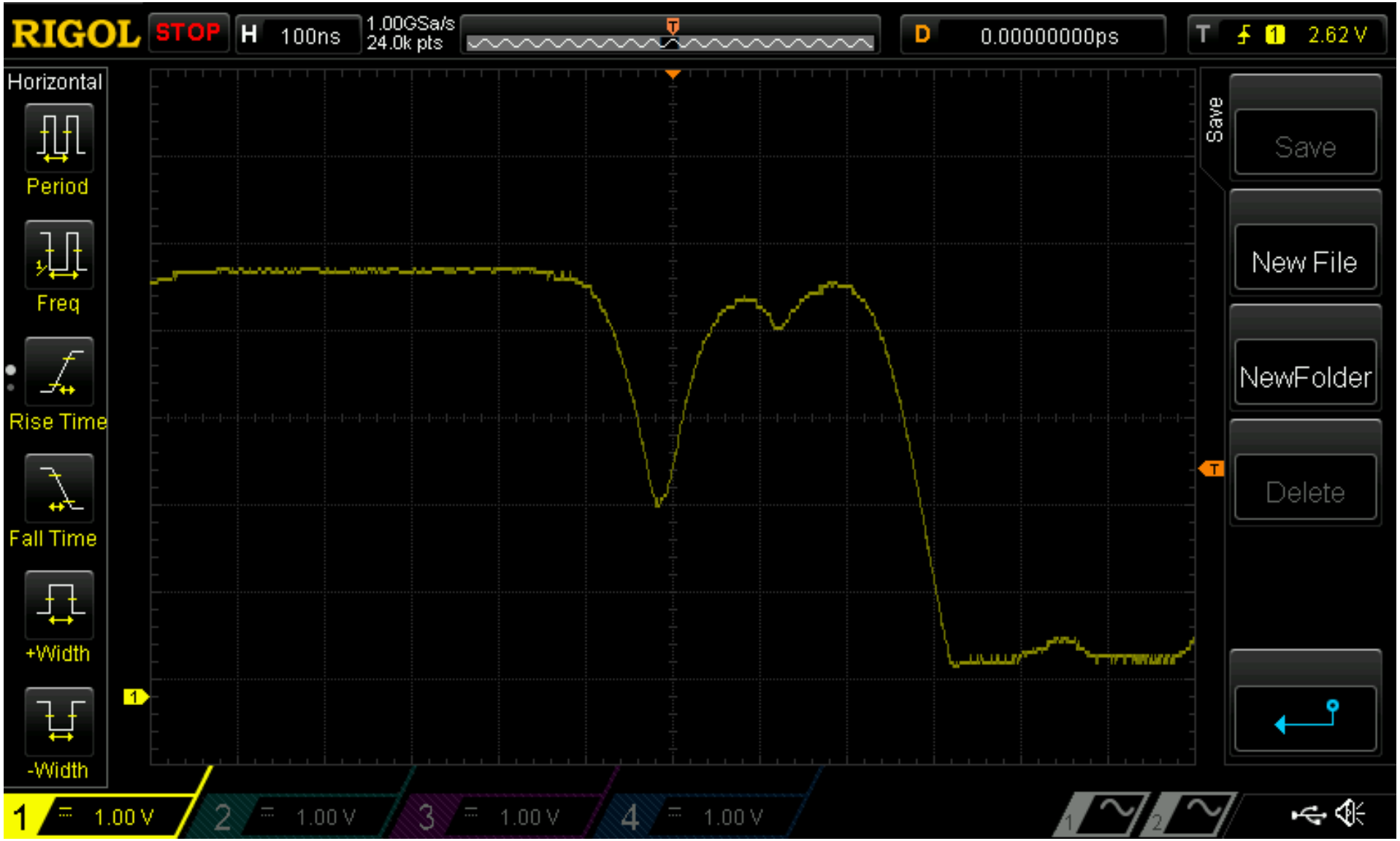
Amplified Output II



Amplified Output III

Amplified Output IV

Amplified Output V



Digitizing Noise

- Trivial approach: XOR n readings
  - Fast
  - Constant speed
  - Not adapting to quality of analog source
  - Not failsafe

Digitizing Noise

- Trivial approach: XOR n readings
  - Fast
  - Constant speed
  - Not adapting to quality of analog source
  - Not failsafe
- Measure (LSB of) time between rising edges
  - Slightly slower
  - Variable speed
  - Adapts to quality of analog source
  - Failsafe behaviour
  - Automatically removing correlation

- Correlation
  - Removed via rising edge algorithm
  - Analog circuit is too simple to store much information,
    $\Rightarrow$ No correlation between bits possible

From Noise to Entropy

- Correlation
  - Removed via rising edge algorithm
  - Analog circuit is too simple to store much information,
    $\Rightarrow$ No correlation between bits possible
- (Bitwise) bias
  - Follow up with a von Neumann extractor:
  - Read two bits
  - If the same, discard both
  - Else return the first
  - Rinse and repeat as needed

Why the “ARRGH” board?

- It’s the **A**uditable **R**eal **R**andom Number **G**enerator **H**ardware
- It has *nothing* to do with a Makefile bug that made me generate four weeks worth of test data using the XOR extraction on a less-than-magic Zener diode. . .

Part IV

Preliminary Finale

Conclusions

- ICs suck (especially from FTDI)
- THT components suck
- SMD/SMT-only components suck
- USB sucks even worse

Conclusions

- ICs suck (especially from FTDI)
- THT components suck
- SMD/SMT-only components suck
- USB sucks even worse

- Auditable hardware is difficult
- . . . but apparently possible

Conclusions

- ICs suck (especially from FTDI)
- THT components suck
- SMD/SMT-only components suck
- USB sucks even worse

- Auditable hardware is difficult
- . . . but apparently possible

- Complexity is a problem, not a solution

Conclusions

- ICs suck (especially from FTDI)
- THT components suck
- SMD/SMT-only components suck
- USB sucks even worse

- Auditable hardware is difficult
- . . . but apparently possible

- Complexity is a problem, not a solution

- Randomness *looks* really simple
- . . . until you really take a look

Outlook: Testing

- There are no proper test methods
- . . . let alone ready-to-use tools

Outlook: Testing

- There are no proper test methods
- . . . let alone ready-to-use tools

- Testing for pseudo randomness is much better known
- . . . but largely unrelated

Outlook: Testing

- There are no proper test methods
- . . . let alone ready-to-use tools

- Testing for pseudo randomness is much better known
- . . . but largely unrelated

- Testing for randomness is “the wrong way ’round”
- Best starting point is still Knuth’s ACP Vol. 2

Outlook: Testing

- There are no proper test methods
- . . . let alone ready-to-use tools

- Testing for pseudo randomness is much better known
- . . . but largely unrelated

- Testing for randomness is “the wrong way ’round”
- Best starting point is still Knuth’s ACP Vol. 2

- The NIST screwed this up again. Big time.

Outlook: Testing

- There are no proper test methods
- . . . let alone ready-to-use tools

- Testing for pseudo randomness is much better known
- . . . but largely unrelated

- Testing for randomness is “the wrong way ’round”
- Best starting point is still Knuth’s ACP Vol. 2

- The NIST screwed this up again. Big time.

- But this is enough for another year of research. . .
- . . . and hopefully another talk

Part V

Appendix

Resources

The Limits of Cryptography
EasterHegg 2014, Stuttgart
`http://www.youtube.com/watch?v=7bTaKSZQKhc`

BIVBlog: Benedikt's IT Video Blog
`http://www.stepladder-it.com/bivblog/`
Video Blog on IT in general and crypto hardware (and IPv6) in particular

The Cryptech project
`https://cryptech.is/`

Contact Information

Stepladder IT
Training+Consulting GmbH
Benedikt Stockebrand

Fichardstr. 38
D-60322 Frankfurt/Main

contact@stepladder-it.com

Webseiten:
http://www.stepladder-it.com/
http://www.benedikt-stockebrand.de/

Video Blog:
http://www.stepladder-it.com/bivblog/