ZapZap!! BangBang!!

Defeating Secure Boot with EMFI

Ang Cui, PhD & Rick Housley
{a|r}@redballoonsecurity.com

Beat Secure Boot w/ EMP!

+

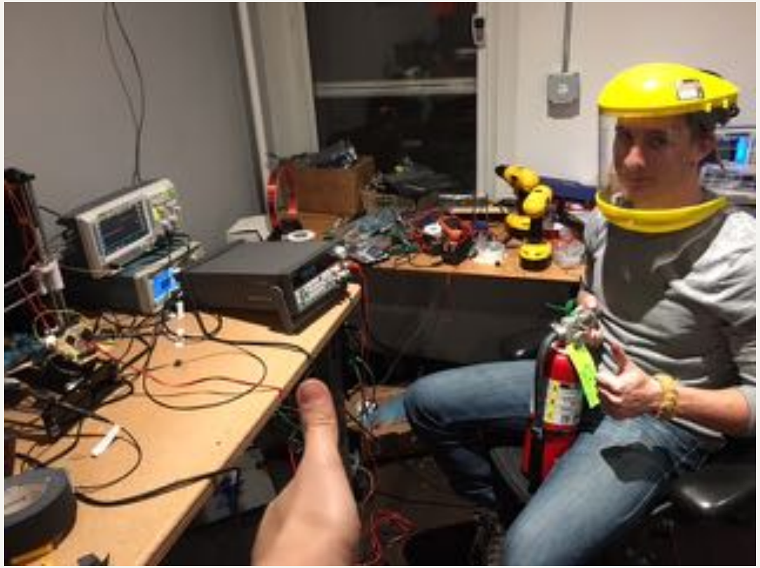
PROJECT

BADFET

1. Open-source project to democratize EMFI research
2. 2 years of work so far

PROJECT

BADFET



Disclaimer:

- BadFET-style EMFI research is hilariously dangerous. (but srsly. It's dangerous)
- Licking any part of BadFET will almost certainly kill you.

Last year…

DISCLAIMER

- BADFET is very experimental
- BADFET uses voltage and current in INSTANT DEATH territory.
- PLEASE be careful, and experiment at your OWN RISK

Ang!

Rick!

chris!

Primary Main Objective!

Cisco 8861

We are jerks to Cisco Phones

Cisco 8861/8851

- Dual Core ARMv7
- Broadcom BCM11125
- Processor @ 1001MHz
- Secure Boot

Cisco 8861/8851

- Dual Core ARMv7
- Broadcom BCM11125
- Processor @ 1001MHz
- Secure Boot

2 orders of magnitude faster than any device In previous EMFI attack

Stage 0 x-loader

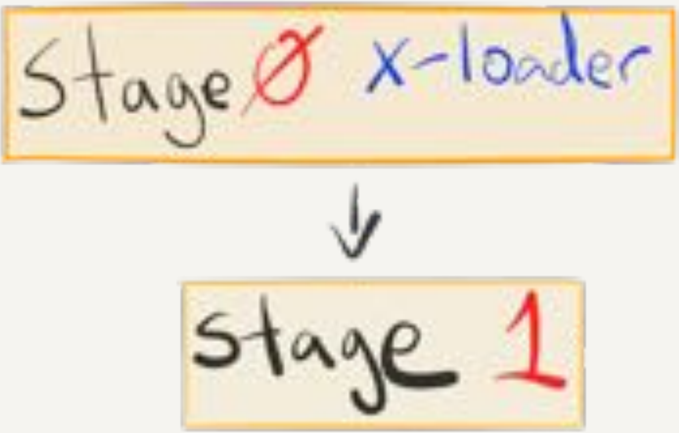
Boot ROM

Small TrustZone API

Init MMU, Clocks

Load Stage 1
From FLASH -> DRAM

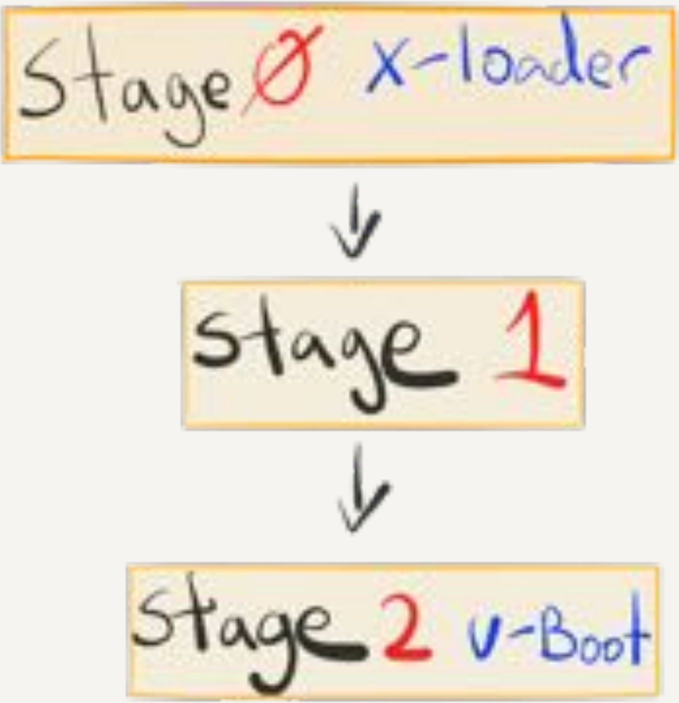
Verify & Execute Stage 1



Inits GPIO, pinmux, i2c, PMU, etc

Load stage 2
From NAND -> DRAM

Verify & Execute
Stage 2 (uBoot)



Load VC4 & Kernel
FLASH -> DRAM

Verify VC4
Execute VC4

Verify Linux Kernel
Execute Linux Kernel

Broadcom TZ SMC

Secure World
Not so Secure World

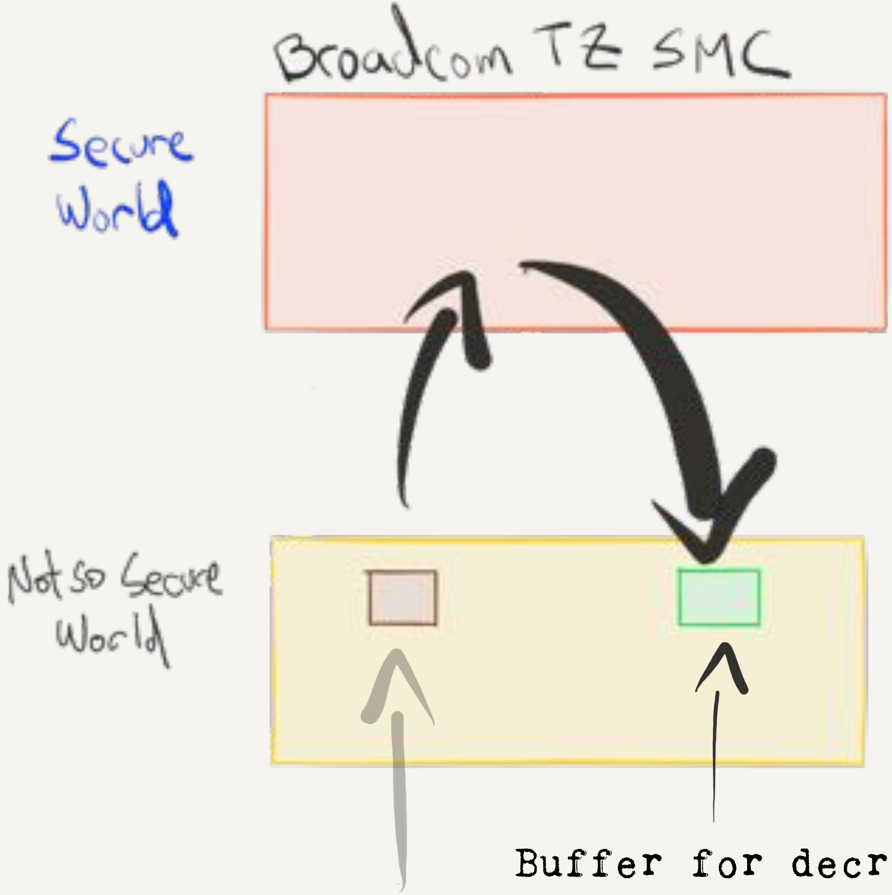
SMC Service ID

0xE00013

RSA_DECRYPT

Does exactly what you think it does

SMC = Secure Monitor Call



SMC Service ID
0xE00013

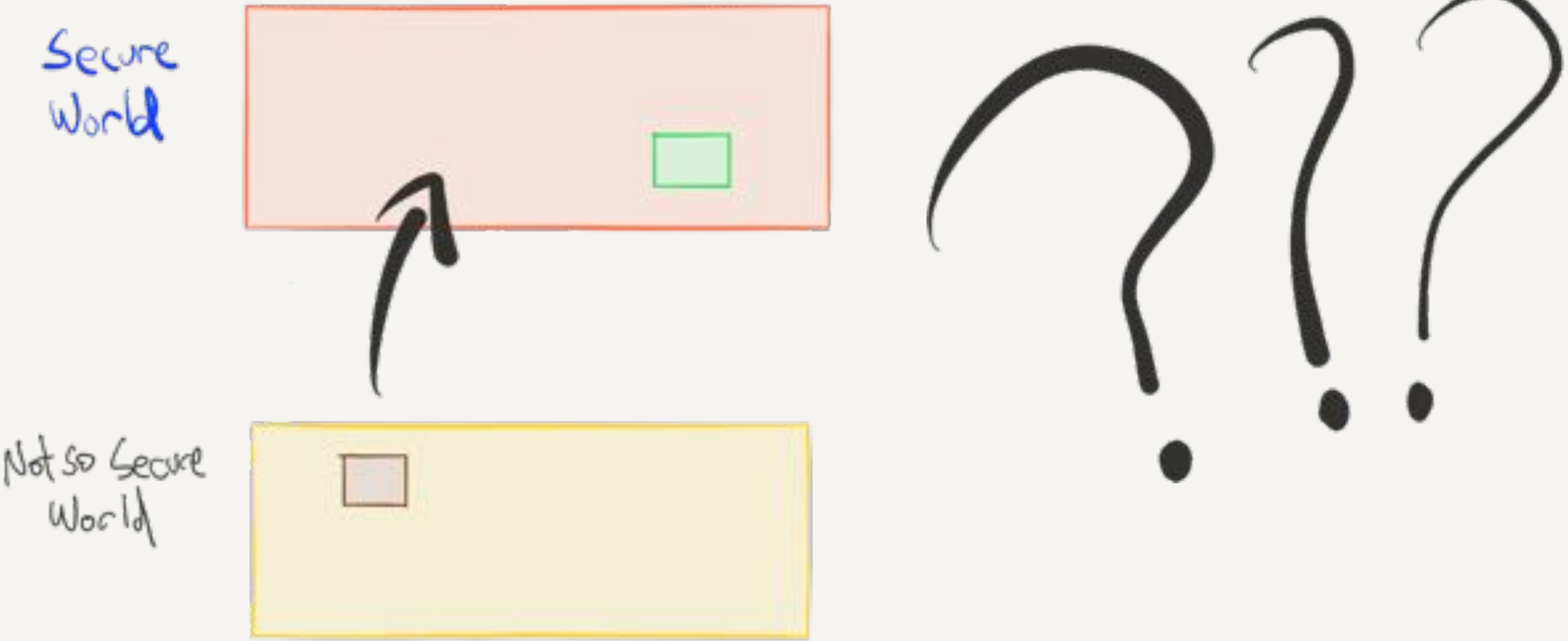
RSA_DECRYPT

Buffer for decrypted data

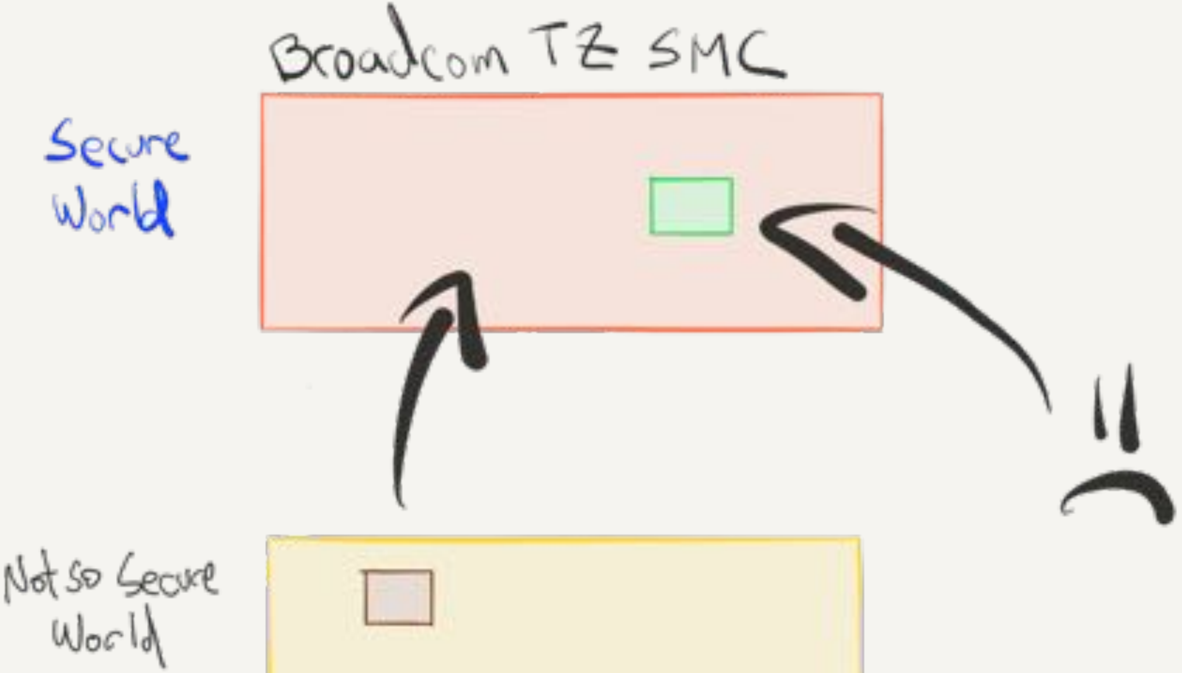
Encrypted Data

SMC = Secure Monitor Call

Broadcom TZ SMC



SMC = Secure Monitor Call



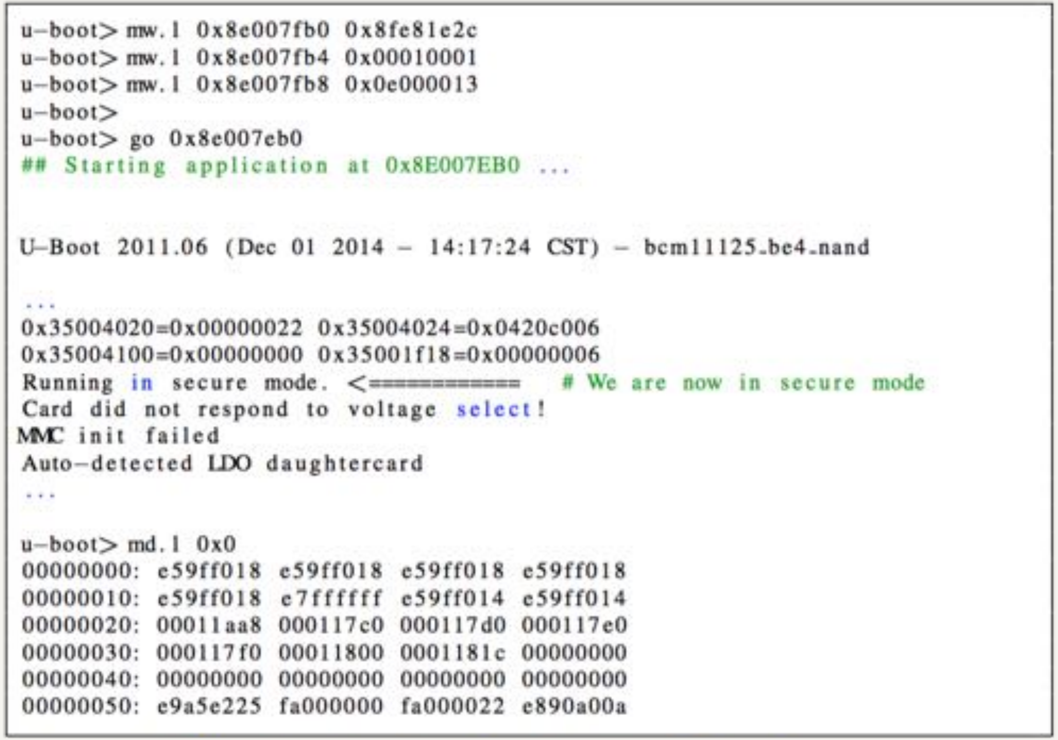
Whelp

SMC = Secure Monitor Call

Phone does not take user input during boot

Phone does not take user input during boot

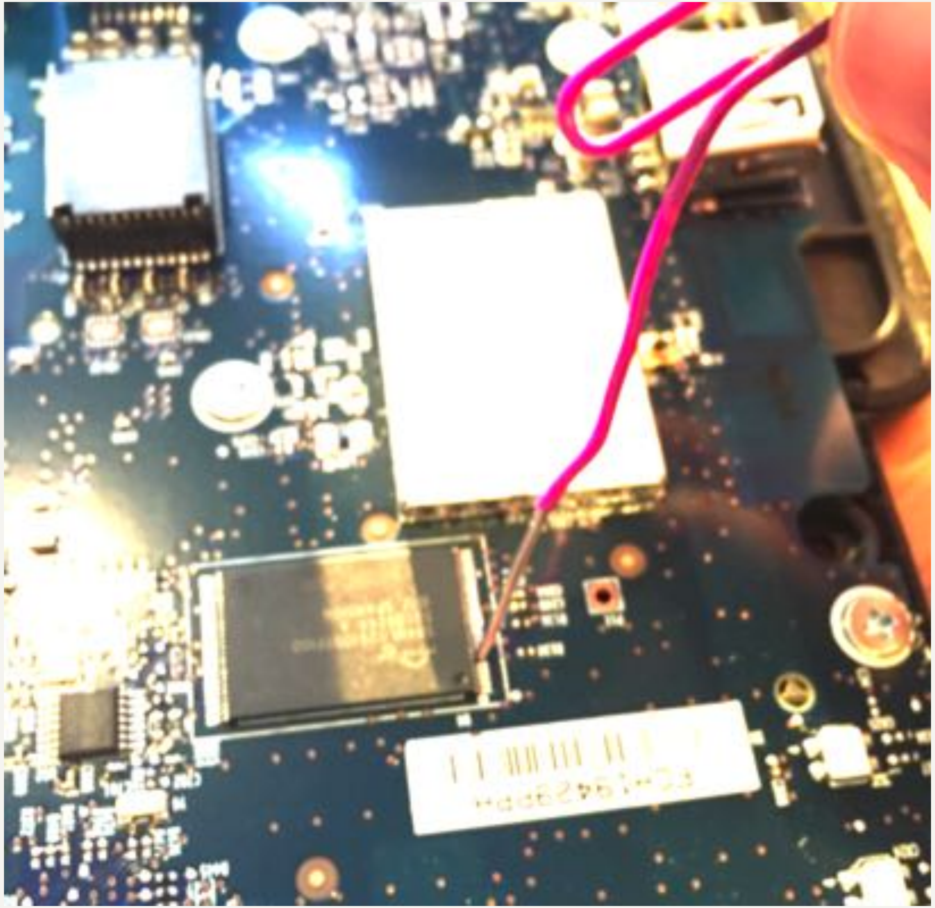
Get to uBoot console, defeat TrustZone



```
u-boot> mw.l 0x8e007fb0 0x8fe81e2c
u-boot> mw.l 0x8e007fb4 0x00010001
u-boot> mw.l 0x8e007fb8 0x0e000013
u-boot>
u-boot> go 0x8e007eb0
## Starting application at 0x8E007EB0 ...


U-Boot 2011.06 (Dec 01 2014 - 14:17:24 CST) - bcm11125_bc4_nand

...
0x35004020=0x00000022 0x35004024=0x0420c006
0x35004100=0x00000000 0x35001f18=0x00000006
Running in secure mode. <============   # We are now in secure mode
Card did not respond to voltage select!
MMC init failed
Auto-detected LDO daughtercard
...

u-boot> md.l 0x0
00000000: e59ff018 e59ff018 e59ff018 e59ff018
00000010: e59ff018 e7ffffff e59ff014 e59ff014
00000020: 00011aa8 000117c0 000117d0 000117e0
00000030: 000117f0 00011800 0001181c 00000000
00000040: 00000000 00000000 00000000 00000000
00000050: e9a5e225 fa000000 fa000022 e890a00a
```

So...

So...



Invasive.

Not Scalable.

Shameful.

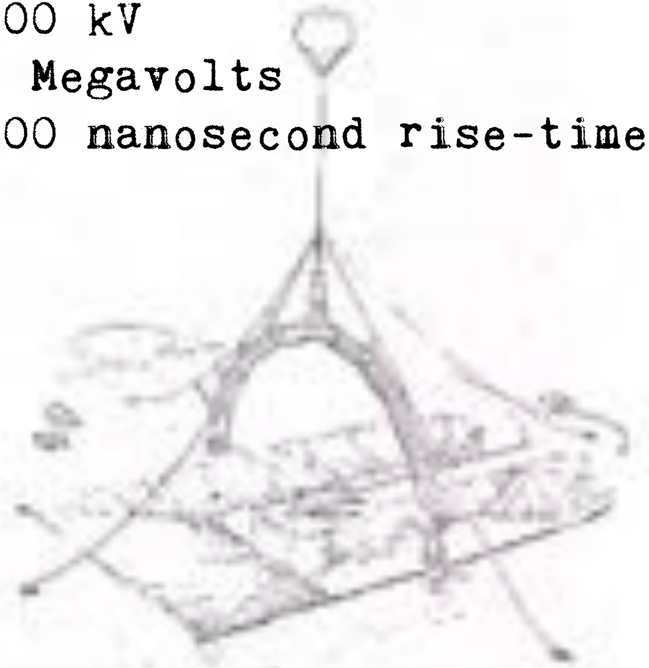
Wire, but without the wire?

EMP

100 kV

5 Megavolts

100 nanosecond rise-time



TRESTLE

EMP FACILITY

ATLAS-I AKA TRESTLE

SANDIA {1972 - 1991}

Electro-Magnetic Fault Injection

EMFI!

Faraday's Law

$$\mathcal{E} = \frac{d\Phi_B}{dt}$$

$\mathcal{E}$ = EMF

Φ_B = magnetic flux

t = time

Ampere's Law

$$B = \frac{\mu_0 I}{2\pi r}$$

B = Magnetic field strength

μ_0 = permeability of free space

I = current

r = wire radius

Magnetic Field Generation

Faraday's Law

$$B = \frac{\mu_0 I}{2\pi r}$$

B = Magnetic field strength

μ_0 = permeability of free space

I = current

r = wire radius

Magnetic Field Induction

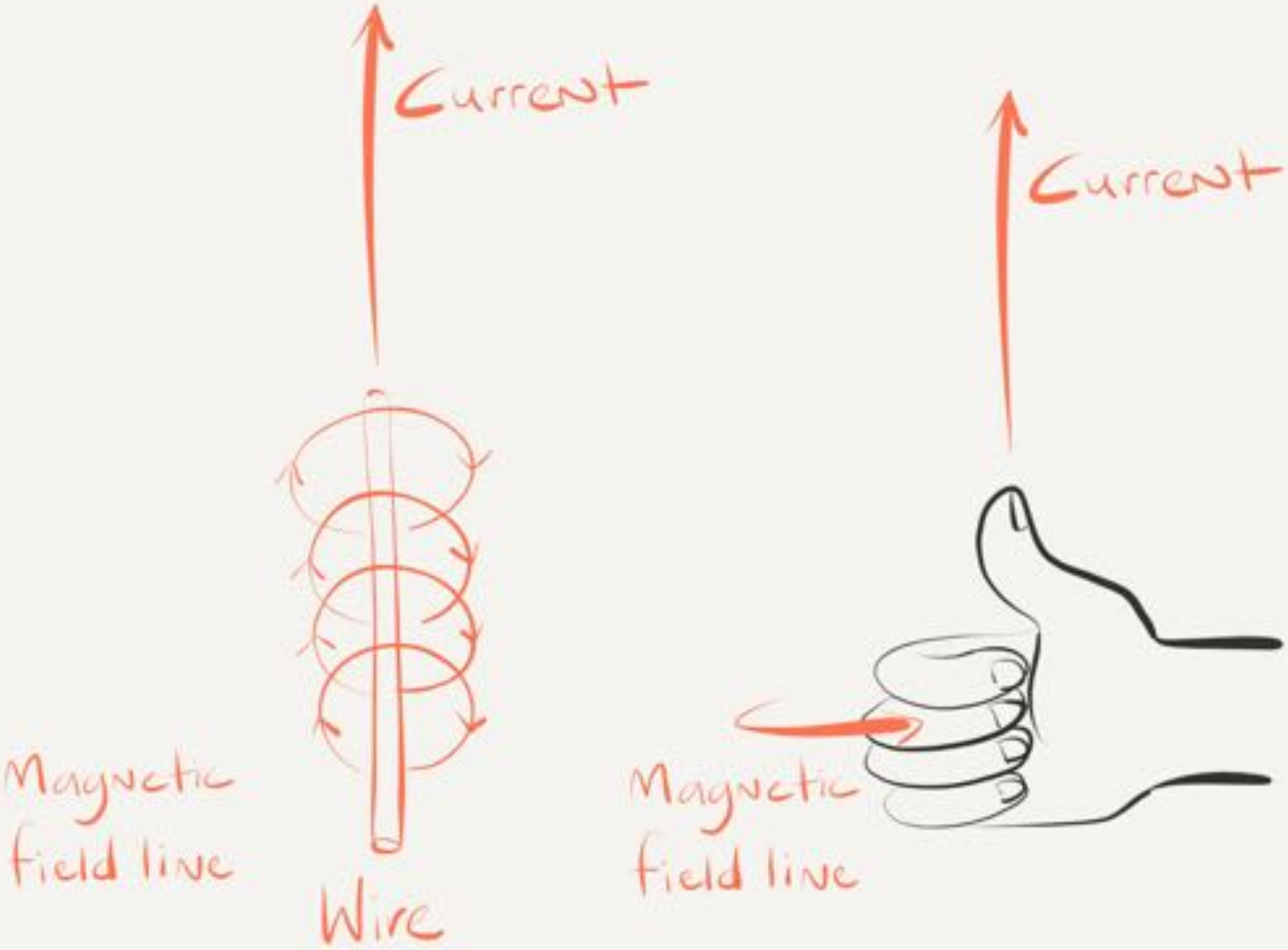
Ampere's Law

$$\mathcal{E} = \frac{d\Phi_B}{dt}$$

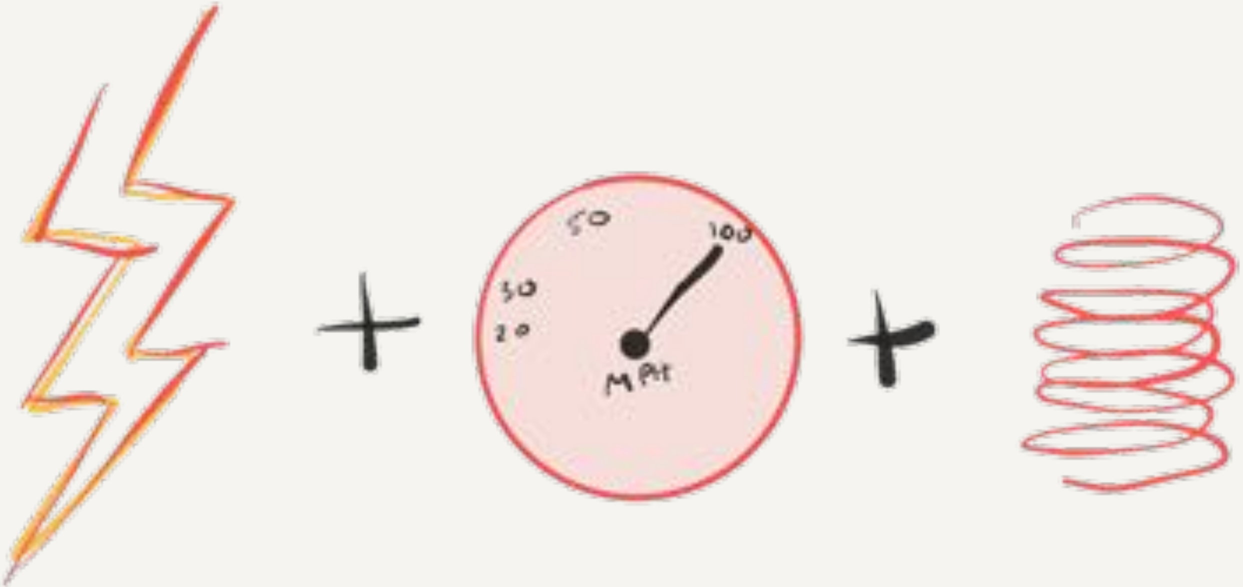
$\mathcal{E}$ = EMF

Φ_B = Magnetic flux

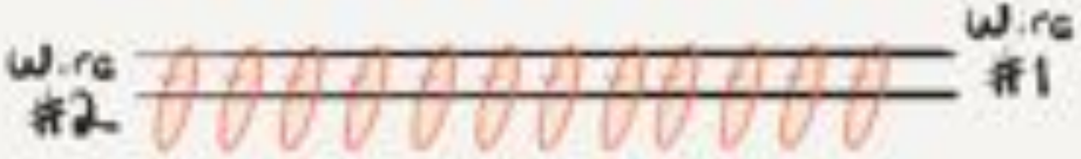
t = time

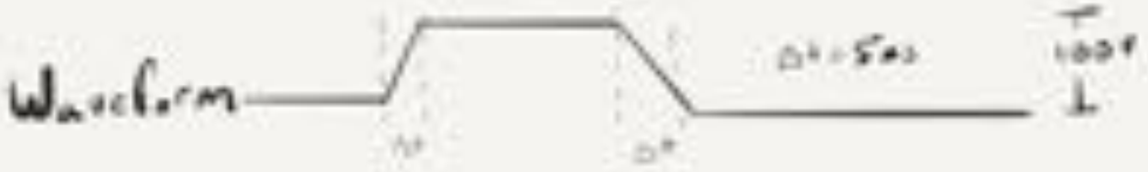

Current
Magnetic field line
Wire
Current
Magnetic field line

SUPER SECRET EMP FORMULA



Power + Speed + Coil


Wire #2
Wire #1


Waveform
Δt
Δt
Δt = 5ns
100V

Biot-Savart Law

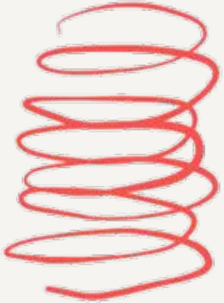
$$B_z = \frac{\mu_0}{4\pi} \frac{2\pi a^2 I}{(a^2 + z^2)^{3/2}}$$

B_z = Magnetic field strength

μ_0 = permeability of free space

I = current through loop

a = loop radius



Magnetic microprobe design for EM fault attack
Omarouayache, R and Raoult, J and Jarrix, S and Chusseau, L and Maurine, P

$$B_z = \frac{\mu_0}{4\pi} \frac{2\pi a^2 I}{(a^2 + z^2)^{3/2}}$$

Inverse Cube Law
field decay

$$\hookrightarrow B_z \propto 1/z^3$$

Magnetic microprobe design for EM fault attack
Omarouayache, R and Raoult, J and Jarrix, S and Chusseau, L and Maurine, P

Vector Potentials

$$B = \nabla \times A$$

$$\nabla \times \left(\frac{1}{\mu} \nabla \times A\right) = J$$

$$\nabla \times E = -\frac{\partial B}{\partial t}$$

$$\nabla \times H = \frac{\partial D}{\partial t} + J$$

$$\nabla \cdot D = \rho$$

$$\nabla \cdot B = 0$$

$$\nabla \cdot J = \frac{\partial \rho}{\partial t}.$$

Perfect Conducting

$$\hat{n} \times E = 0$$

$$\hat{n} \cdot B = 0$$

Imperfectly Conducting

$$E - (\hat{n} \cdot E)\hat{n} = \eta Z_0 \hat{n} \times H$$

$$\frac{1}{\mu_{r_1}} \hat{n} \times (\nabla \times E) - \frac{jk_0}{\eta} \hat{n} \times (\hat{n} \times H) = 0$$

Vector Wave Equations

$$\nabla \times \left(\frac{1}{\mu} \nabla \times E\right) - \omega^2 \epsilon E = -j\omega J$$

$$\nabla \times \left(\frac{1}{\epsilon} \nabla \times H\right) - \omega^2 \mu H = \nabla \times \left(\frac{1}{\epsilon} J\right)$$

Time Harmonic Fields

$$\nabla \times E = -j\omega B \quad \nabla H = j\omega D + J$$

$$\nabla \cdot J = -j\omega\rho$$

$$E(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} E(\omega) e^{j\omega t} d\omega$$

$$E(\omega) = \int_{-\infty}^{\infty} E(t) e^{-j\omega t} dt$$

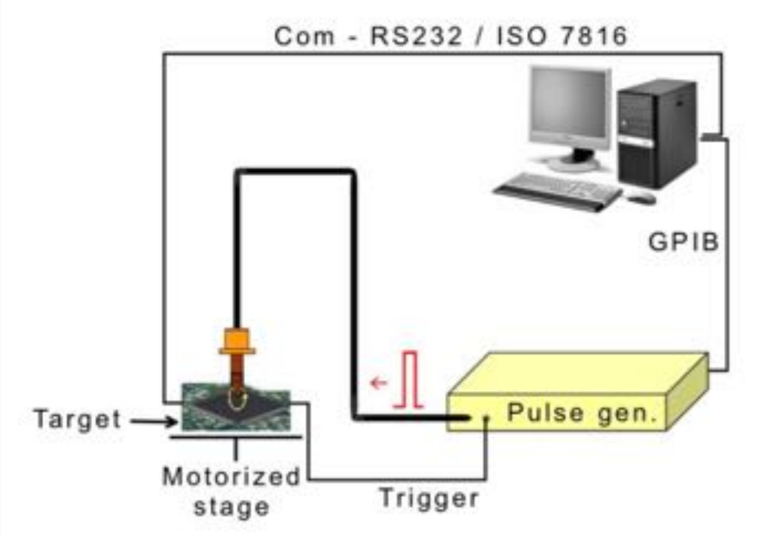
Radiation Condition

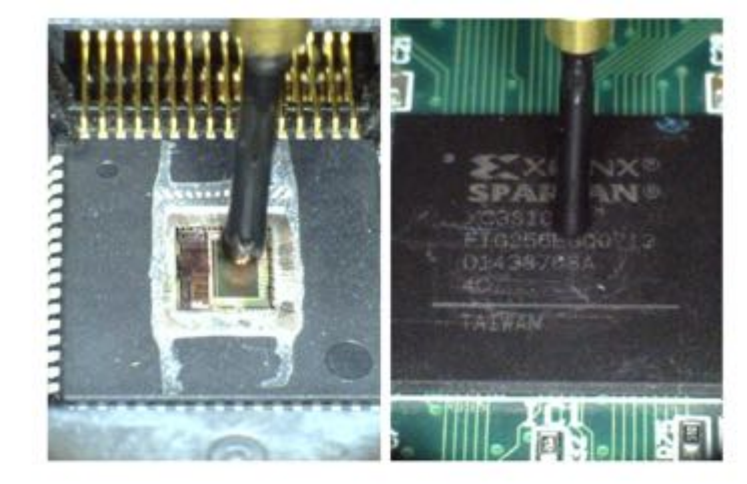
$$\lim_{r \to \infty} r\left[\nabla \times \begin{pmatrix} E \\ H \end{pmatrix} + jk_0 \begin{pmatrix} E_t \\ H_t \end{pmatrix}\right] = 0$$

Scalar Wave Equation

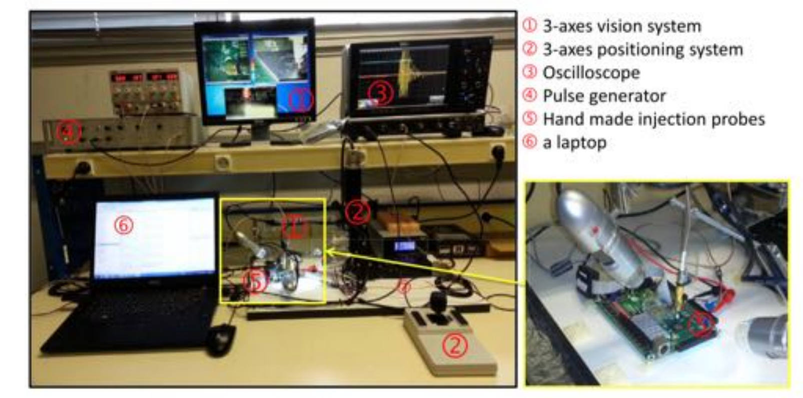
$$\left[\frac{\partial}{\partial x}\left(\frac{1}{\mu_x} \frac{\partial}{\partial x}\right) + \frac{\partial}{\partial y}\left(\frac{1}{\mu_r} \frac{\partial}{\partial y}\right) + k_0^2 \mu_x\right] E_z = jk_0 Z_0 J_z$$

It's been done…

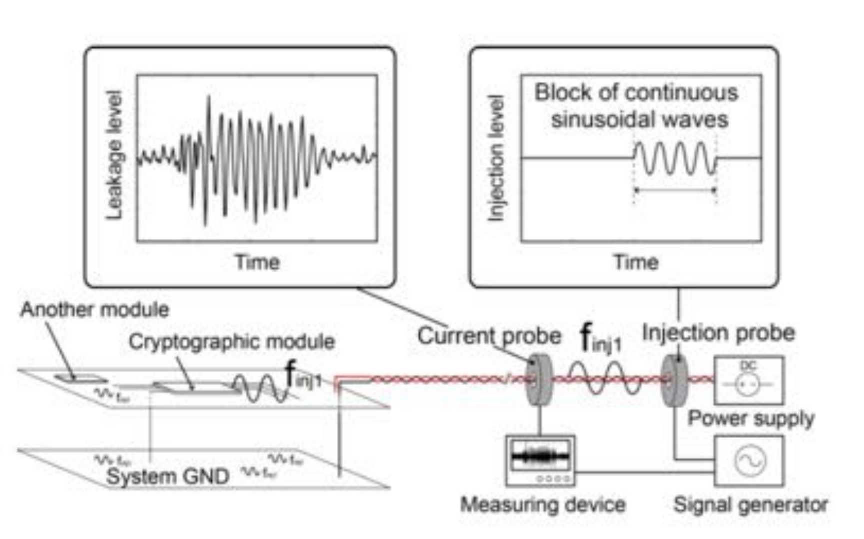




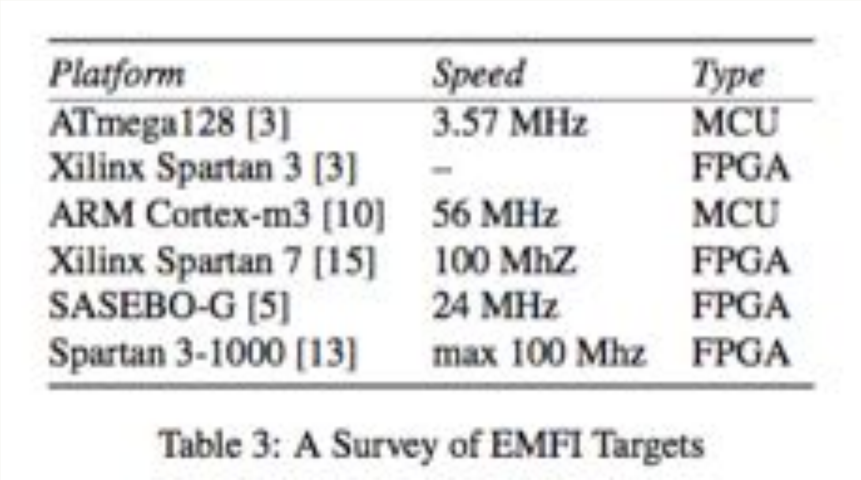
Amine Dehbaoui∗, Jean-Max Dutertre†, Bruno Robisson∗ and Assia Tria∗
S. Ordas1 · L. Guillaume-Sage1 · P. Maurine1,2



S. Ordasl · L. Guillaume-Sagel · P. Maurinel,2



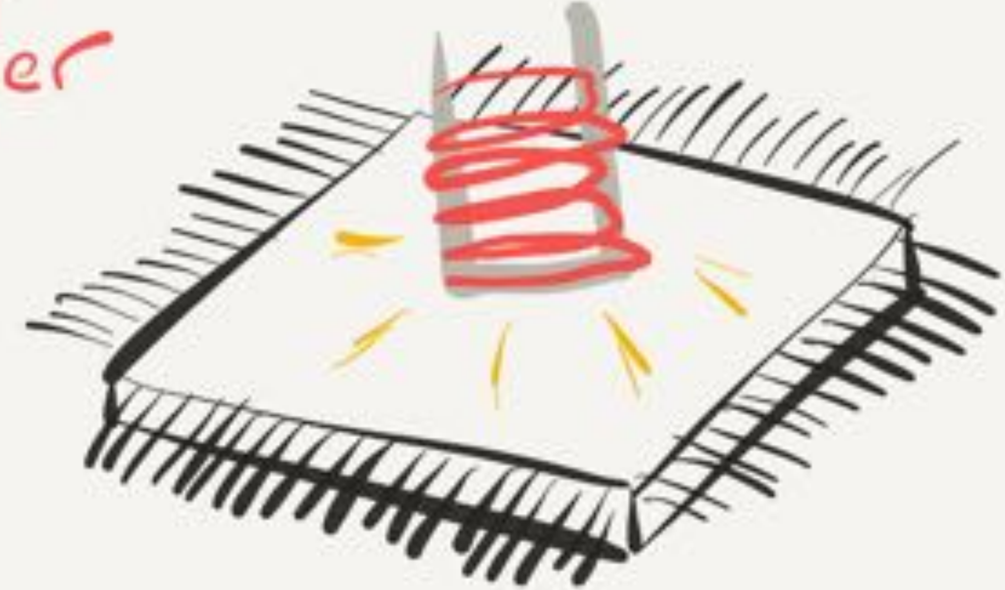
Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone

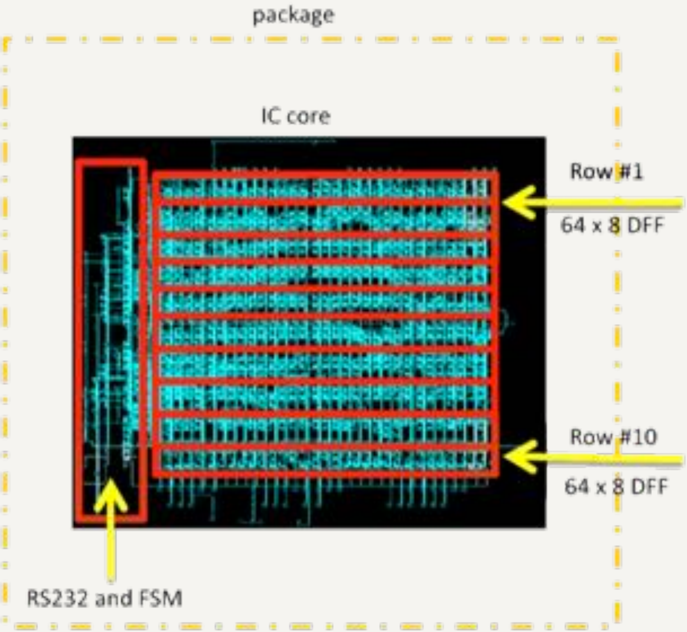


Platform	*Speed*	*Type*
ATmega128 [3]	3.57 MHz	MCU
Xilinx Spartan 3 [3]	–	FPGA
ARM Cortex-m3 [10]	56 MHz	MCU
Xilinx Spartan 7 [15]	100 MhZ	FPGA
SASEBO-G [5]	24 MHz	FPGA
Spartan 3-1000 [13]	max 100 Mhz	FPGA

Table 3: A Survey of EMFI Targets

First Order EMFI





package

IC core

Row #1

64 x 8 DFF

Row #10

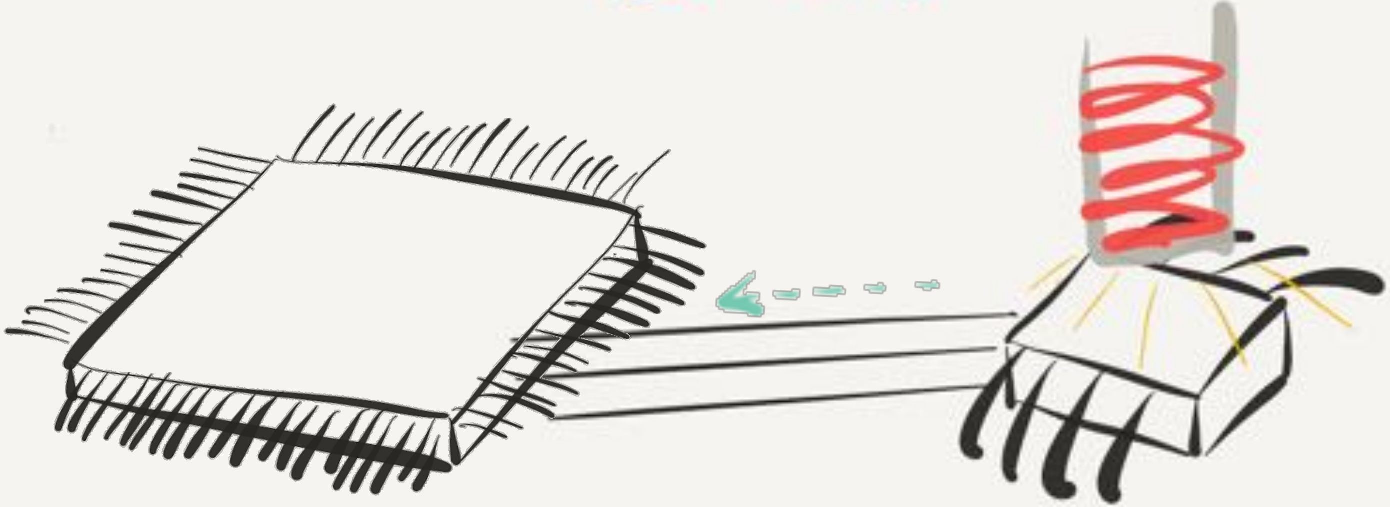
64 x 8 DFF

RS232 and FSM

Cisco 8861/8851

- Dual Core ARMv7
- Broadcom BCM11125
- Processor @ 1001MHz
- Secure Boot

Second Order EMFI



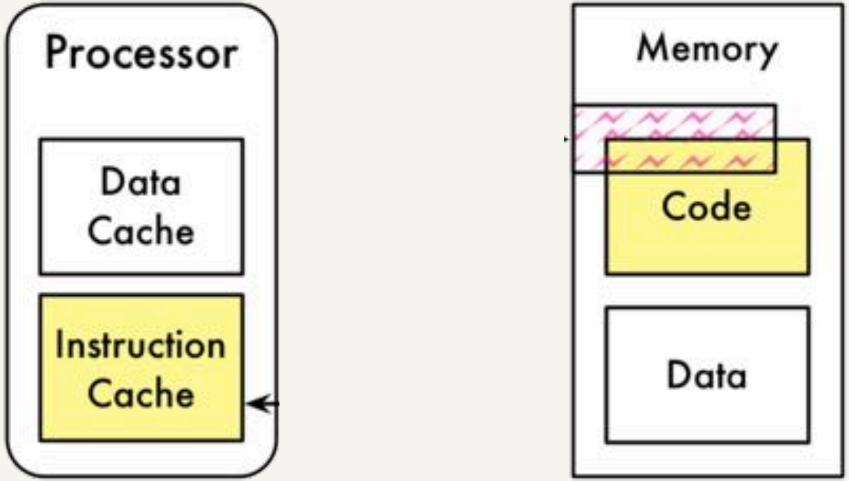


Figure 3: A Second-Order EMFI Attack

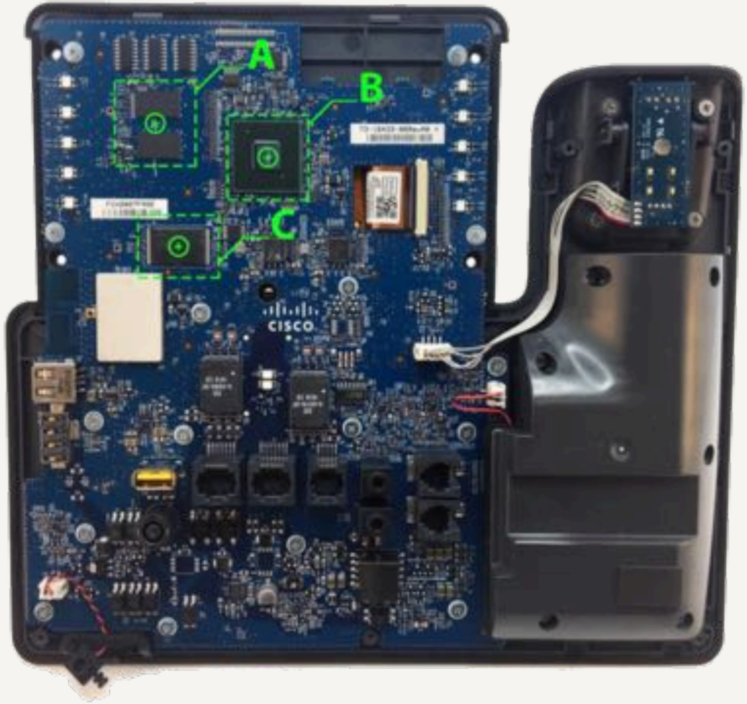


Figure 6: PCB of device under attack.

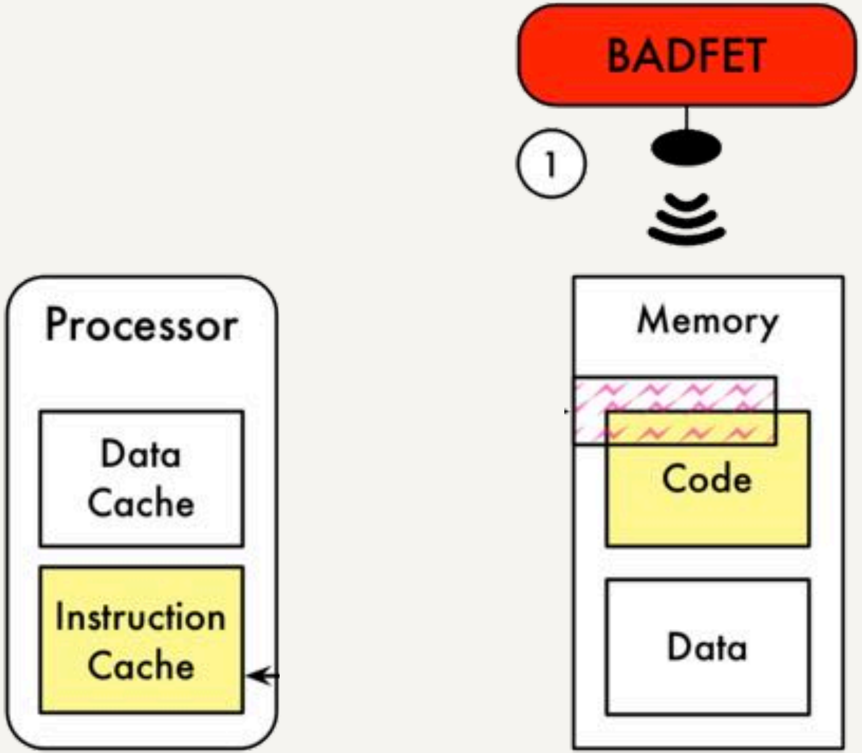


Figure 3: A Second-Order EMFI Attack

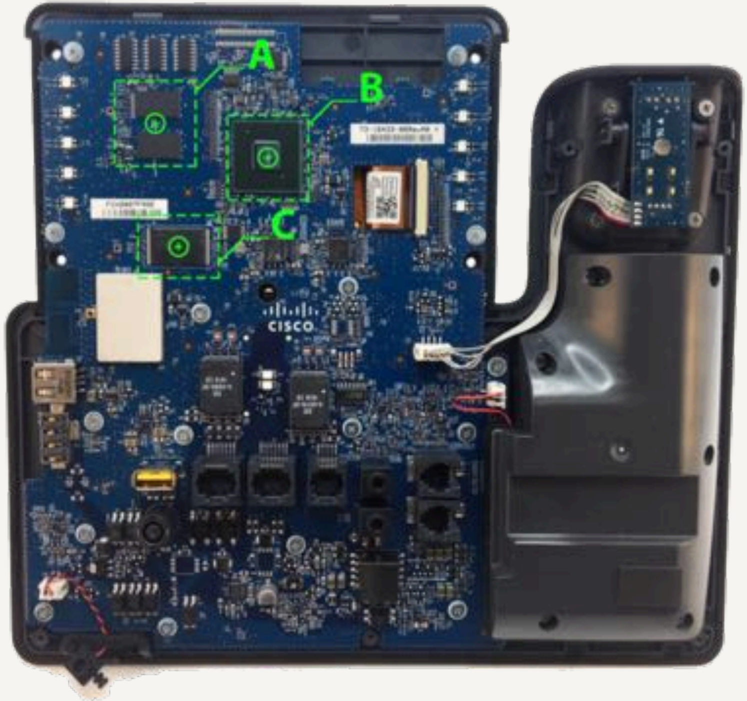


Figure 6: PCB of device under attack.

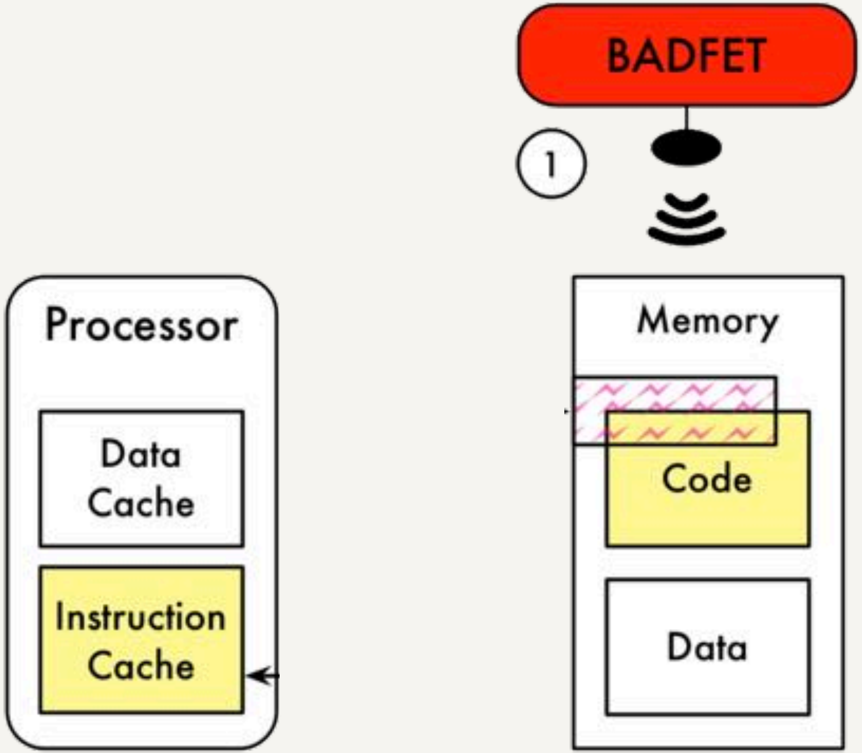


Figure 3: A Second-Order EMFI Attack

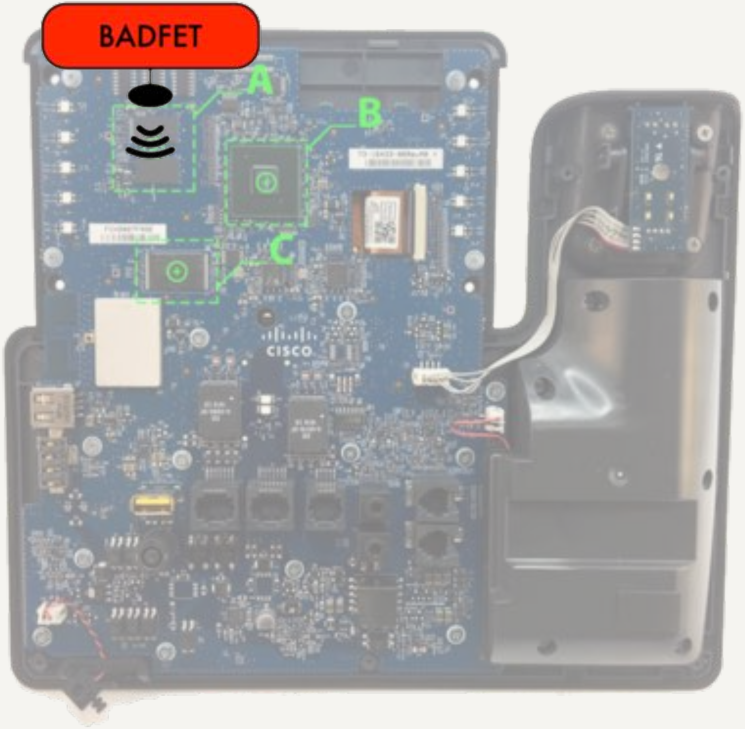


Figure 6: PCB of device under attack.

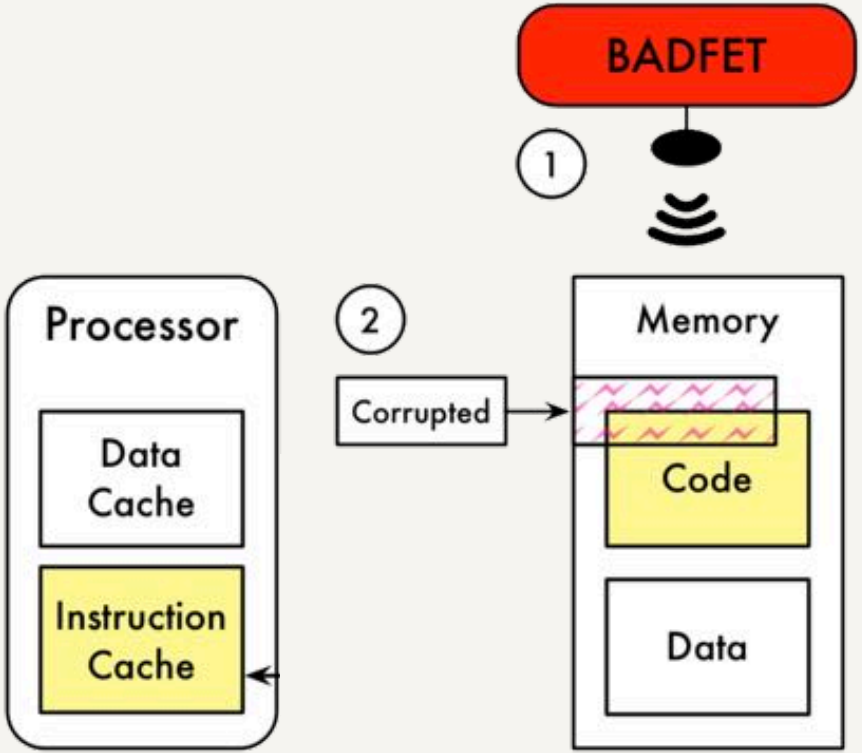


Figure 3: A Second-Order EMFI Attack

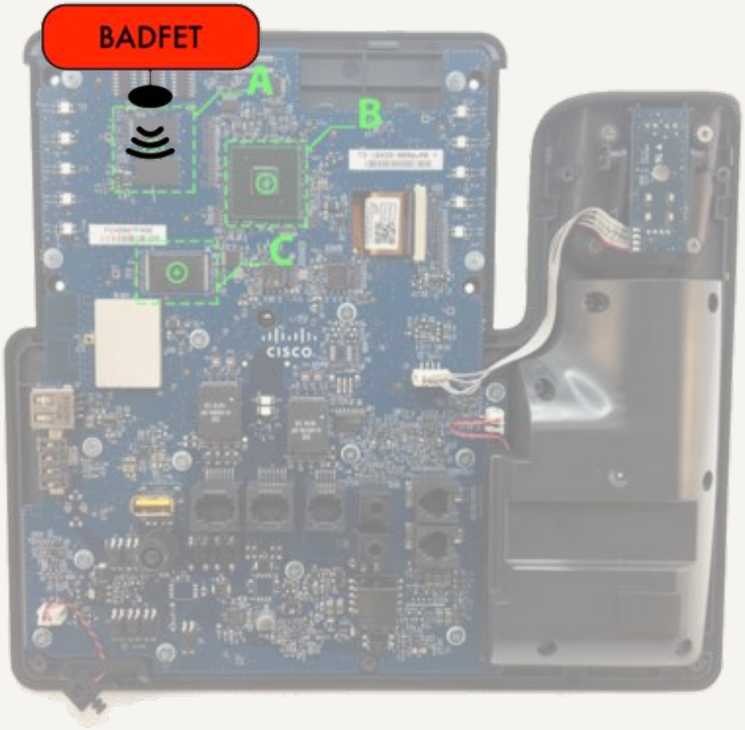


Figure 6: PCB of device under attack.

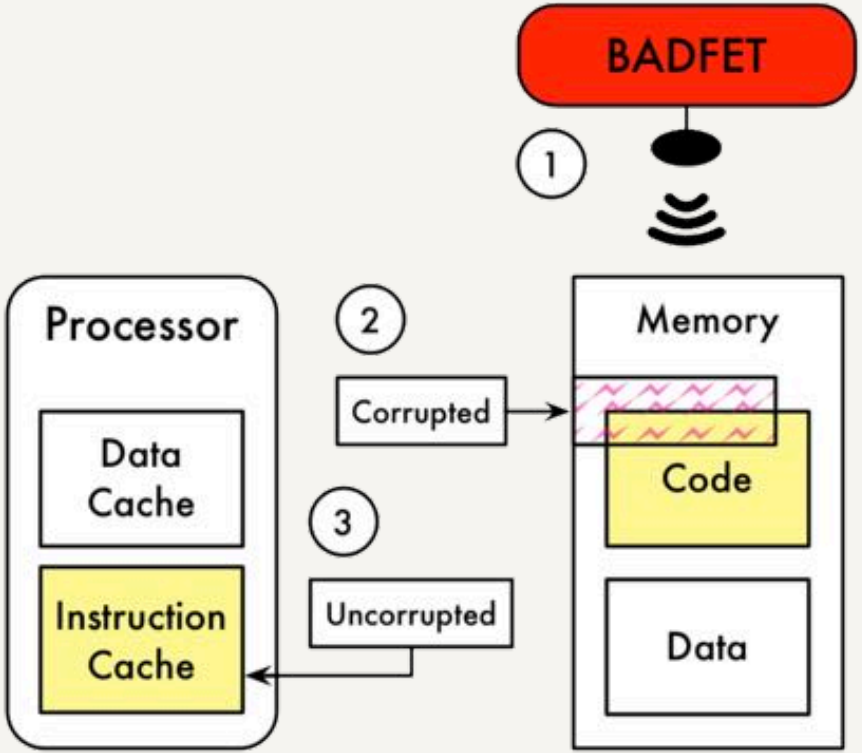


Figure 3: A Second-Order EMFI Attack

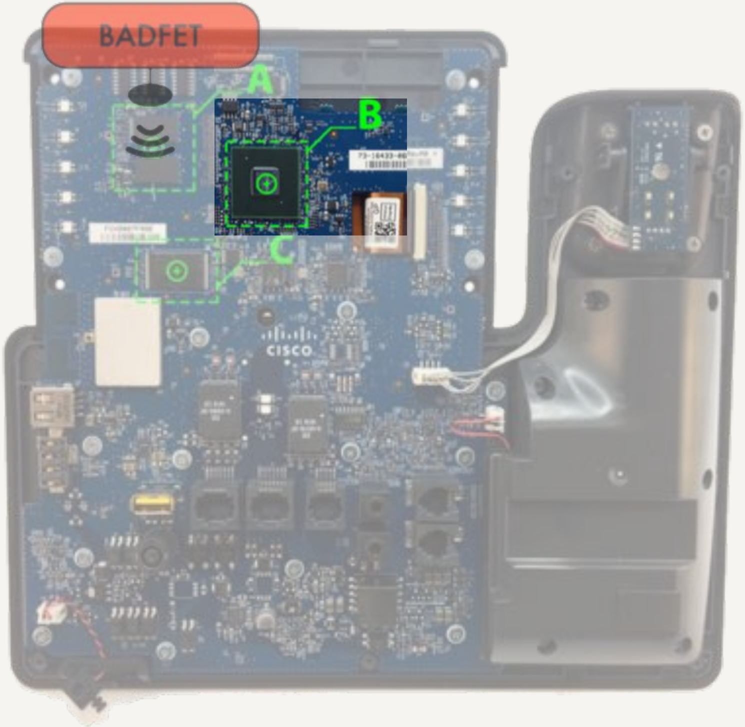


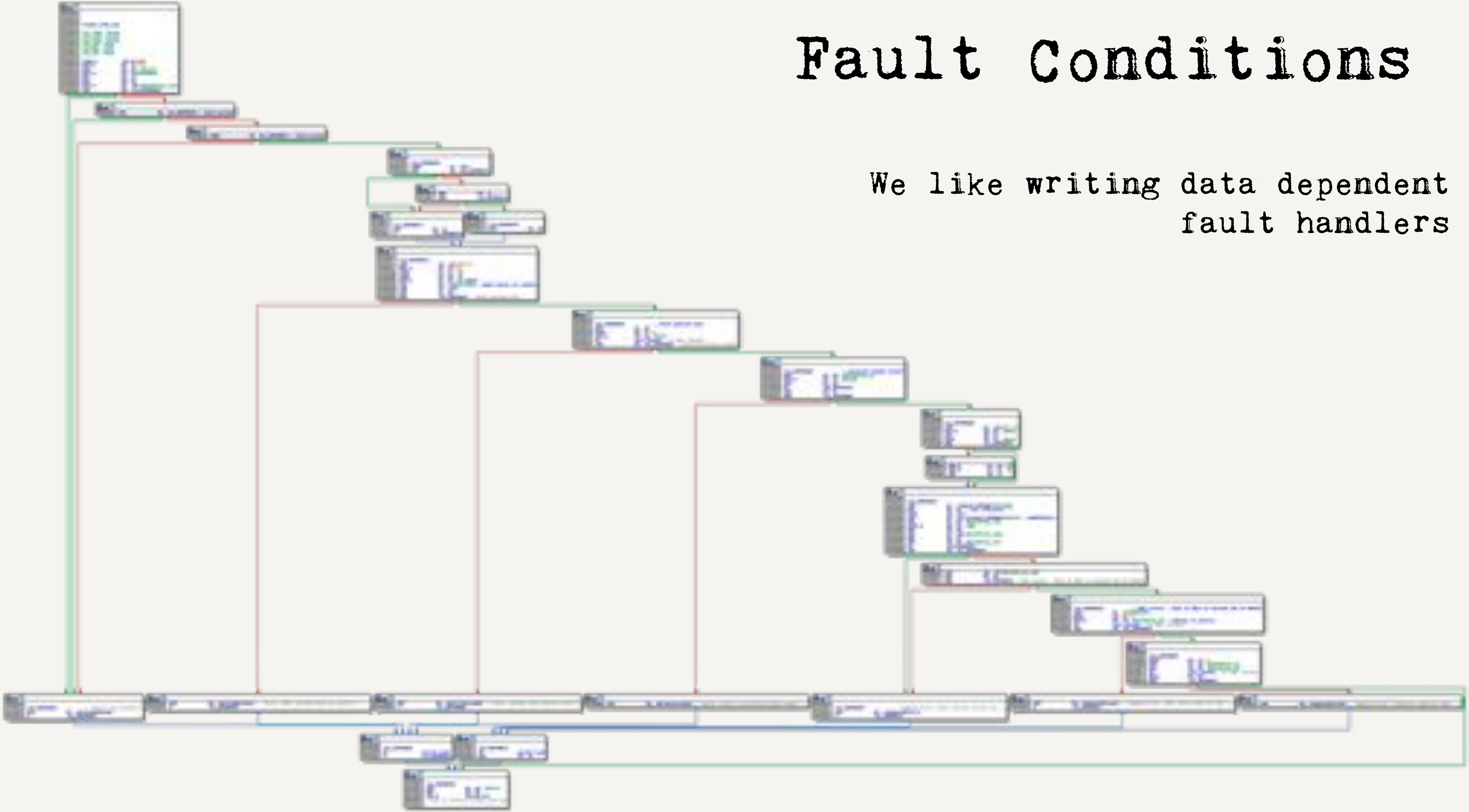
Figure 6: PCB of device under attack.

Example Second-Order EMFI Attack

- Indiscriminant of DATA
- CODE integrity is preserved in ICACHE

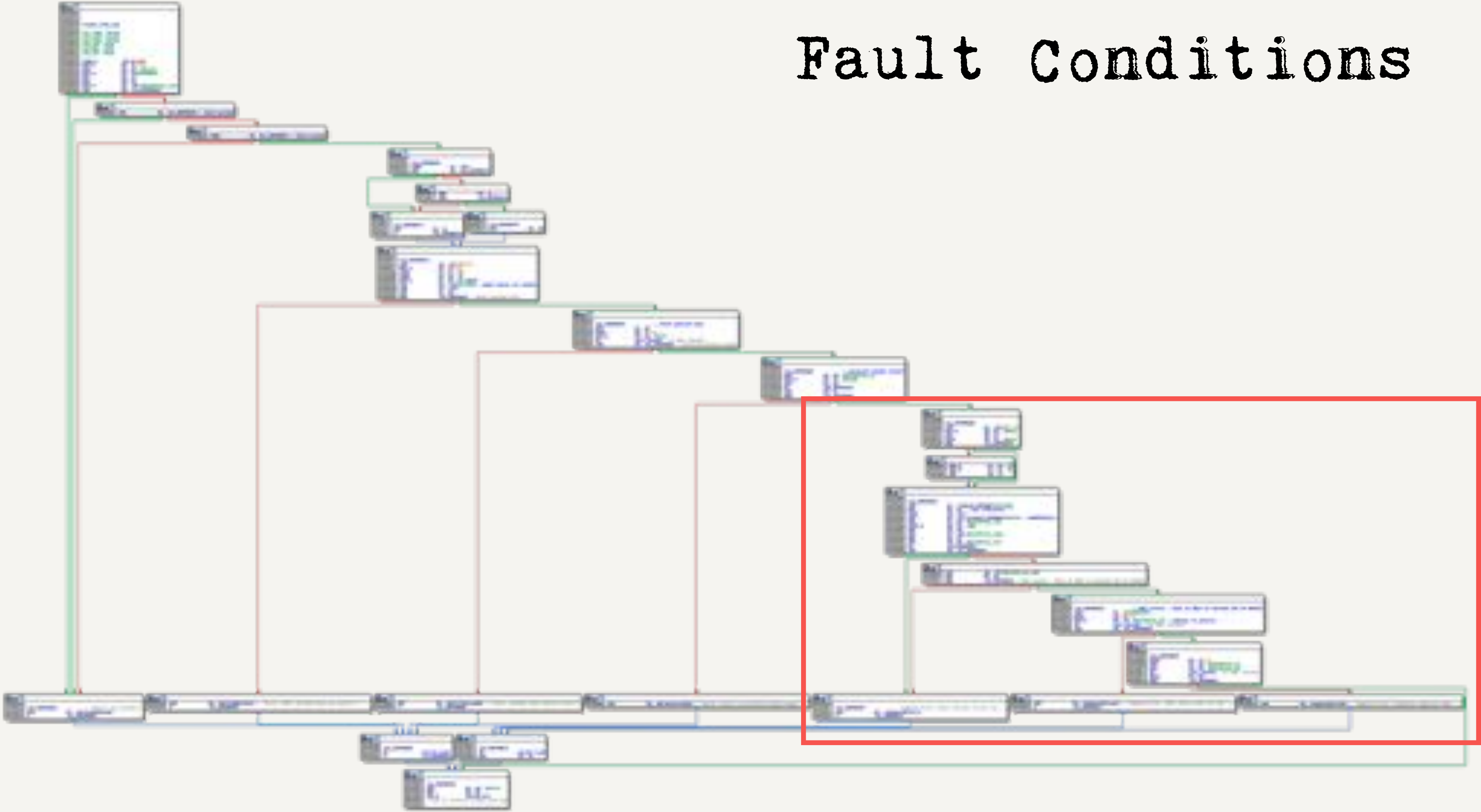
- Cause error-handling code to process corrupted data

Fault Conditions

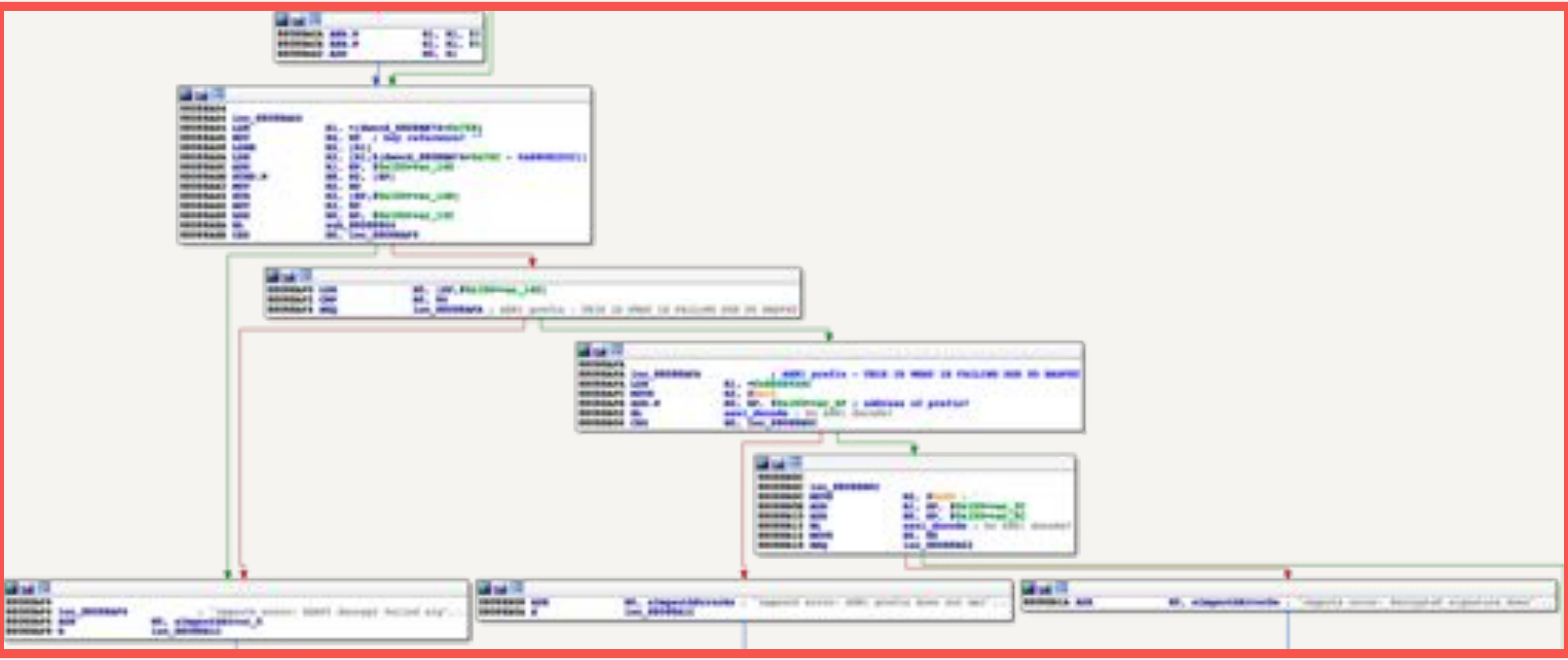


We like writing data dependent fault handlers

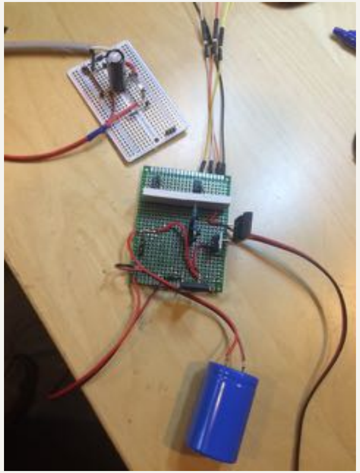
Fault Conditions

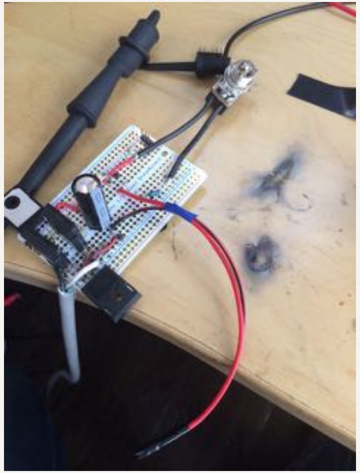


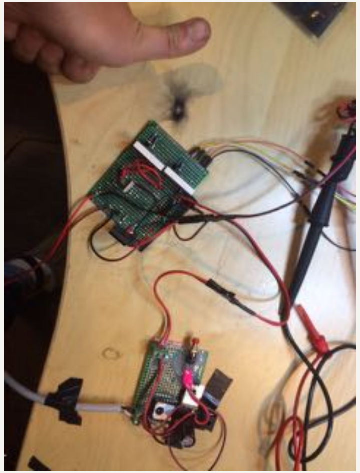
Fault Conditions

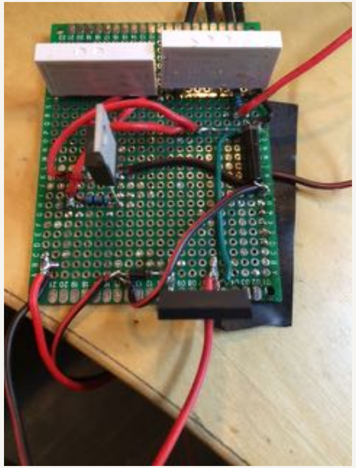


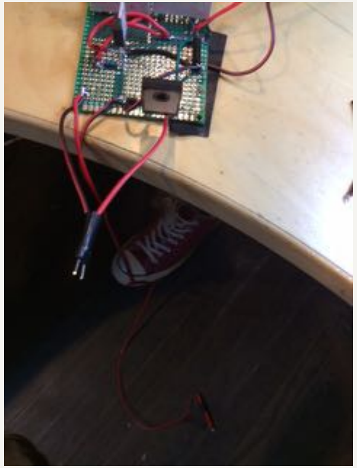
Let's Build Our Own EMP



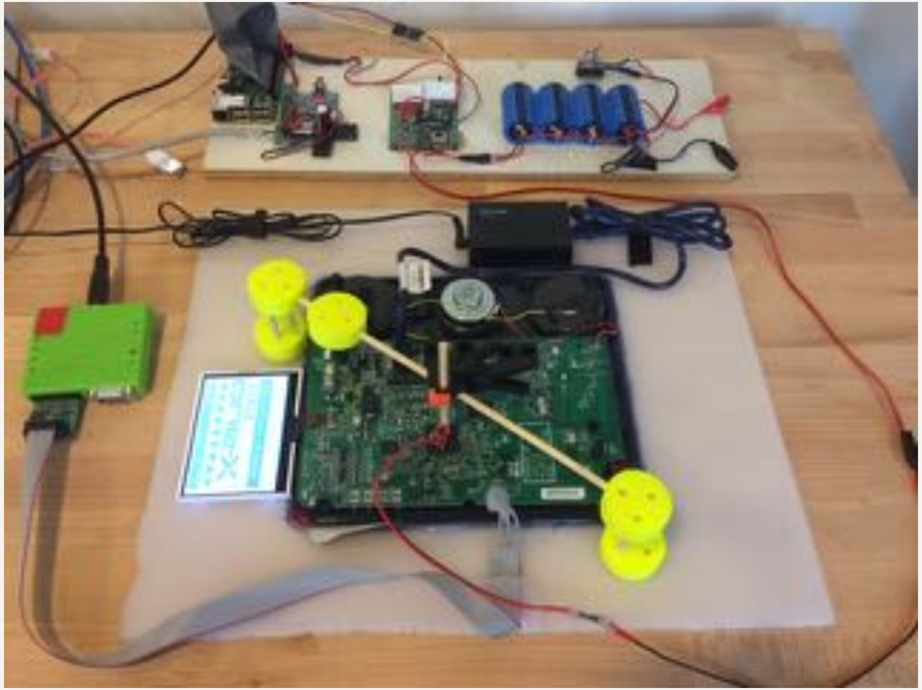








Widowmaker



After the death of many Raspberry PI's…

And lots of loud bangs…

Decided to take a break

Rick knows how electrons work better than me

Rick is either incredibly brave. Or…

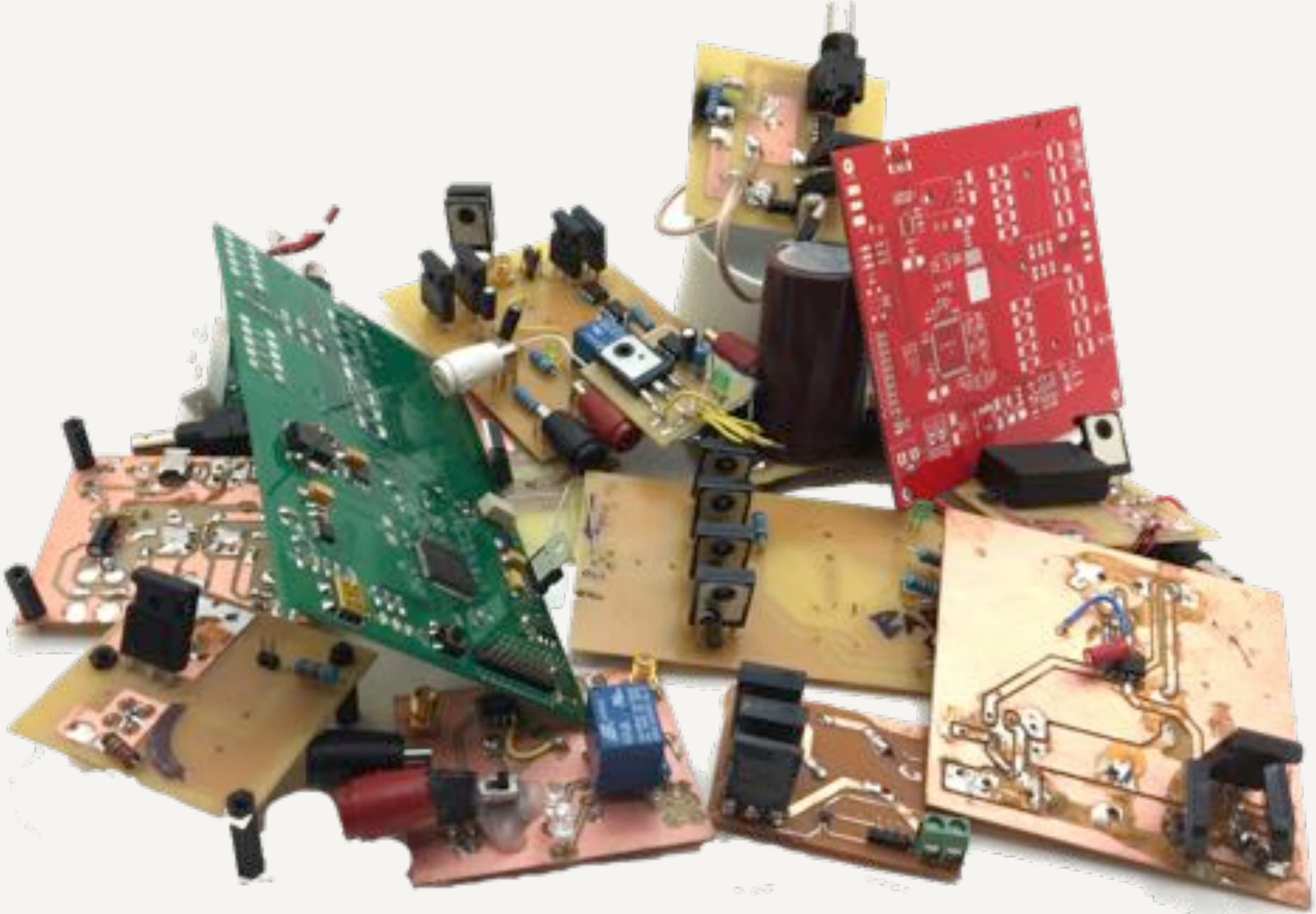
HAY RICK!

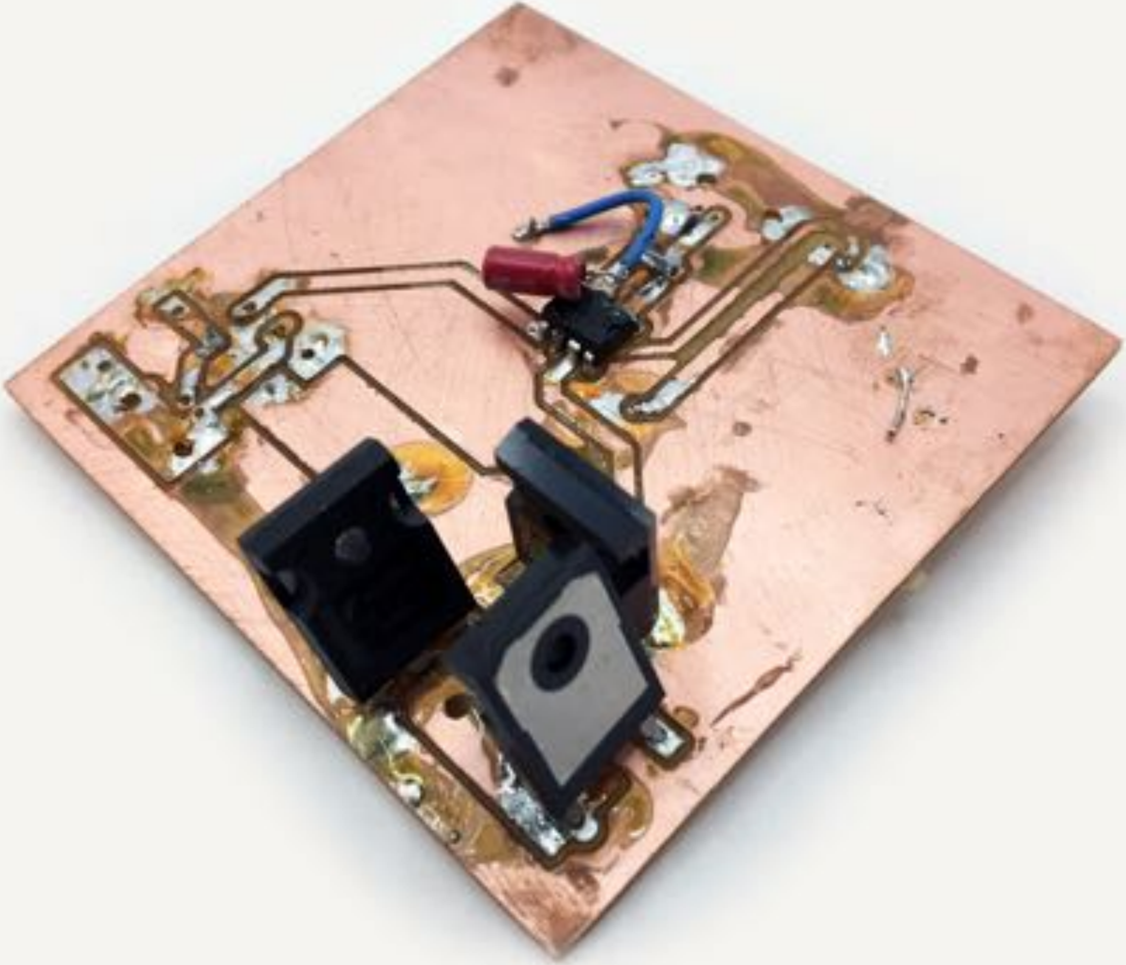
PROJECT

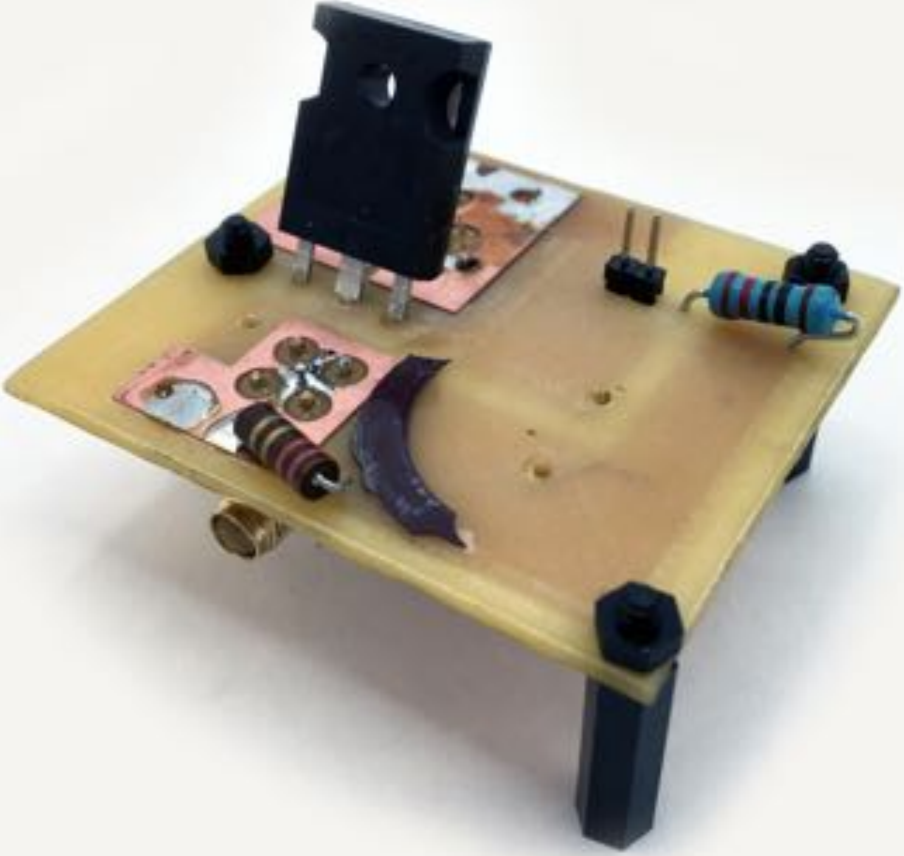
RADFET

- Requirements
  - Fast pulsing
  - Multiple pulses
  - Larger Distance (no decapping)
  - Cheaper
  - Controllable/Standalone

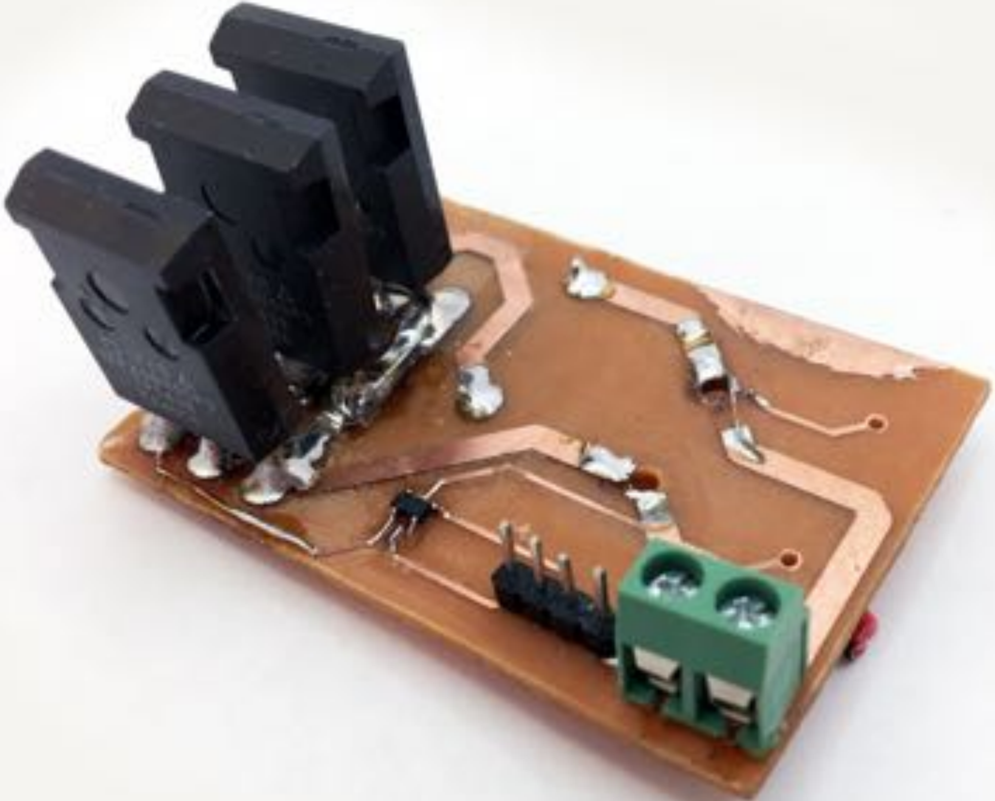
went through many versions of BADFETS

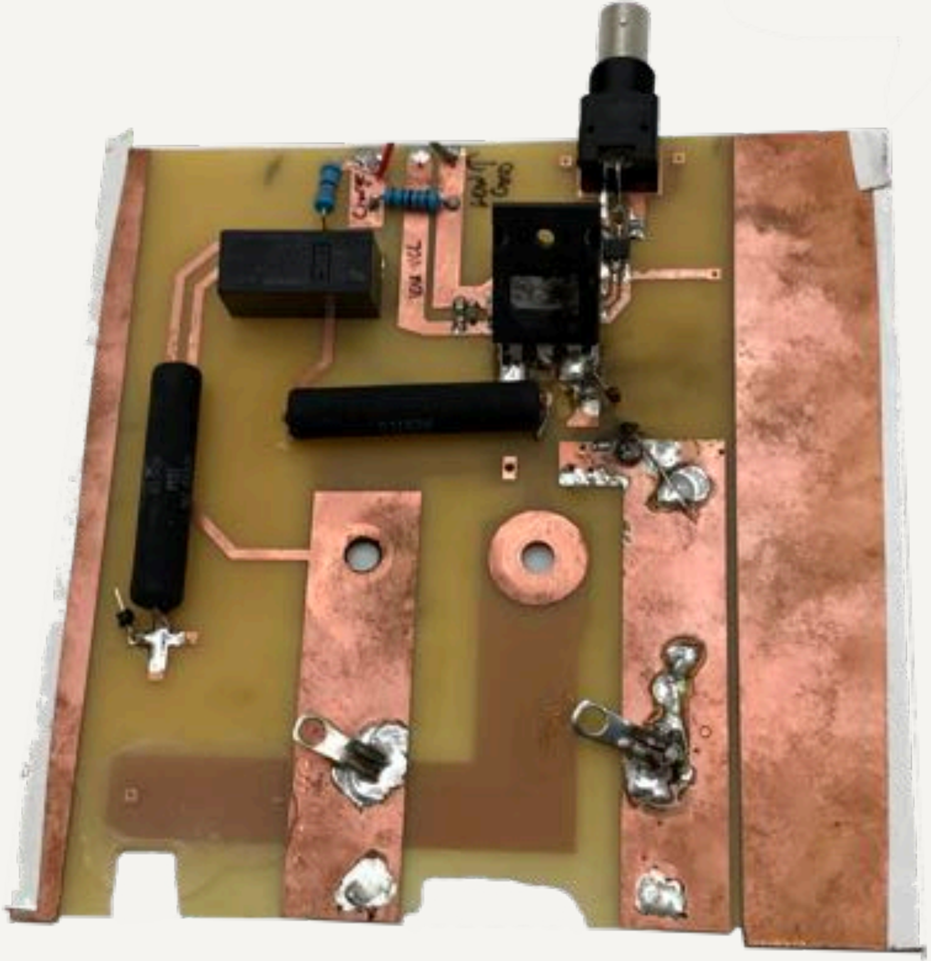


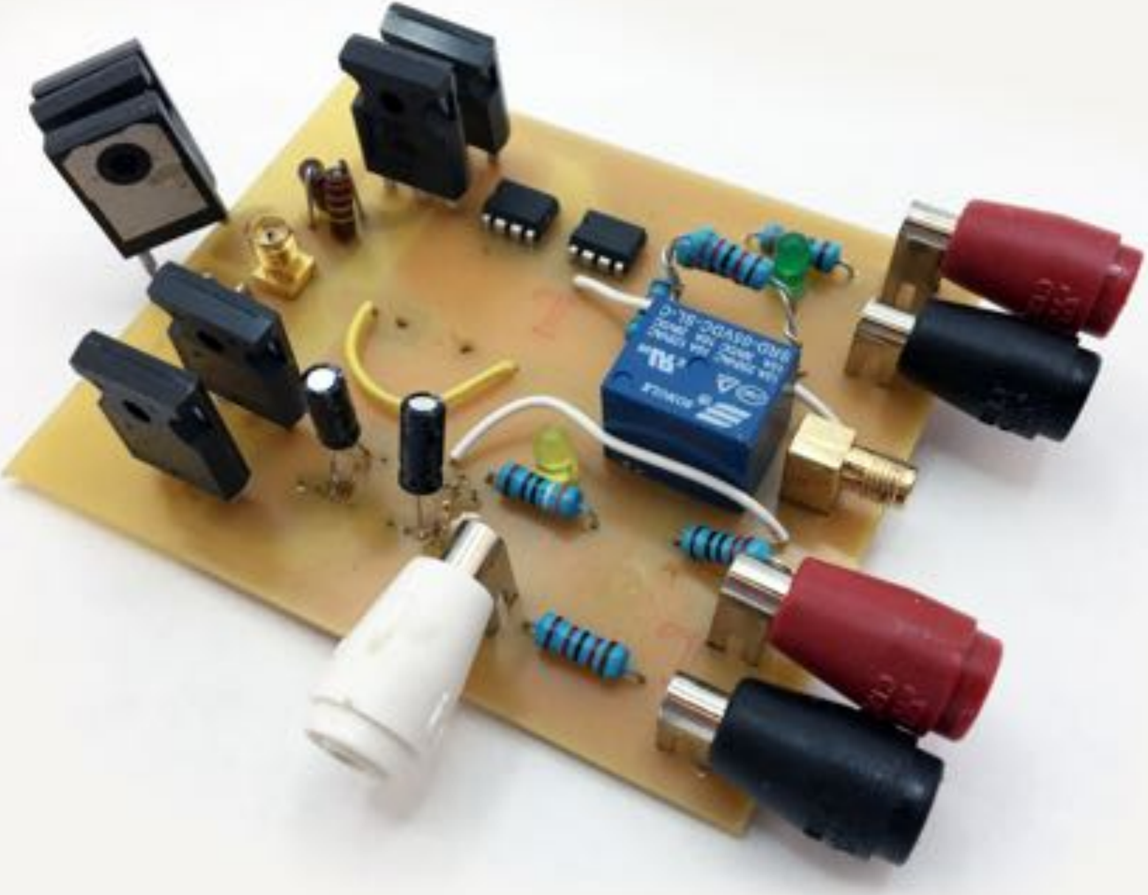


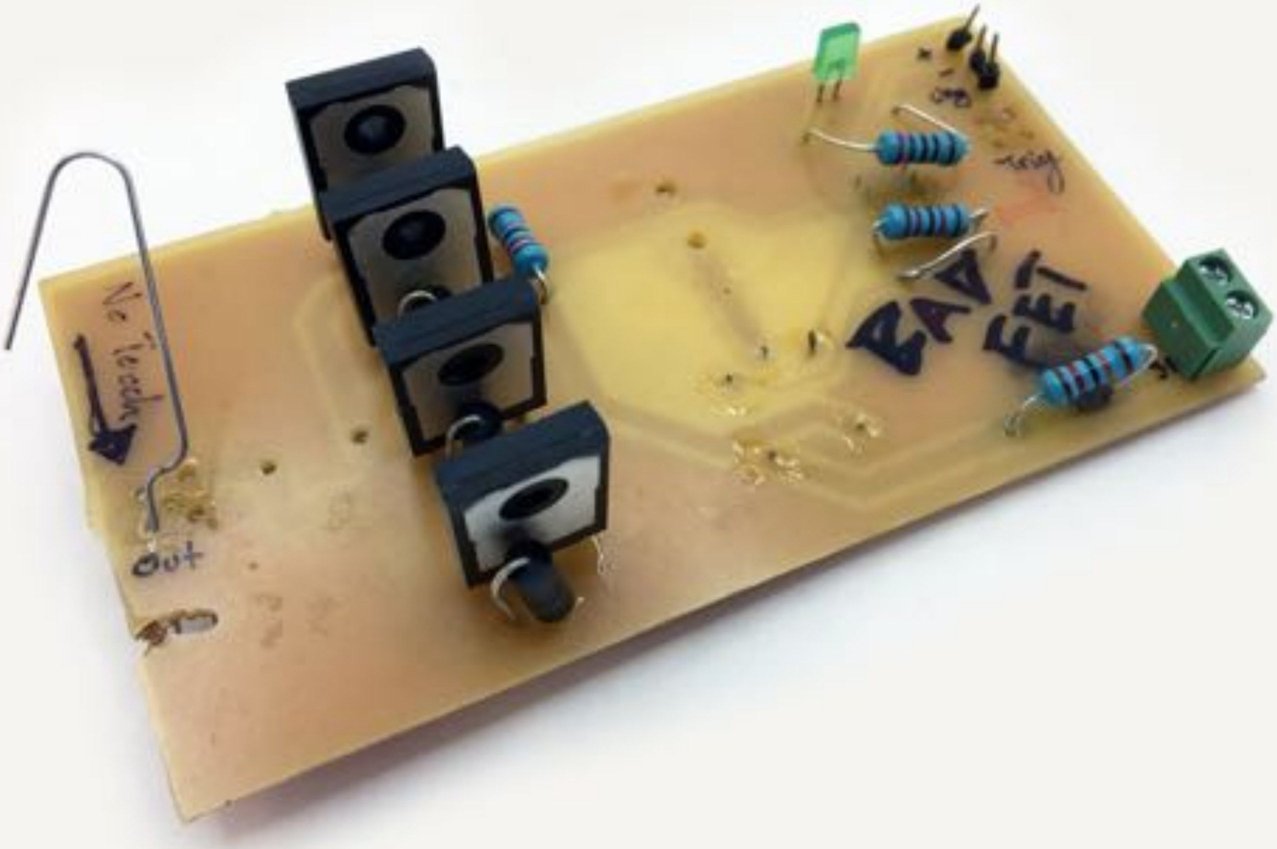


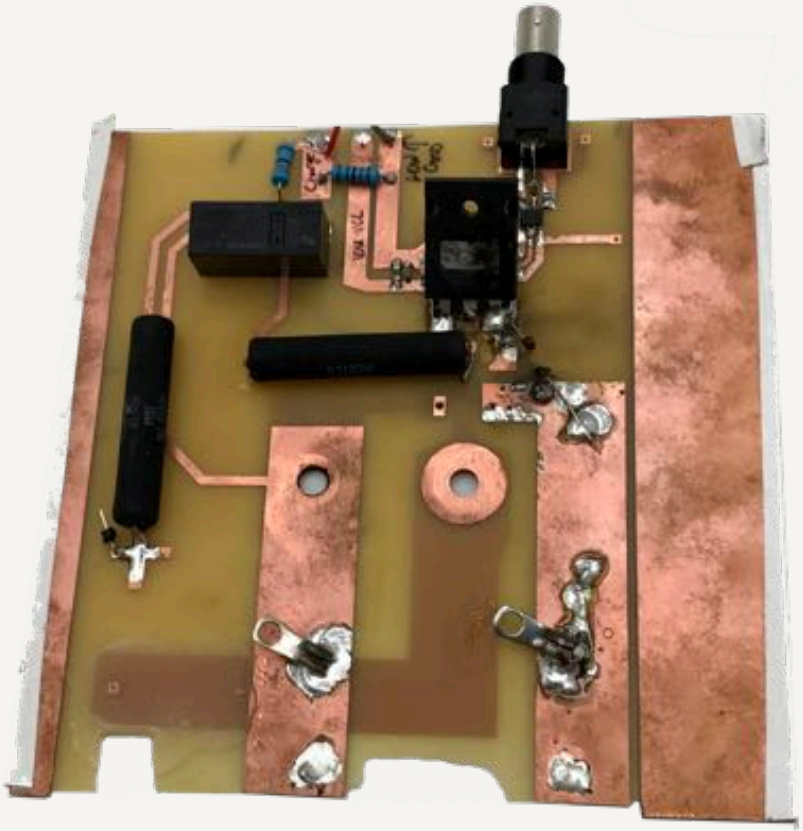
SONGLE
10A 250VAC 10A 125VAC
10A 30VDC 10A 28VDC
SRD-05VDC-SL-C



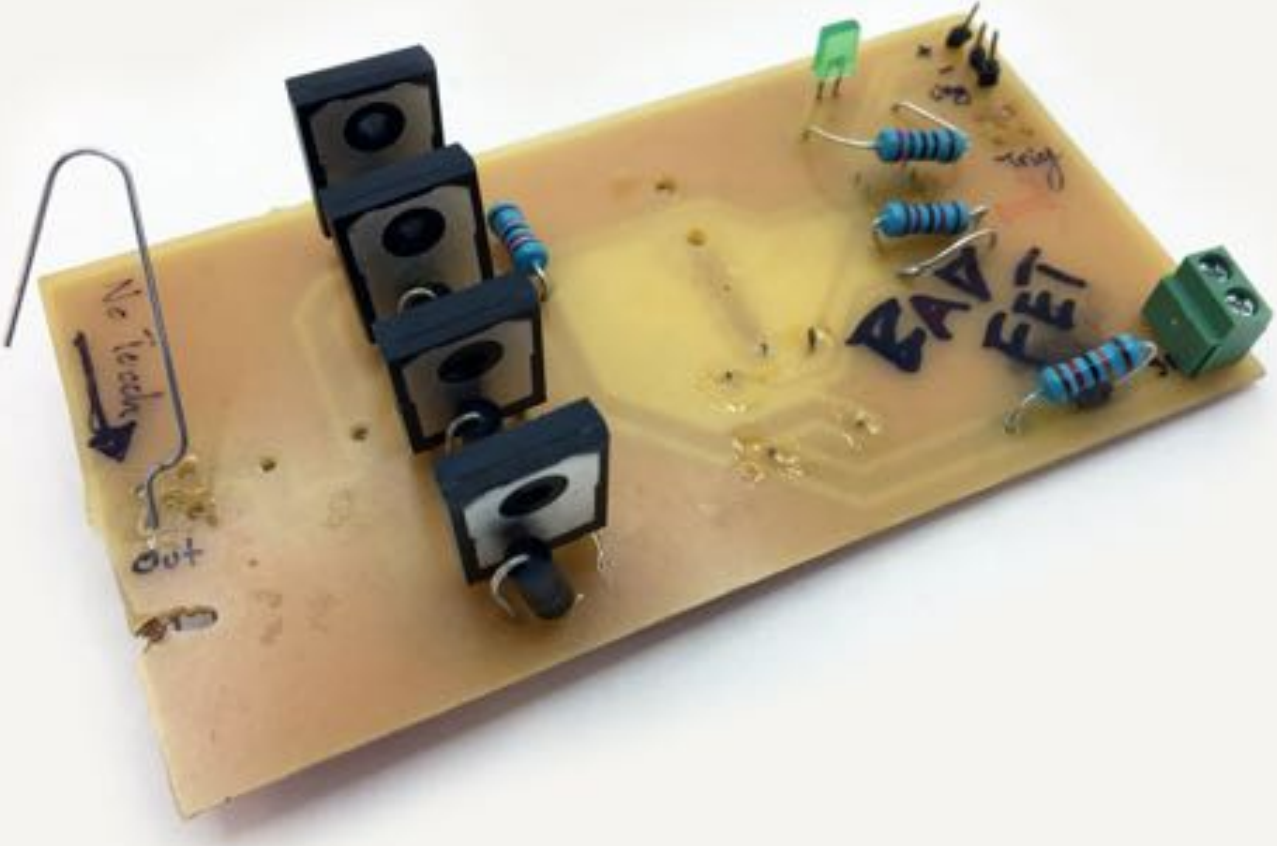

10V VCC

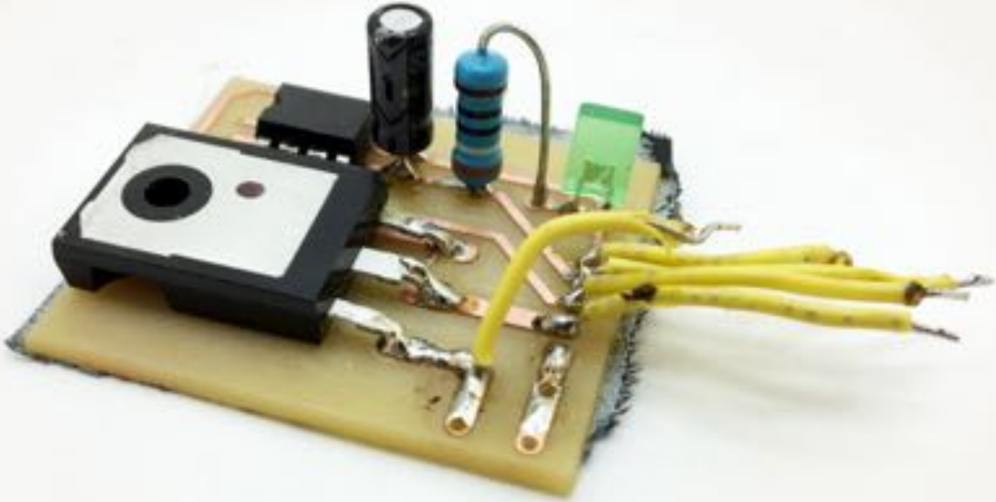



Ne Touchy
Out
trig
BAD FET

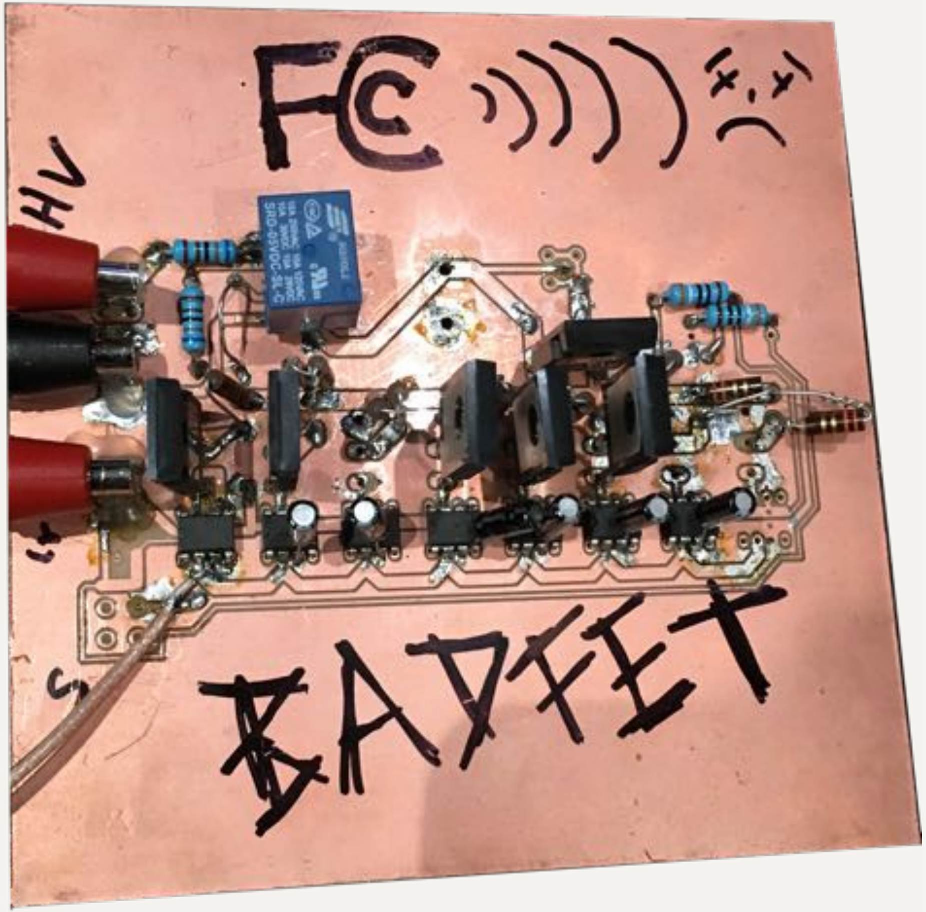


±10%
600 Vdc
+85°C


Ve Teach
Out
trig
BAD
FET

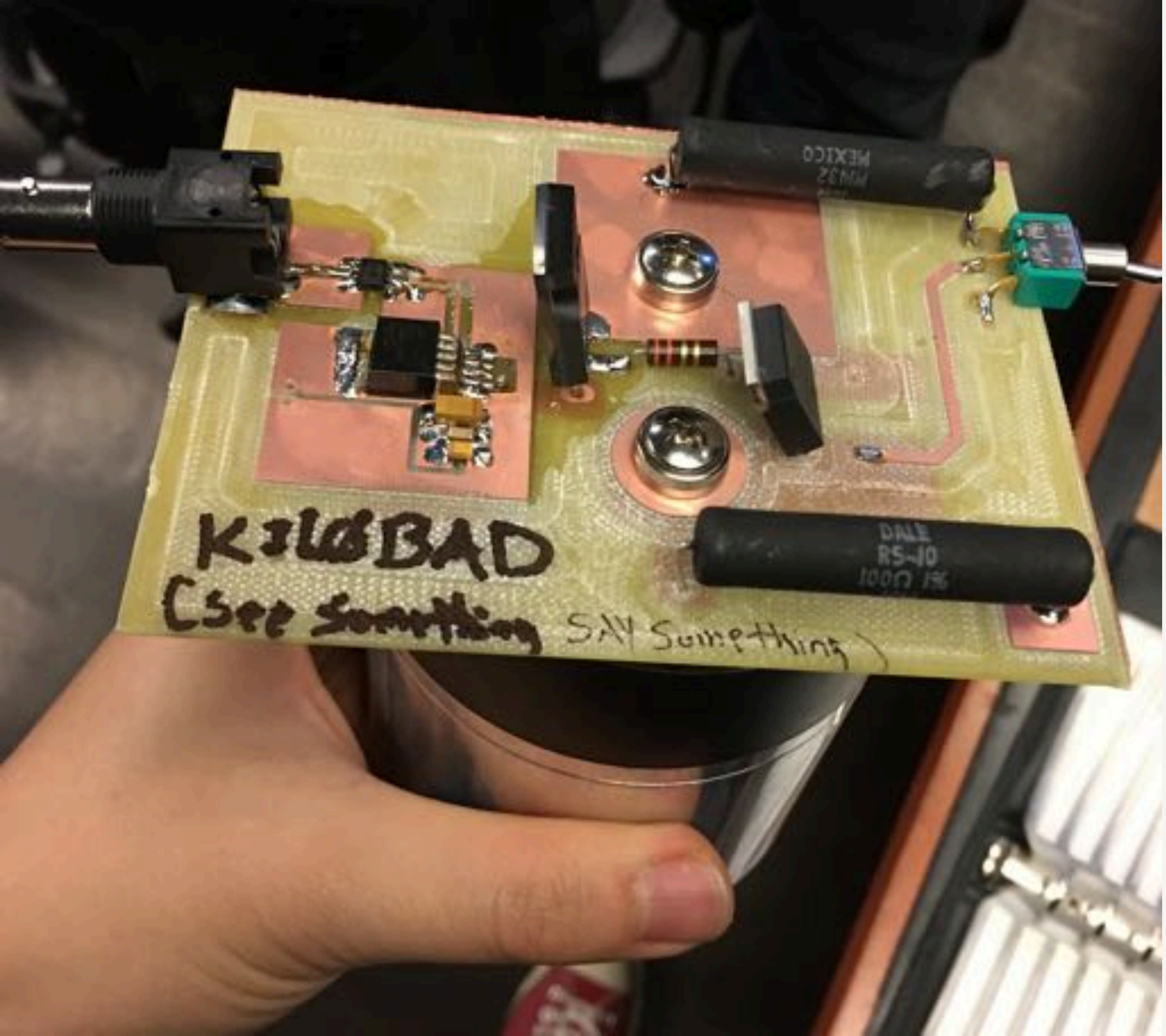


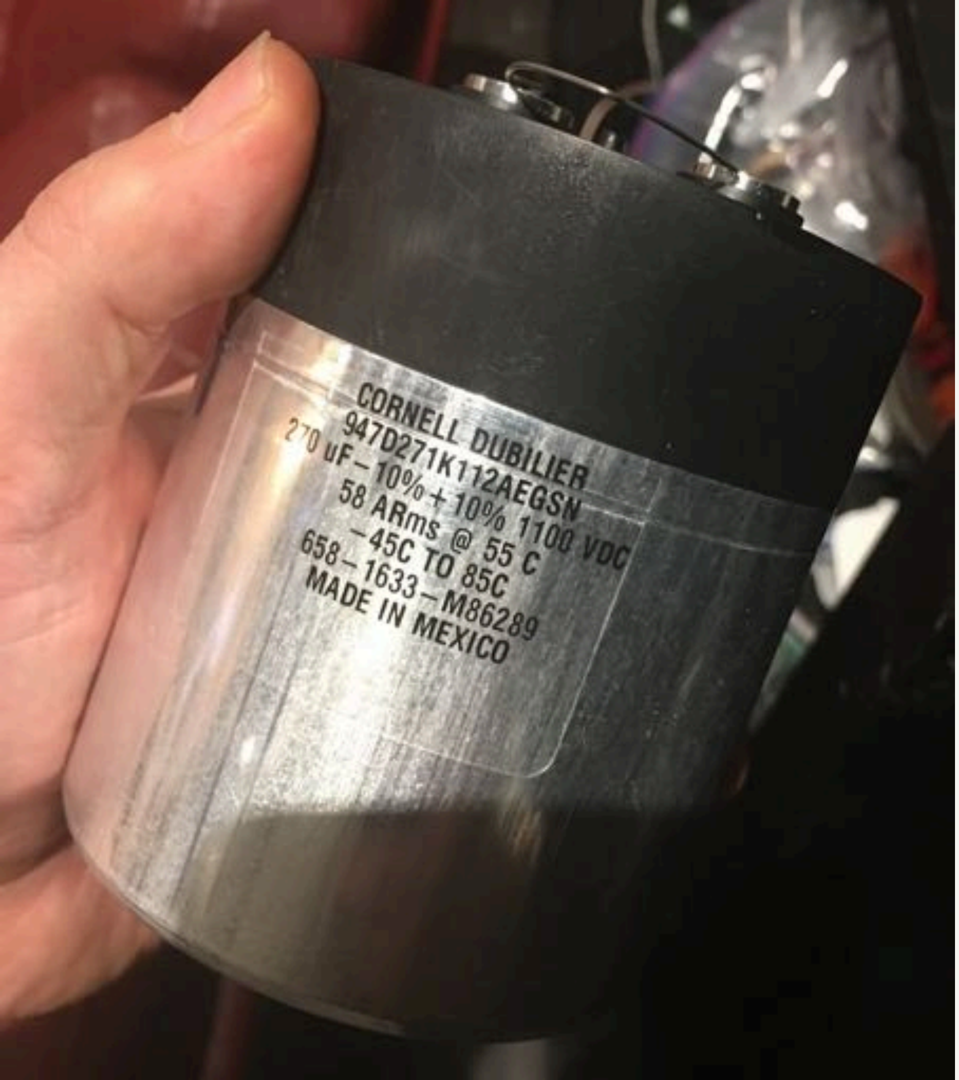
Some mistakes are more precious than others



OCTALBAD

KILOBAD

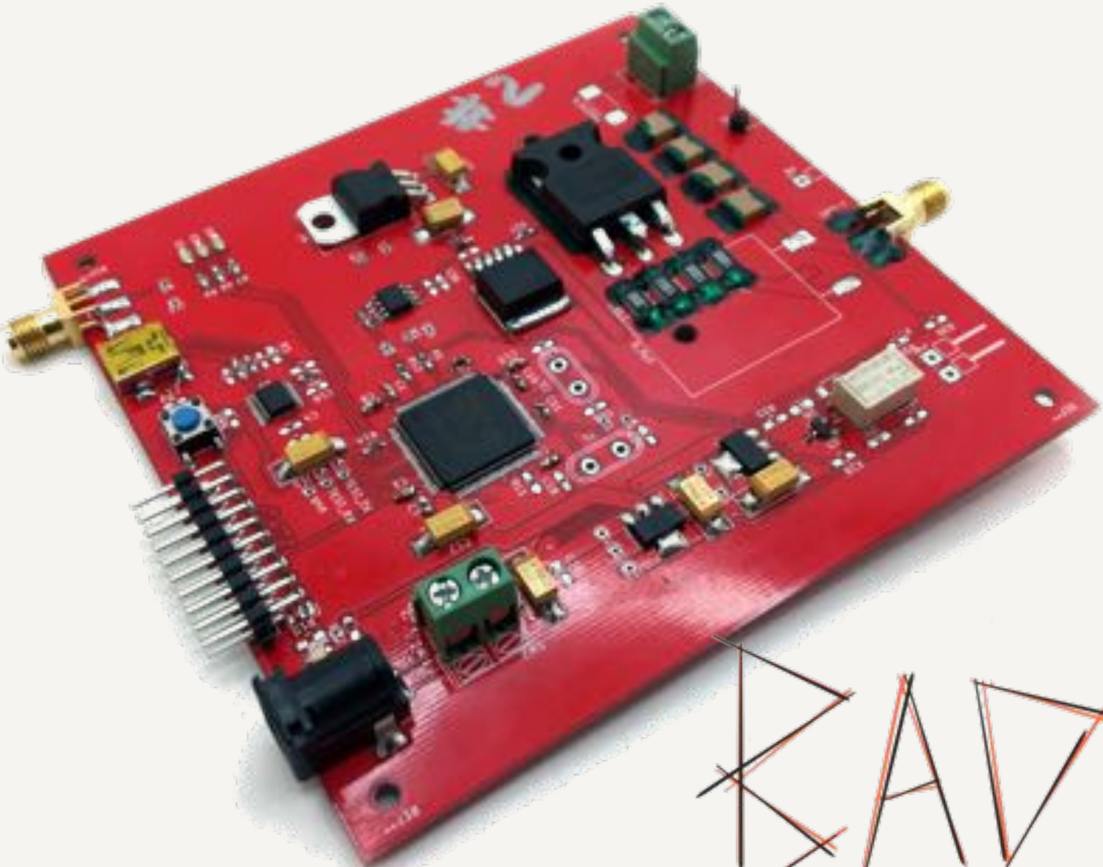

KILOBAD
(See Something SAY Something)
DALE
RS-10
100Ω 1%
MEXICO


CORNELL DUBILIER
947D271K112AEGSN
270 uF−10%+10% 1100 VDC
58 ARms @ 55 C
−45C TO 85C
658−1633−M86289
MADE IN MEXICO

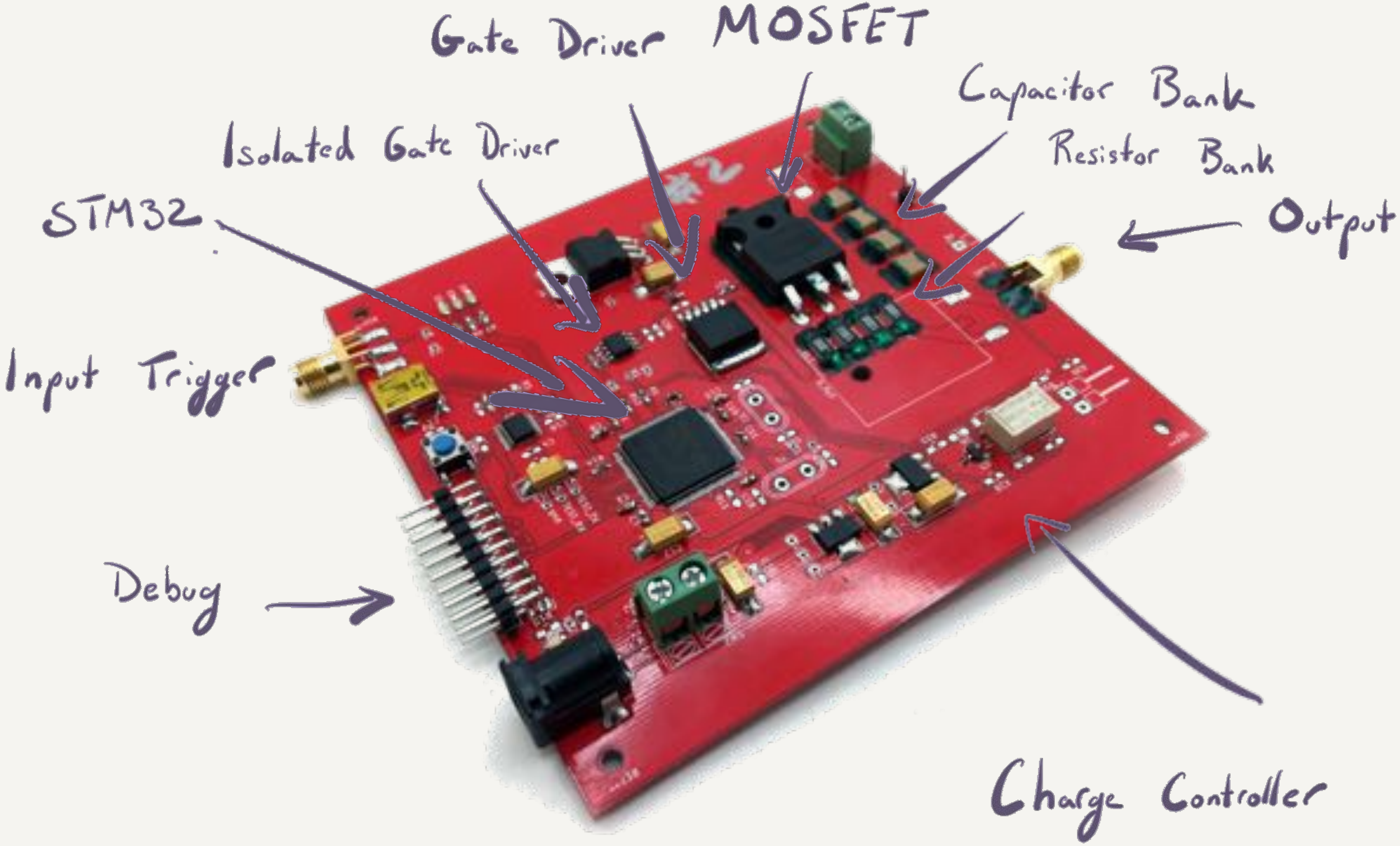
KILOBAD

BADFET

v1.0!

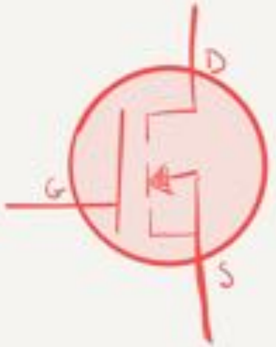


BADFET

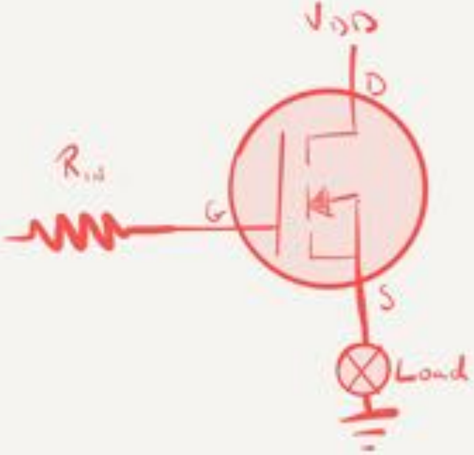

Gate Driver
MOSFET
Capacitor Bank
Isolated Gate Driver
Resistor Bank
STM32
Output
Input Trigger
Debug
Charge Controller

BADFET's relationship with Magic Smoke

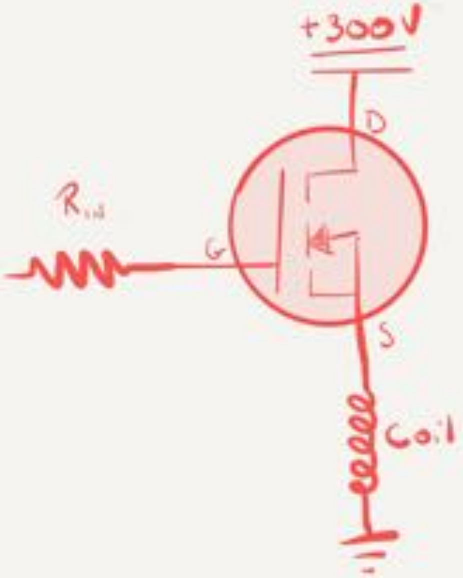
N-Channel MOSFET



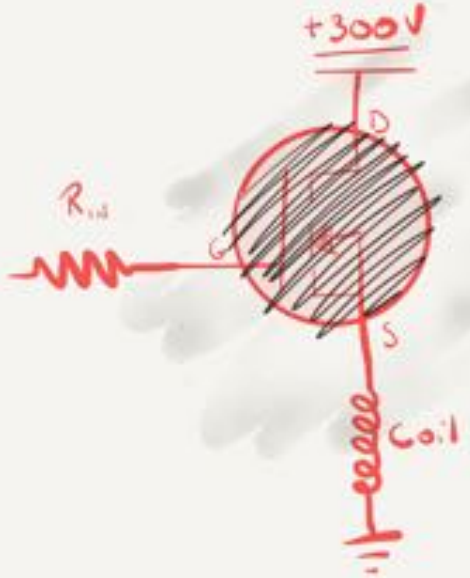
N-Channel MOSFET



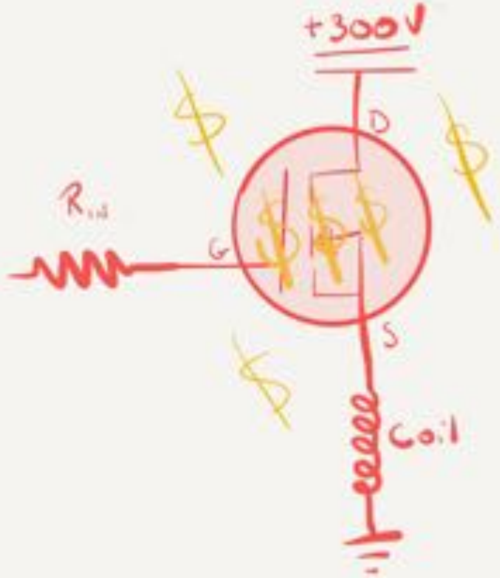
N-Channel MOSFET



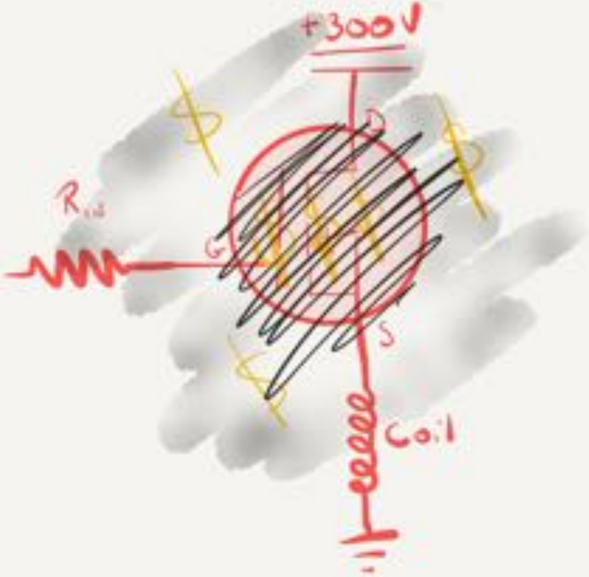
N-Channel MOSFET



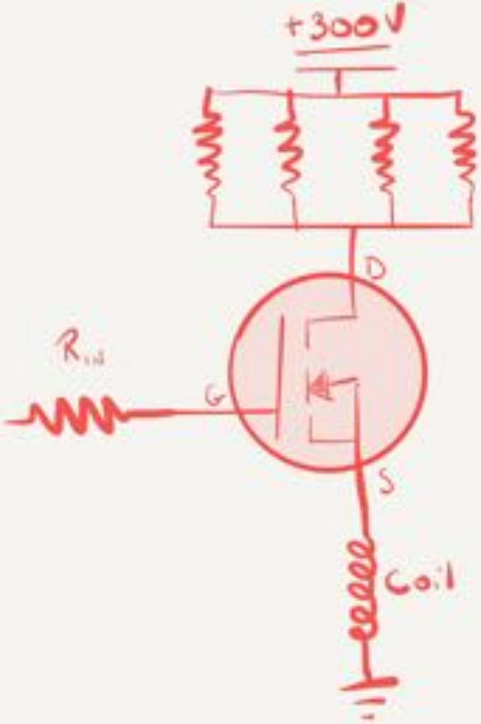
N-Channel MOSFET



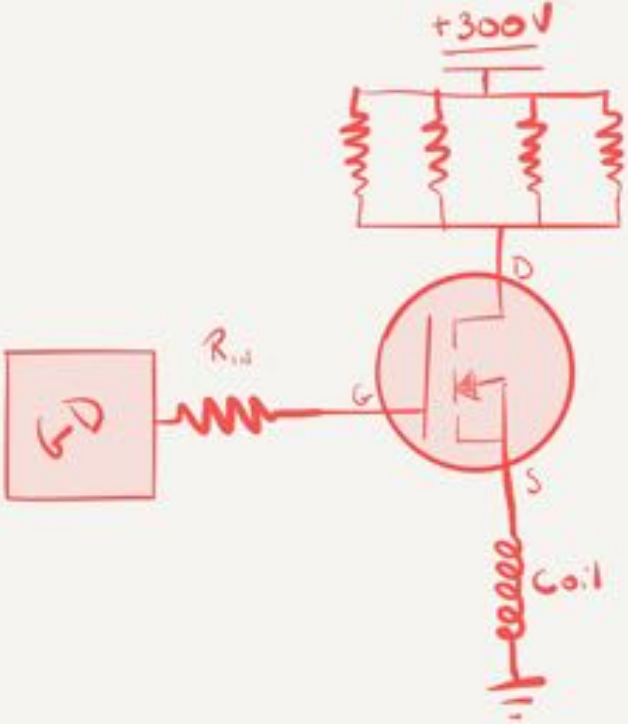
N-Channel MOSFET



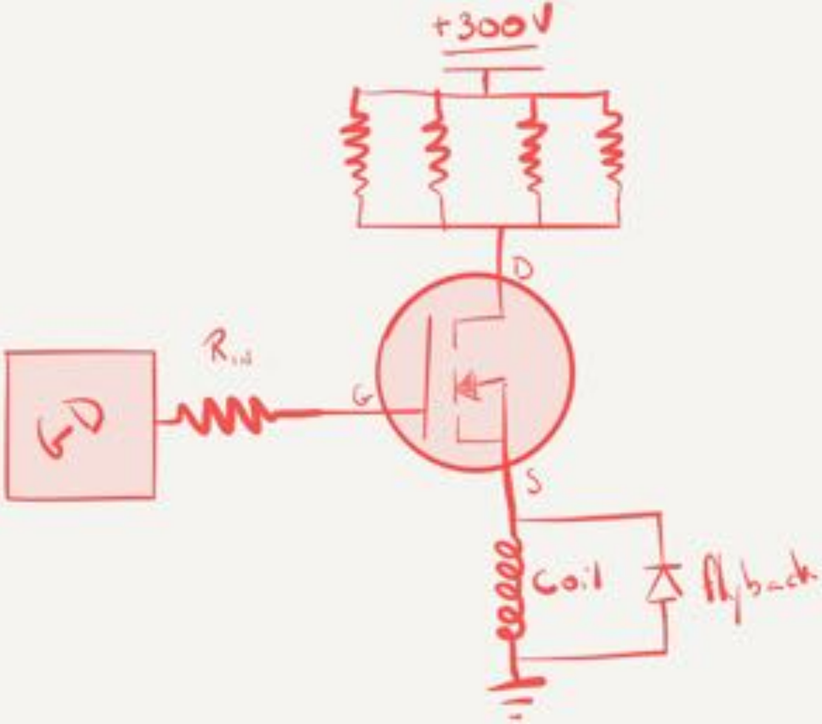
N-Channel MOSFET



N-Channel MOSFET



N-Channel MOSFET



Additional problems

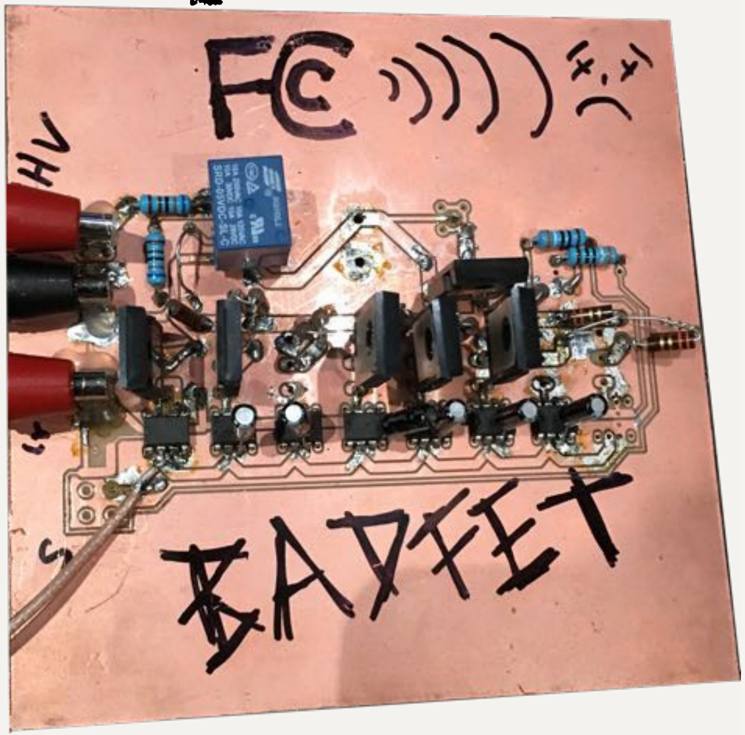
- Need intelligent board design for high speed designs, etc.

Parallel! - nope -(

$$C_M = C(1 + A_v)$$

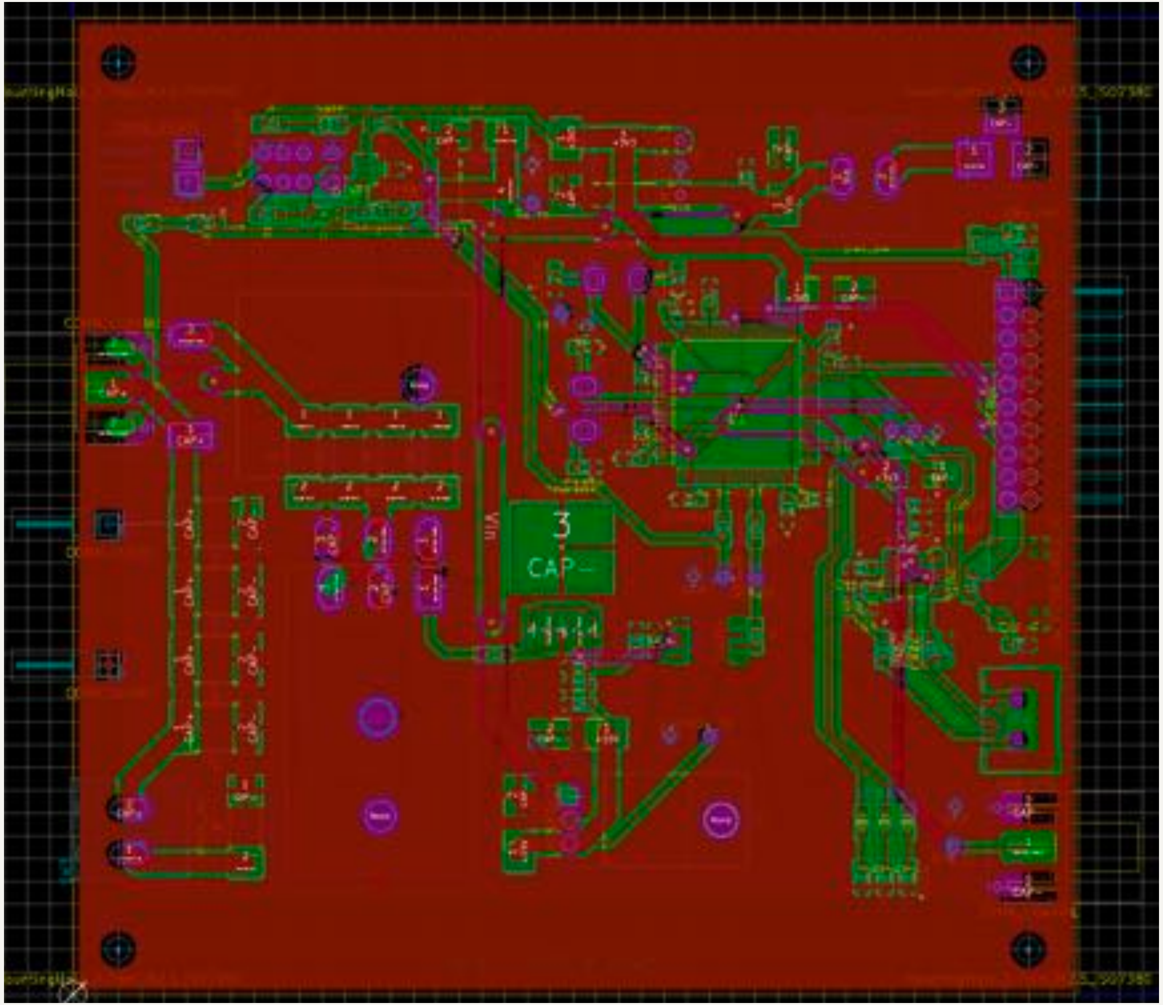
A_v = Amplifier Gain

C = Feedback Capacitance



Class D voltage-switching MOSFET power amplifier

Kazimierczuk, Marian K

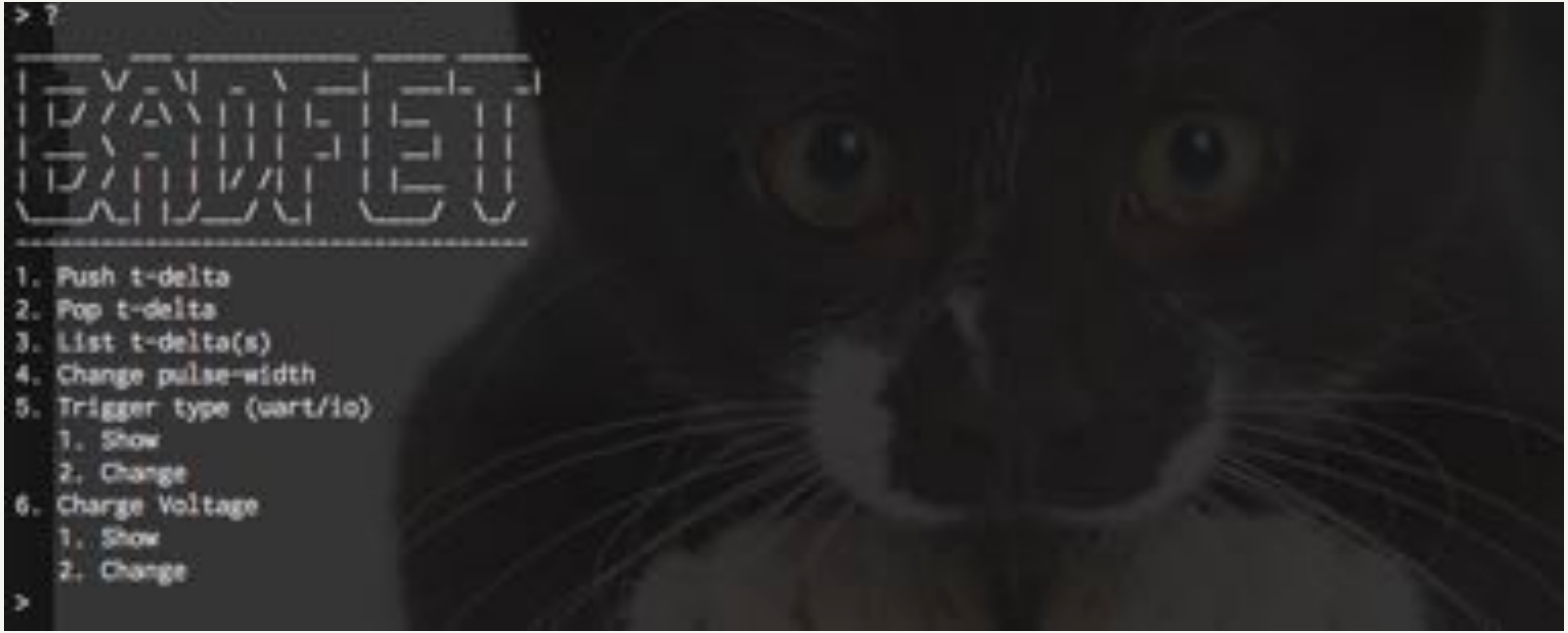

3
CAP-
Vin
CAP+
MountingHole

DANGER
HIGH
VOLTAGE
ALUNAR

Features

- Programmable + Debug (SWD)
- Scriptable
- Microsecond Pulse Time
- 350 Voltage (Current Configuration)
- 10 Microsecond Recharge Time (Current Configuration)
- ~~Child Friendly~~
- ~~Adult Friendly~~
- ~~Safe~~

Please just don't use it

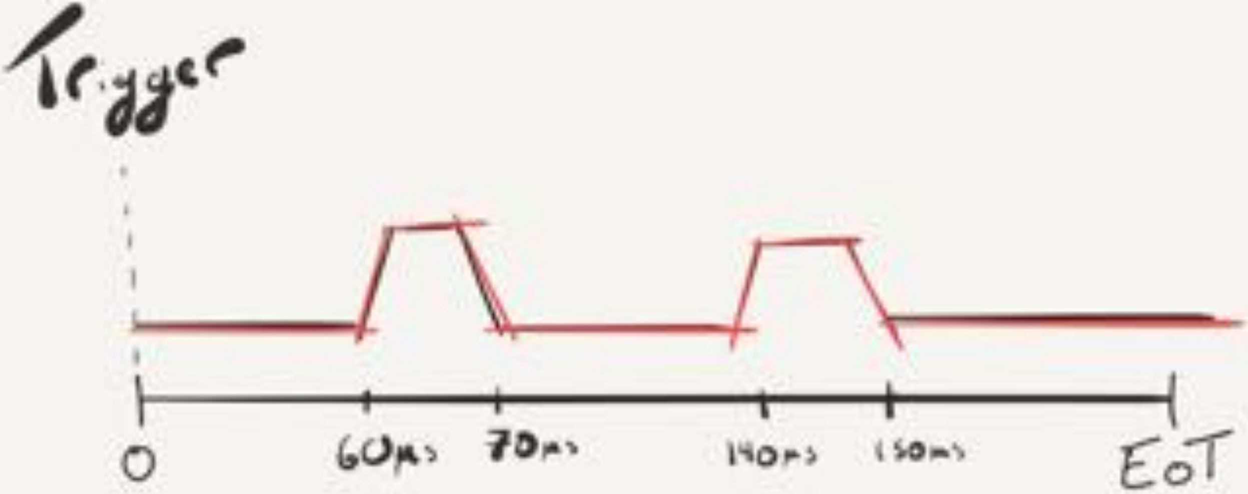


```
> ?

1. Push t-delta
2. Pop t-delta
3. List t-delta(s)
4. Change pulse-width
5. Trigger type (uart/io)
   1. Show
   2. Change
6. Charge Voltage
   1. Show
   2. Change
>
```

Push 140

Push 60

Pulse 10



Magnetic Microprobe Design for EM Fault Attack

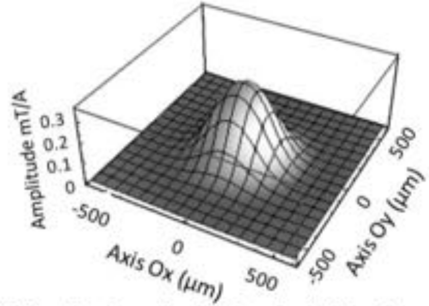


Fig. 2. B_z spatial distribution calculated at the height $d = a = 200$ µm.

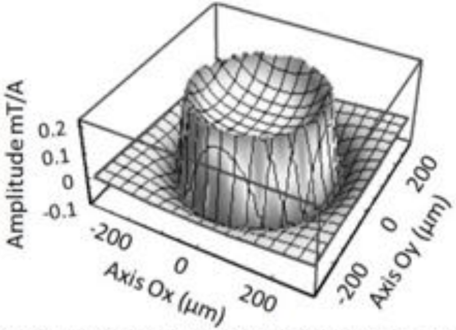
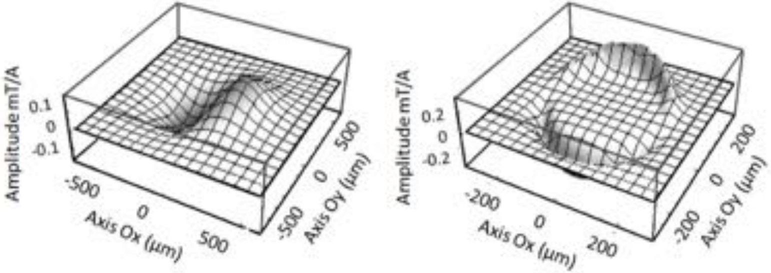
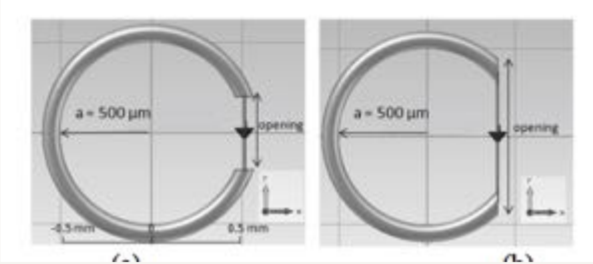
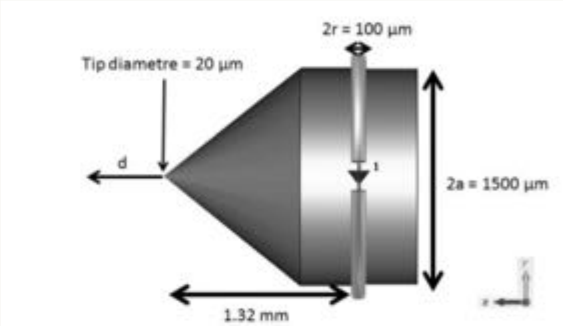


Fig. 3. B_z spatial distribution calculated at the height $d = a/10 = 20$ µm.

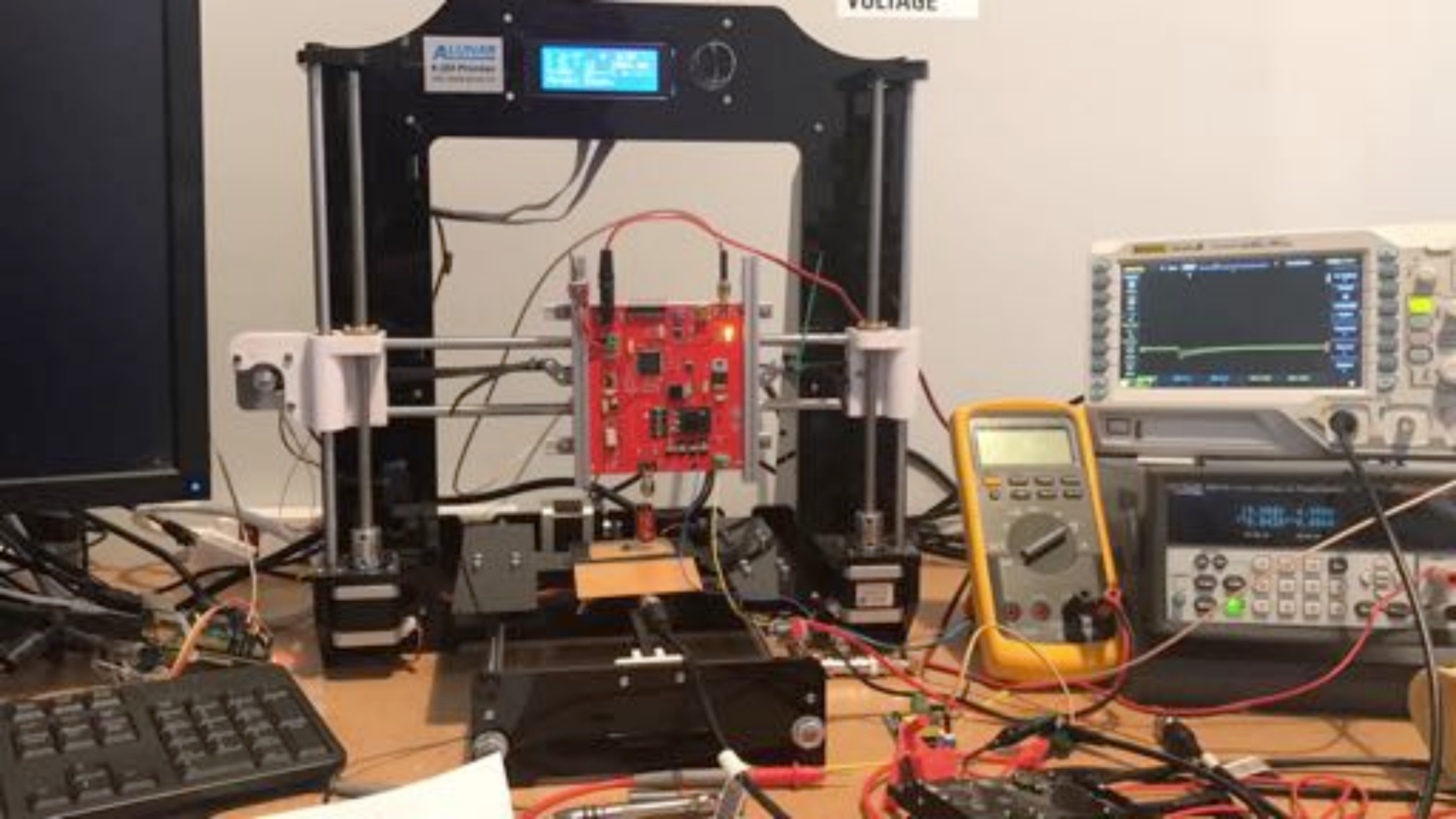






R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau

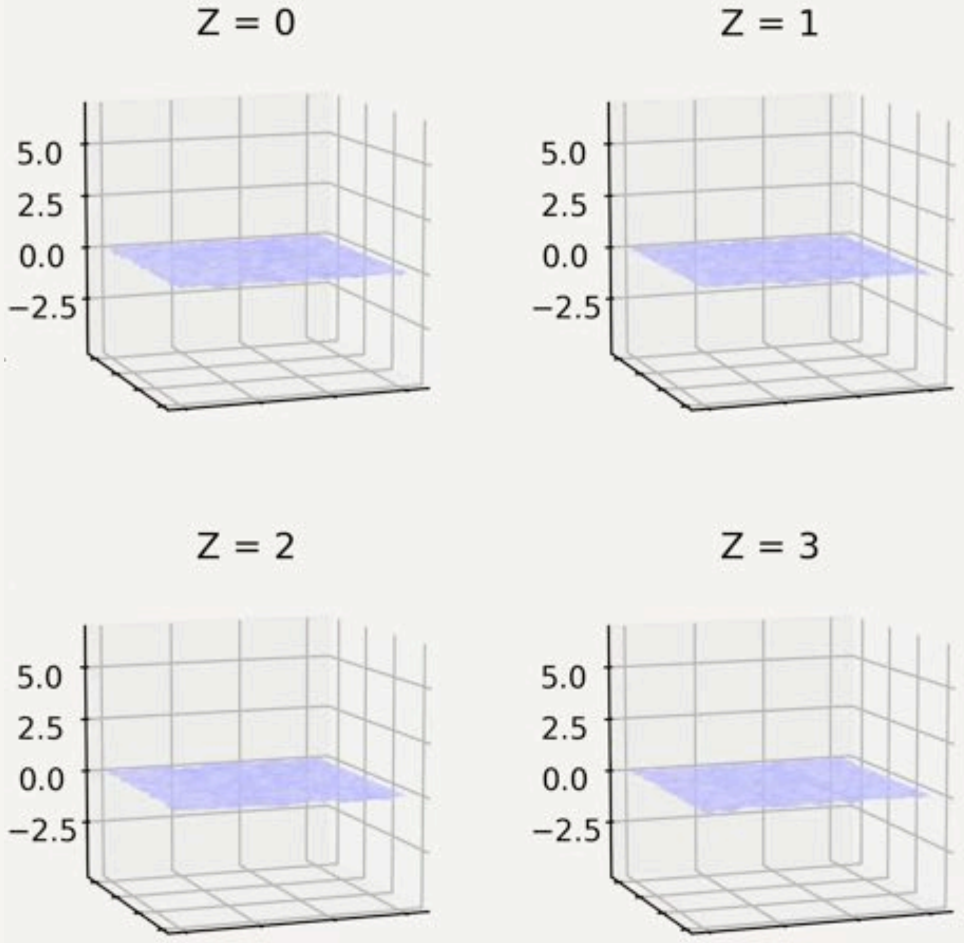
Automate!

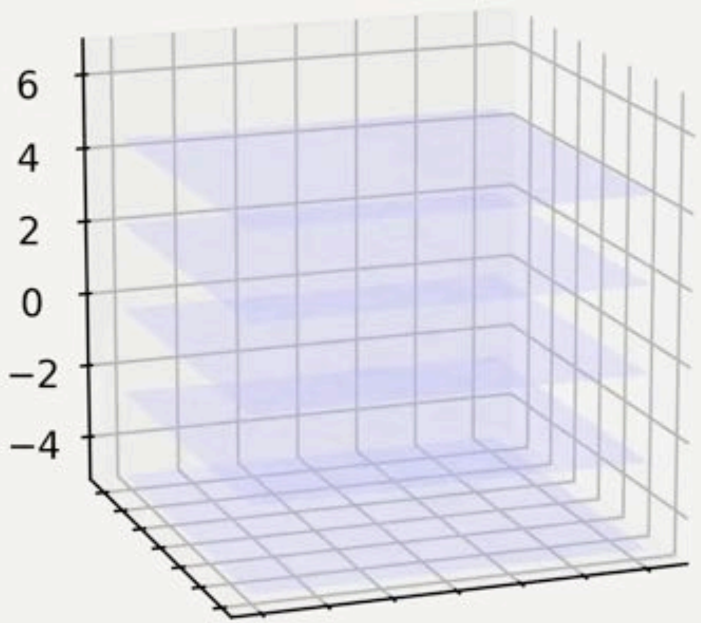

VOLTAGE

The Following Slides are videos

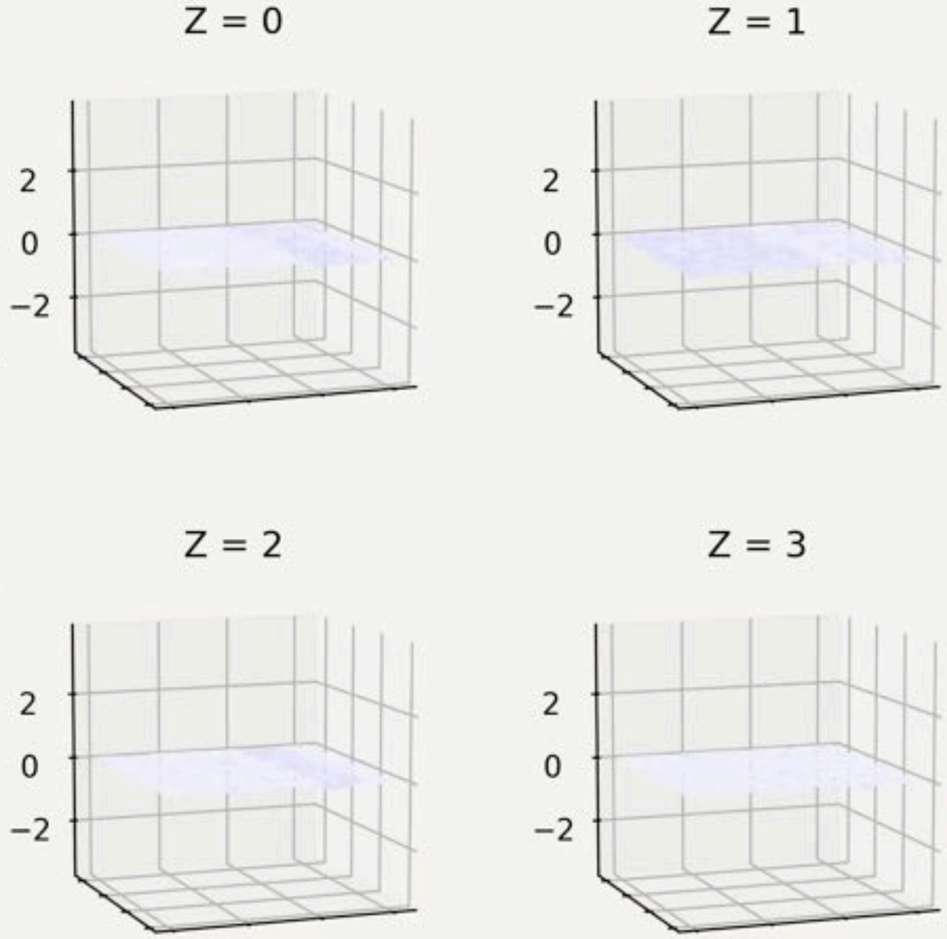
Please visit the gitlab /docs to view these

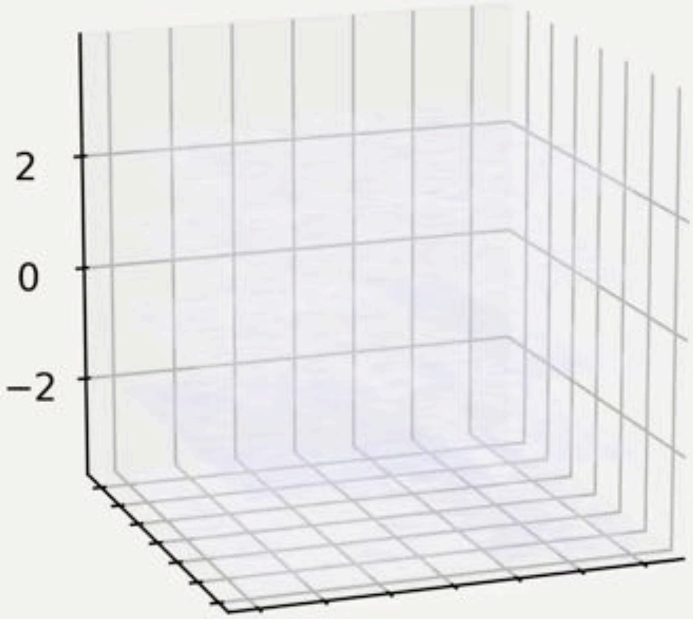
Square Probe



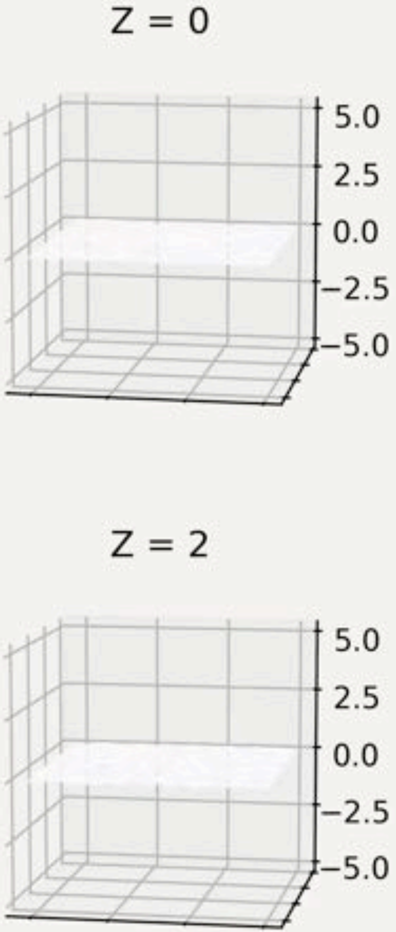


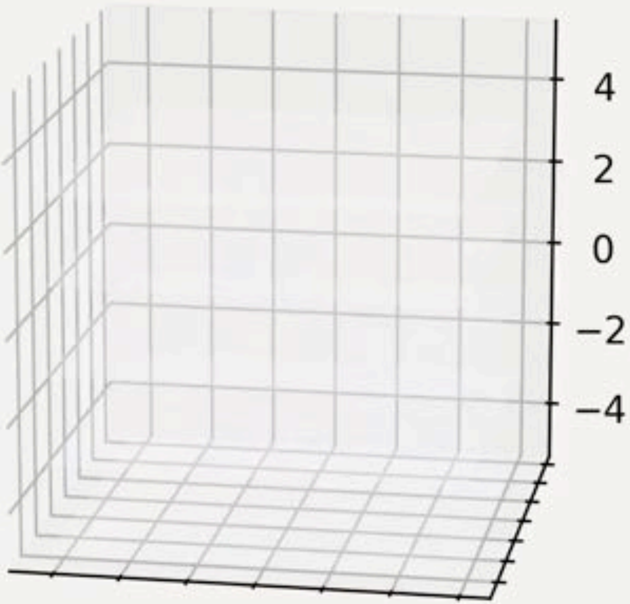
Core-less Coil

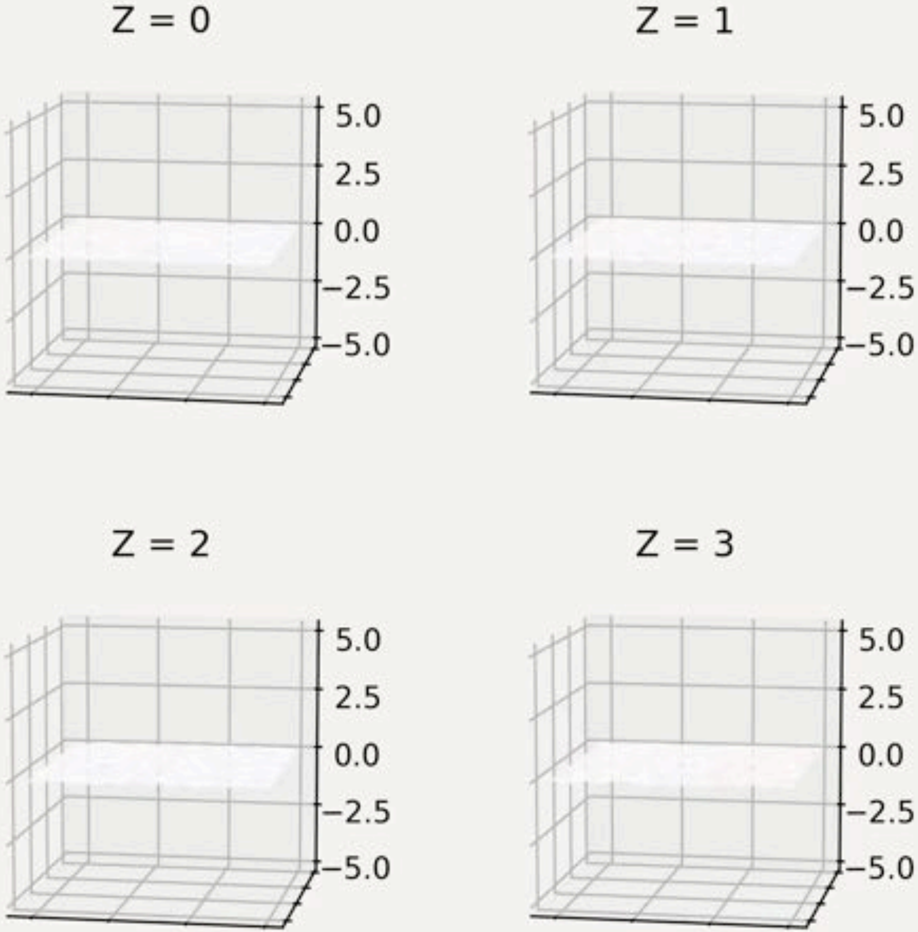




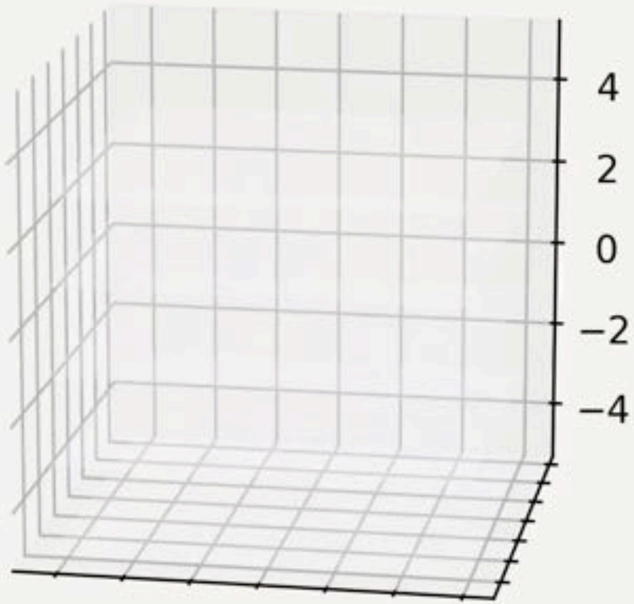
Sharpened Core

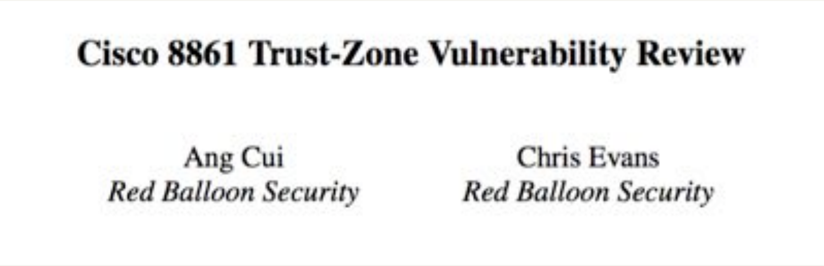





Z = 0
5.0
2.5
0.0
−2.5
−5.0
Z = 1
5.0
2.5
0.0
−2.5
−5.0
Z = 2
5.0
2.5
0.0
−2.5
−5.0
Z = 3
5.0
2.5
0.0
−2.5
−5.0

Flat Core

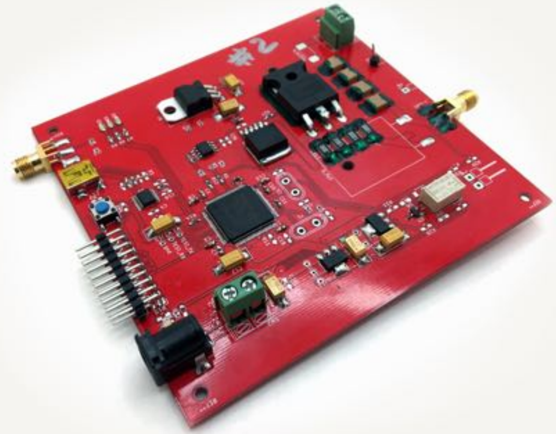

4
2
0
−2
−4



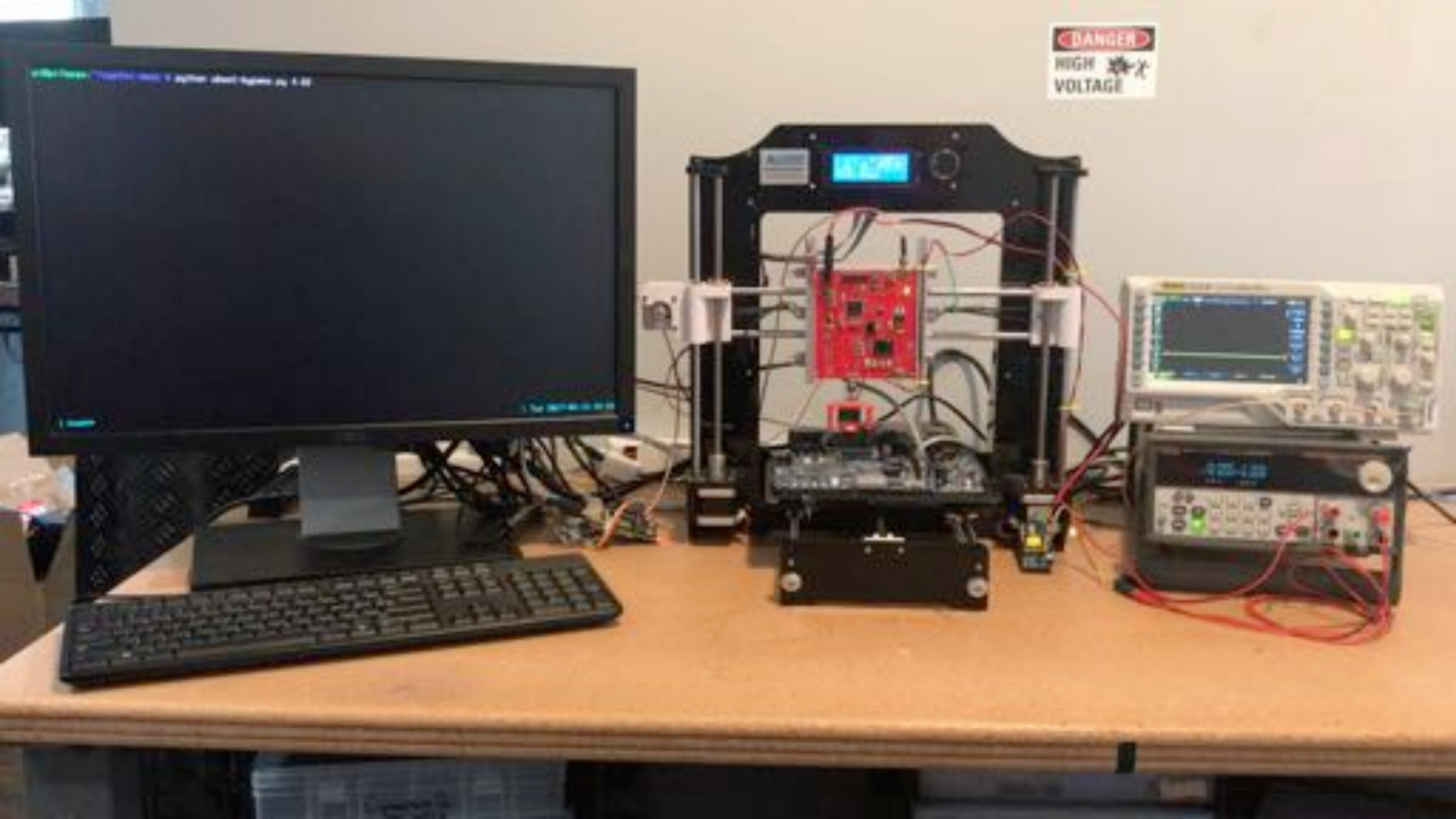
Cisco 8861 Trust-Zone Vulnerability Review

Ang Cui
Red Balloon Security

Chris Evans
Red Balloon Security



Let's Do This.


DANGER
HIGH
VOLTAGE

{R|A}@redballoonsecurity.com

www.github.com/RedBalloonShenanigans/BADFET

Safety

At LEAST Class 1 Insulating gloves

7500 VAC 15,000 VDC

MAKE SURE THEY FIT

- Eye Protection
- Fire Extinguisher
- Common Sense