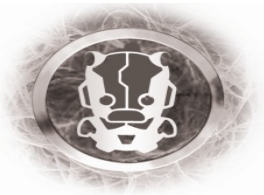
IOActive
Hardware | Software | Wetware
SECURITY SERVICES

No MAS:

(misadventures in high security lock design)

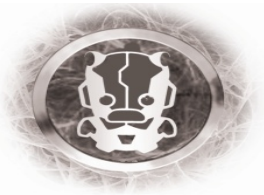
Mike Davis



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Introduction

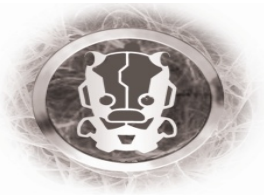
- I Hack stuff for IOActive
  - Weird embedded stuff
- Amateur lock picker
  - I'm not very good
- Pretty good understanding of how the pixies flow
- I'm not interested in hacking one thing, I want to hack all of the things.



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Todays plan

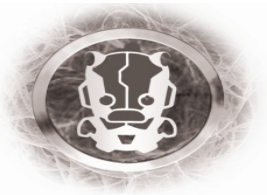
- We’re going to (try to) think like a lock vendor
- Quick look at the evolution of ”High Security” lock design
  - and a look at the seemingly pervasive flaw that these design requirements and decisions lead to.
- Look at how the same flaw keeps expressing itself.
- Discuss responsible cdisclosure a bit



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

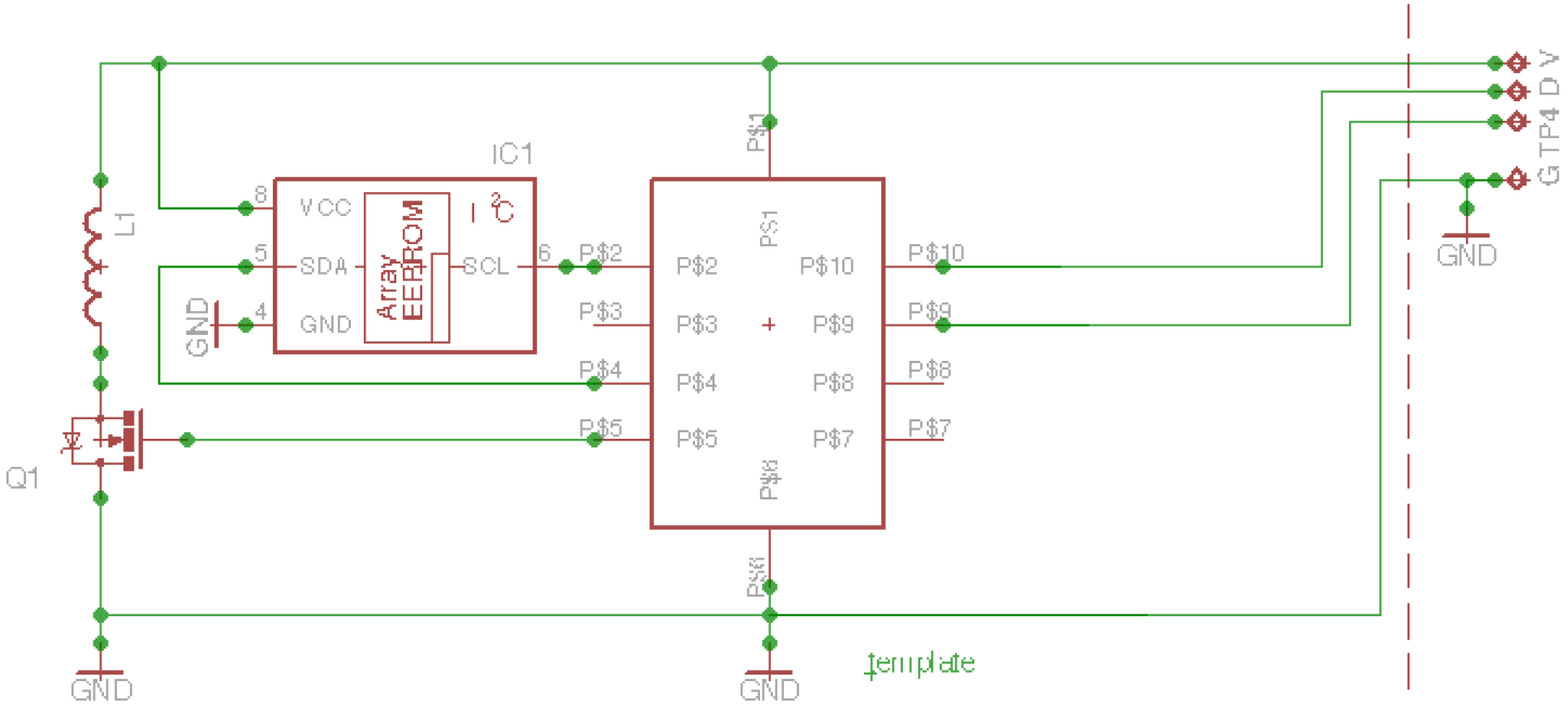
Design Requirements!

- Lock
- Electronic
- Audit trail
- Long lived power solution
  - Replacing batteries isn't really an option.
- Permissions systems not entirely related to physical possession of the key
- Drop-in replacement for the traditional mechanisms.
  - Mmm physical constraints…
- More secure-er then traditional (mechanical) designs!
  - Because… electronic!



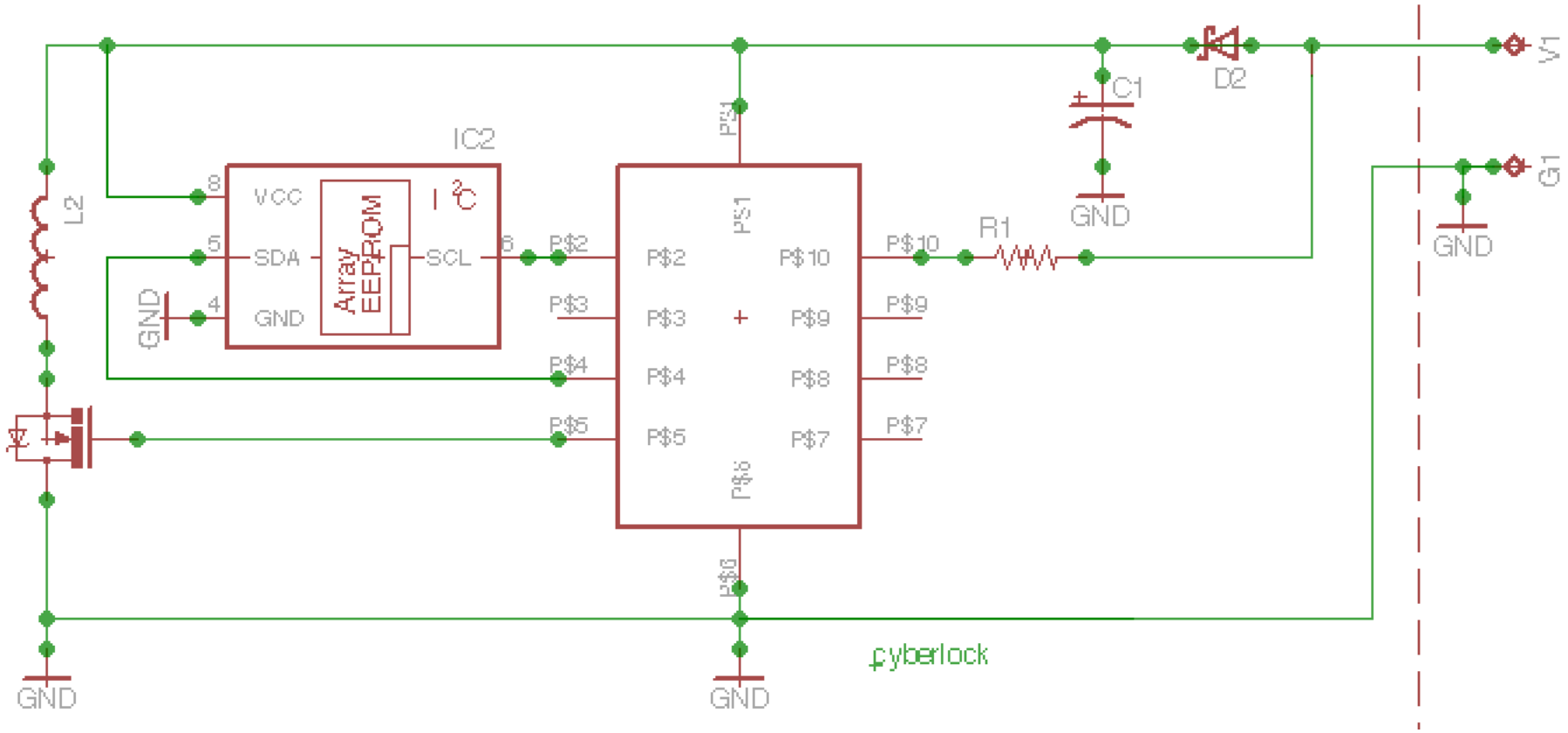
IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Lock Design



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Lock Design + Security



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

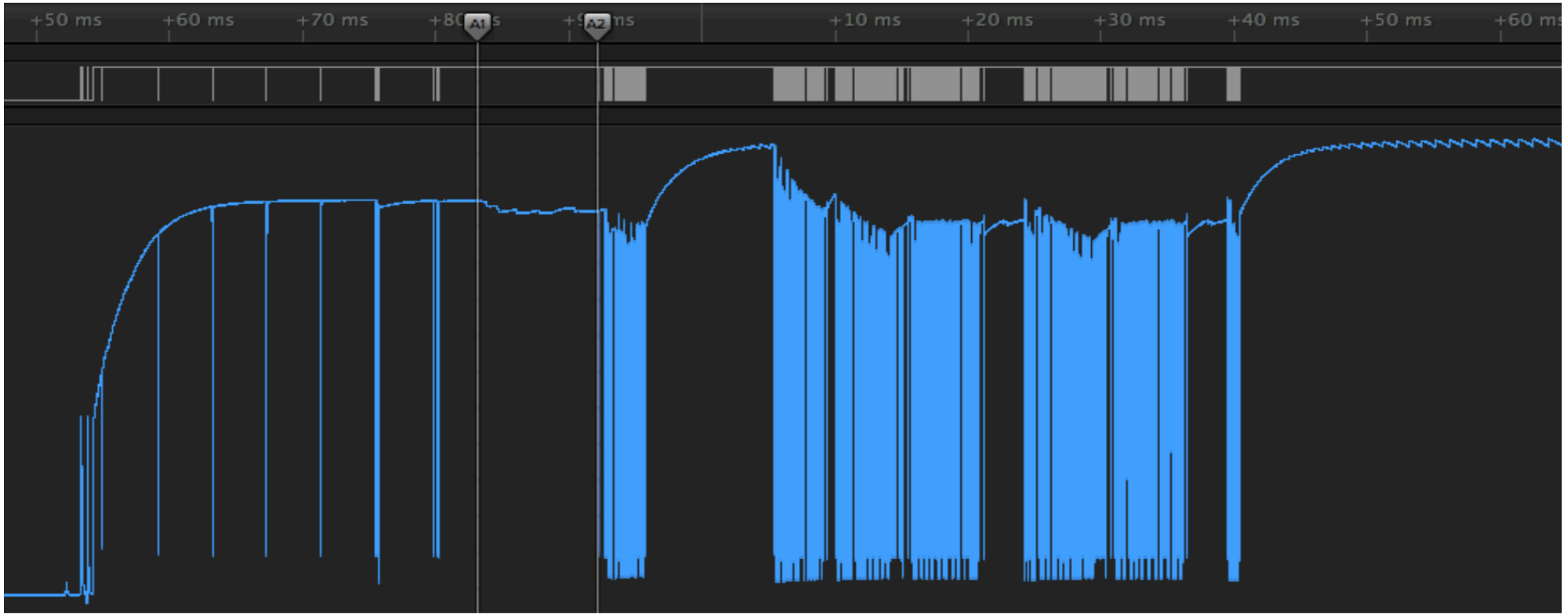
Cyberlock

"As the CyberLock is directly powered through the communications port, it appears that an SPA (power analysis) attack may succeed against a CyberLock in-situ, as the lock leaks a significant power side-channel to any potential "key" as the processor slowly clocks the key across an I2C bus at the Fcpu/4 bps. However, this approach seems somewhat overboard given the existing issues."

-IOActive Cyberlock Advistory

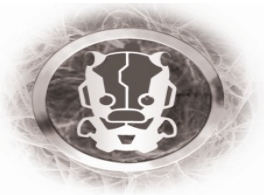
IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Cyberlock – power hungry



Some lessons learned

- Pluses
  - Drop in replacements for classical design
  - Locks don’t need batteries
  - Audit trails and permission systems
- Minuses
  - Bullshit crypto
  - Reliant on external power
  - Could not be fixed



A Quick Tangent

JONES DAY

555 CALIFORNIA STREET • 26TH FLOOR • SAN FRANCISCO, CALIFORNIA 94104.1500
TELEPHONE: +1.415.626.3939 • FACSIMILE: +1.415.875.5700

Direct Number: (415) 875-5850
jratkin@jonesday.com

JP020437 April 29, 2015

VIA EMAIL AND OVERNIGHT MAIL

Mike Davis

Re: Intellectual Property

Dear Mike:

As discussed today, Jones Day is outside counsel for , Inc. In that regard, I write on behalf of in response to IOActive's recent communication regarding "the ystem," IOActive's claim that is has "discovered a number of serious vulnerabilities," and IOActive's plans for a "public advisory on April 30 where [it] will release [its] findings to the general public."

Specifically, requests that IOActive refrain from the public reporting of any security vulnerabilities relating to the ystem or products until ; has had an opportunity to identify these supposed security vulnerabilities, and, if appropriate, take any necessary remedial steps.

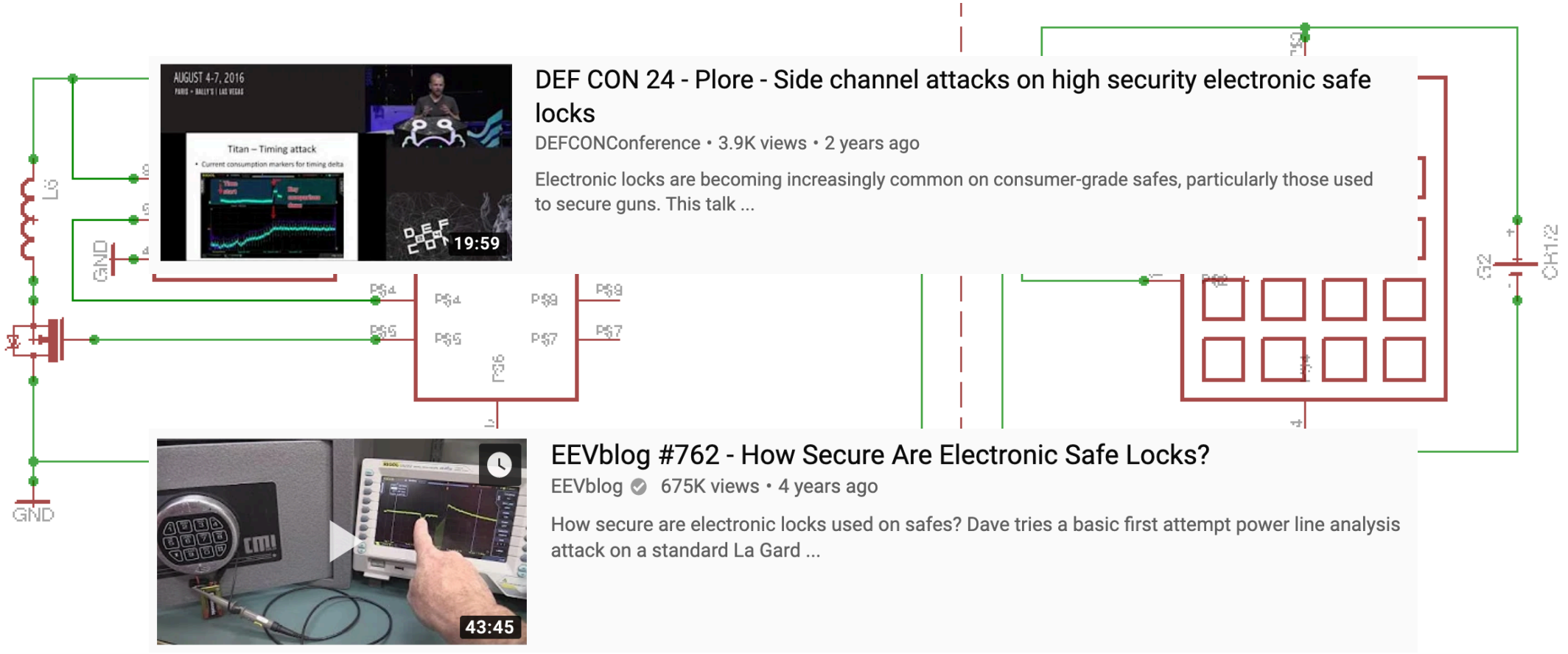
I note that your correspondence to states that IOActive prefers to "release vulnerabilities (security flaws) responsibly by sharing them with prior to a public advisory." Yet, when I reached out to discuss this matter with you today, you declined to share any information about your activities concerning the products, what products IOActive allegedly researched, the nature of the supposed vulnerabilities, or how you uncovered such vulnerabilities. I understand your reluctance may have been based on a need to verify our relationship to and hopefully this letter satisfies those concerns.

Of course, as you know, the public reporting of security vulnerabilities can have significant consequences. also takes the protection and enforcement of its intellectual property rights seriously and, prior to any public reporting, wants to ensure that there has been no violation of those rights, including 's license agreements or other intellectual property laws such as the anticircumvention provision of the Digital Millennium Copyright Act. Presumably, IOActive is also aligned with ensuring responsible disclosure and compliance with the laws.

SVI-700165417v1

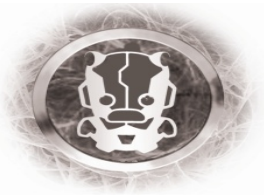
ALKHOBAR • AMSTERDAM • ATLANTA • BEIJING • BOSTON • BRUSSELS • CHICAGO • CLEVELAND • COLUMBUS • DALLAS
DUBAI • DUSSELDORF • FRANKFURT • HONG KONG • HOUSTON • IRVINE • JEDDAH • LONDON • LOS ANGELES • MADRID
MEXICO CITY • MIAMI • MILAN • MOSCOW • MUNICH • NEW YORK • PARIS • PITTSBURGH • RIYADH • SAN DIEGO
SAN FRANCISCO • SÃO PAULO • SHANGHAI • SILICON VALLEY • SINGAPORE • SYDNEY • TAIPEI • TOKYO • WASHINGTON

Yet Another Design

- 

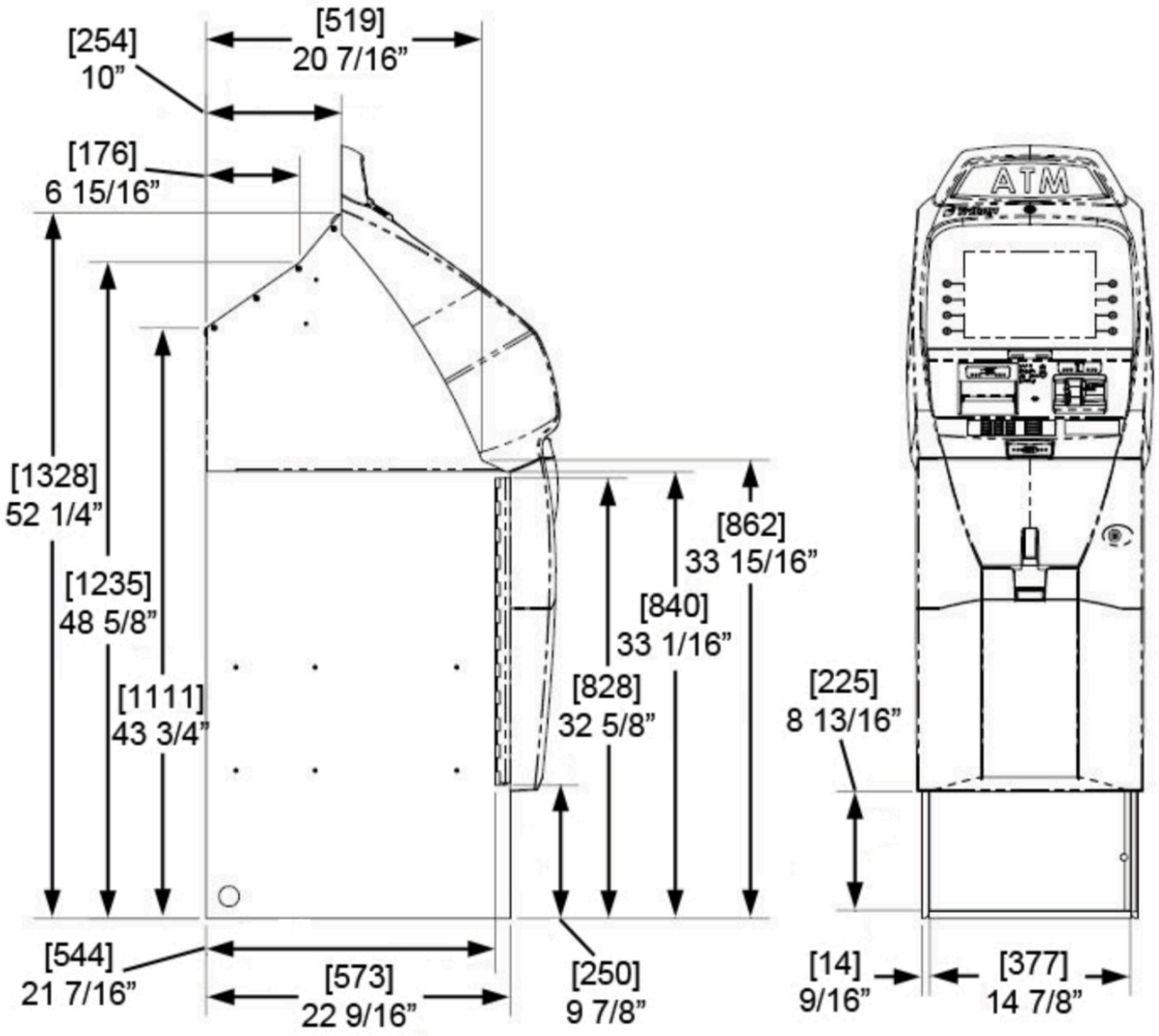
Some lessons learned

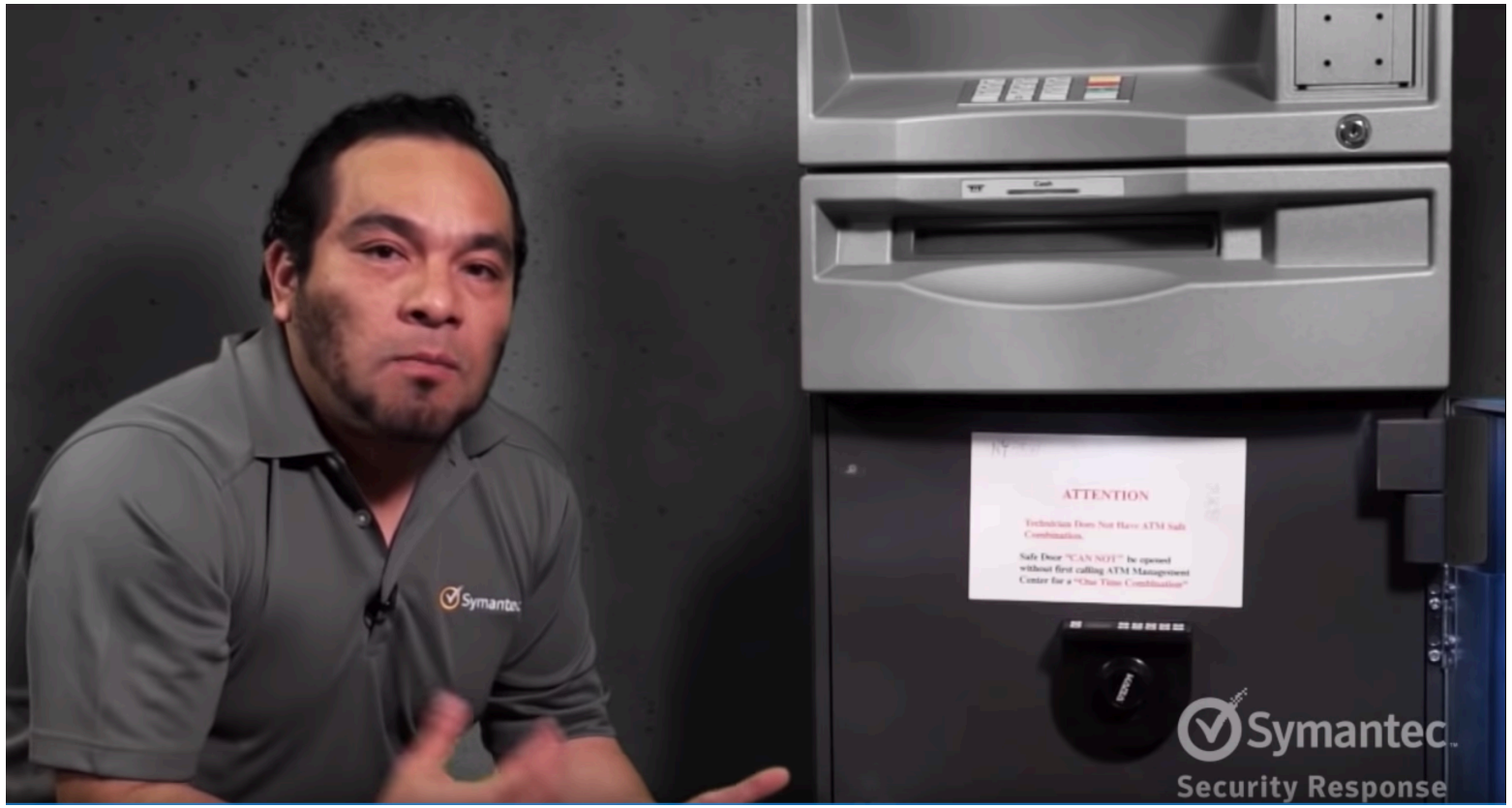
- Pluses
  - Cheap
  - Battery failure doesn't kill safe
- Minuses
  - Still reliant on external power
  - Introduction of secondary side-channels (beep)



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Another quick Tangent



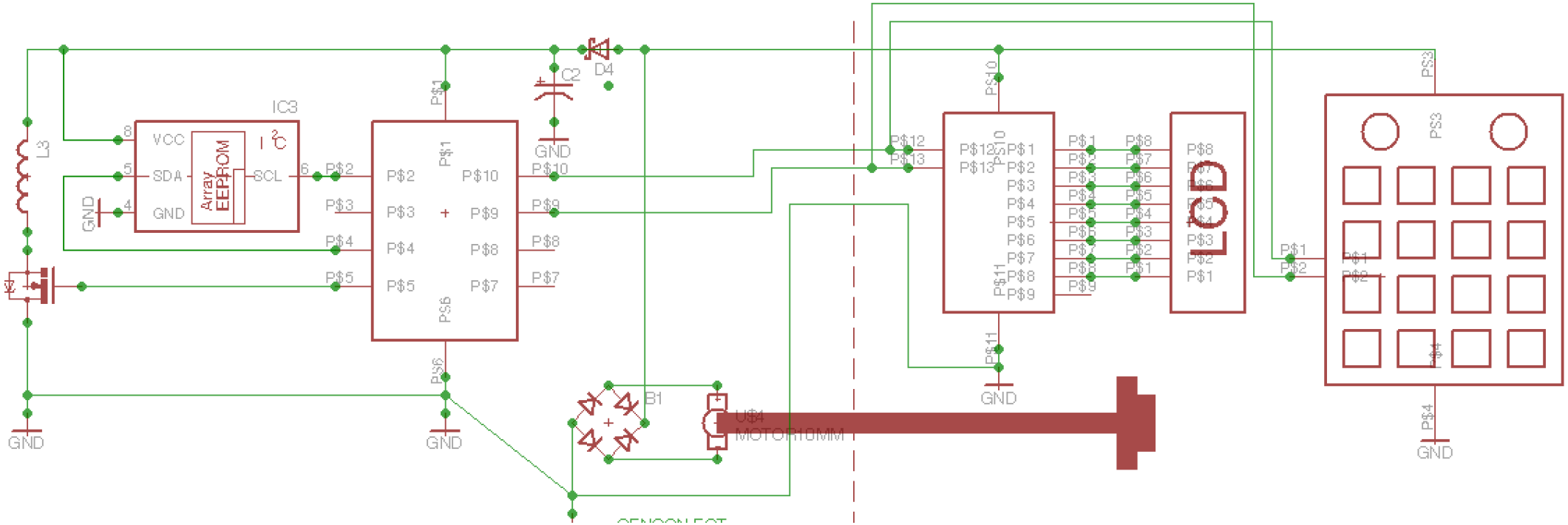


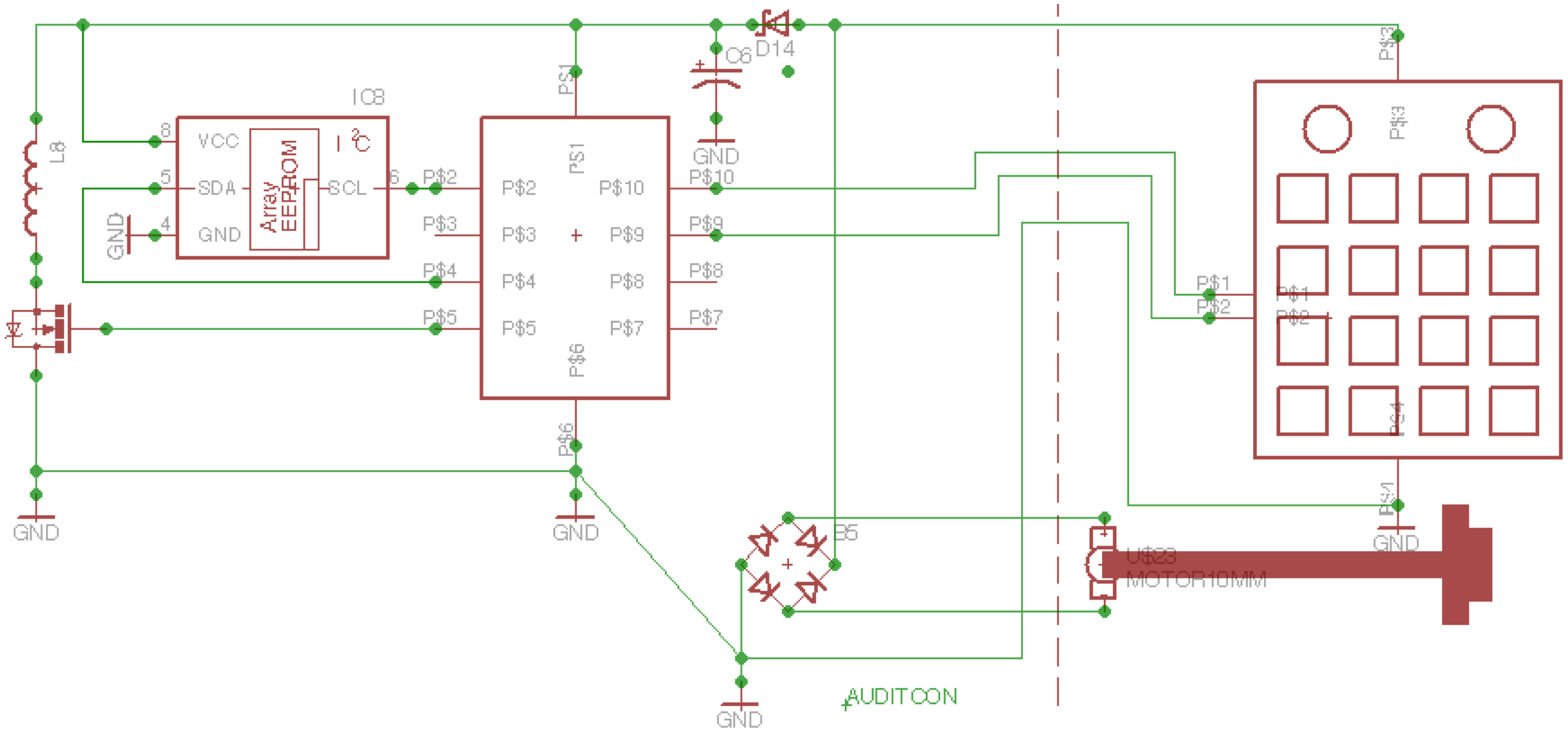
“So, here’s where the money is stored in an ATM, as you can see it's protected with this heavy door; which in the old days criminals were trying to break into this, so by now they are more sophisticated” – Guy I owe a beer to.

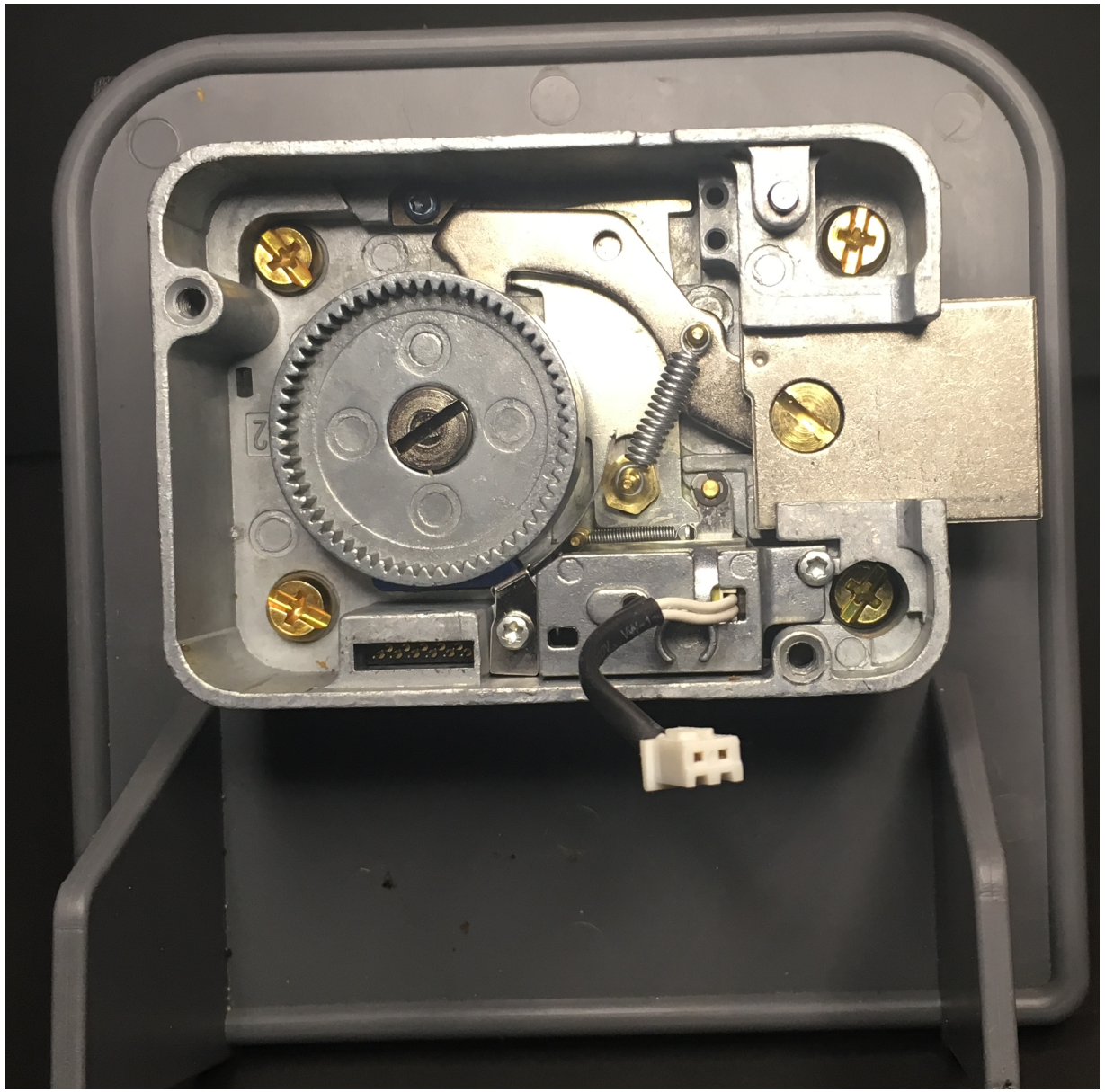

*
#
1 2 3 4 5
6 7 8 9 0
KABA


1 2
3 4 5
KABA
6 7
8 9 0
*
#

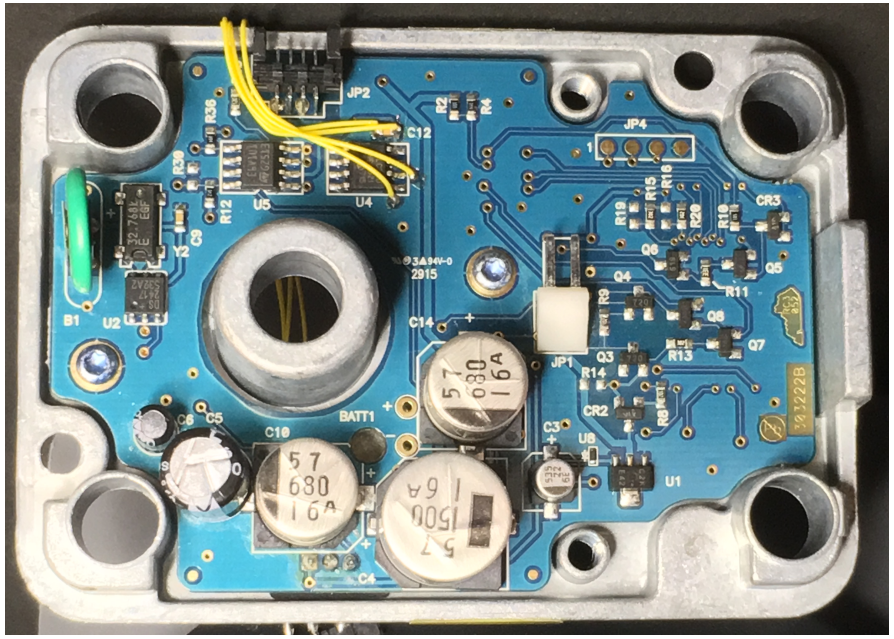

KABA


IC3
VCC
SDA
GND
SCL
Array EEPROM
L3
GND
C2
D4
B1
U$4
MOTOR10MM
LCD
PS1
PS2
PS3
PS4
PS5
PS6
PS10
PS11
P$1
P$2
P$3
P$4
P$5
P$6
P$7
P$8
P$9
P$10
P$11
P$12
P$13

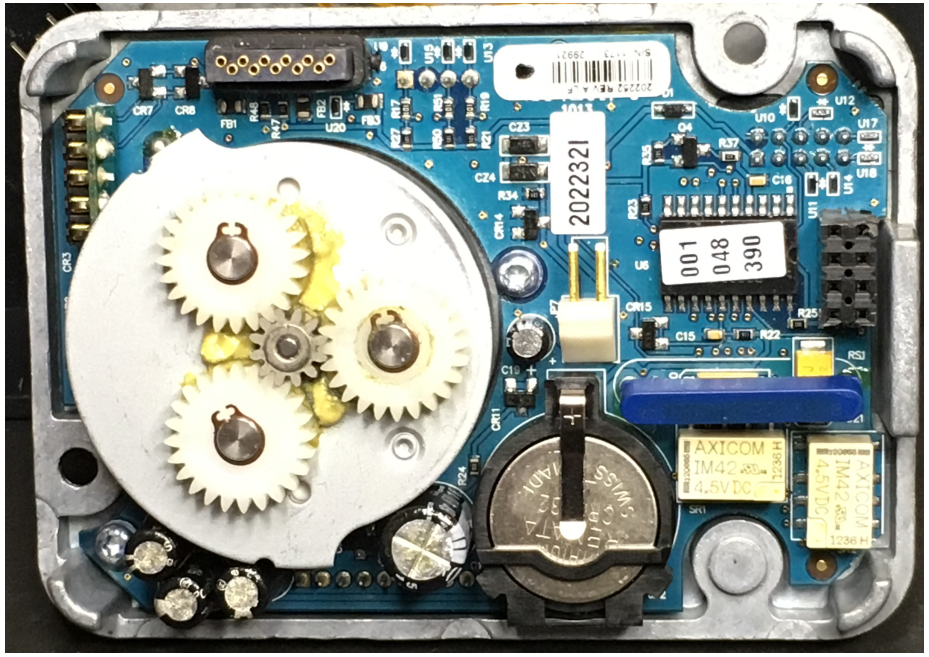

IC8
VCC
SDA
GND
SCL
Array EEPROM
I²C
GND
L8
PS1
P$1
P$2
P$3
P$4
P$5
P$6
P$7
P$8
P$9
P$10
C6
D14
B5
U$23
MOTOR10MM
AUDITOON
GND



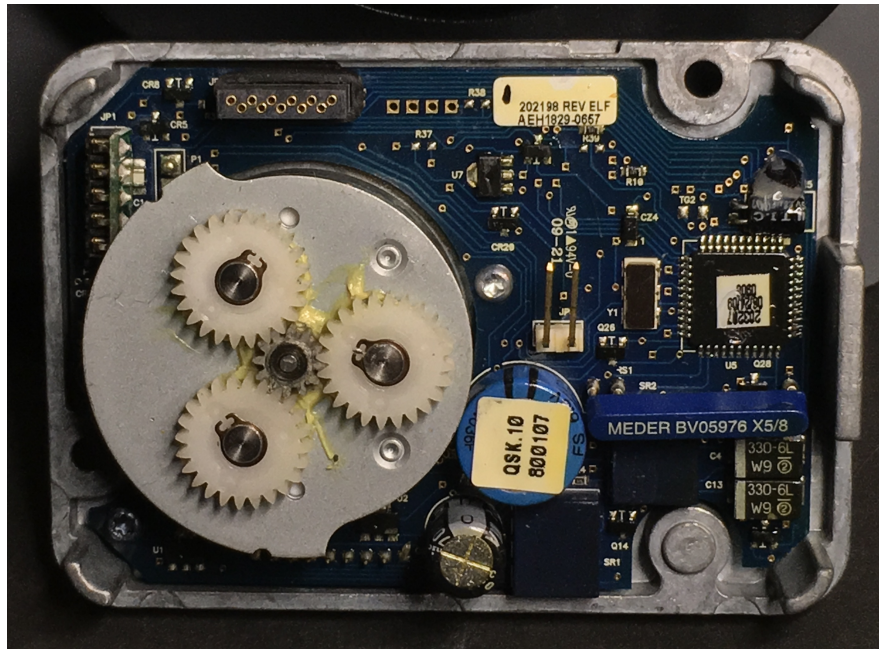
IOActive
Hardware | Software | Wetware
SECURITY SERVICES



AuditCon



Gen2



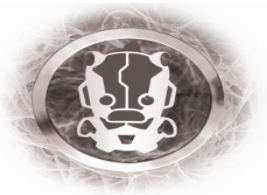
S2000

”Encrypted”

The combinations, ATM, bank and master, are typically stored in encrypted form as an added security factor; the form of encryption is not critical. The preferred encryption is to distribute the bits of a binary representation of the combination in various locations of a memory and filling the unoccupied locations in the memory with random binary bits to disguise the combination. Decryption involves removal of the random binary bits and reassemblage of the remaining bits representing combination. Other encryption/decryption schemes may be used in lieu of the preferred scheme if desired.

- Patent US5488660A

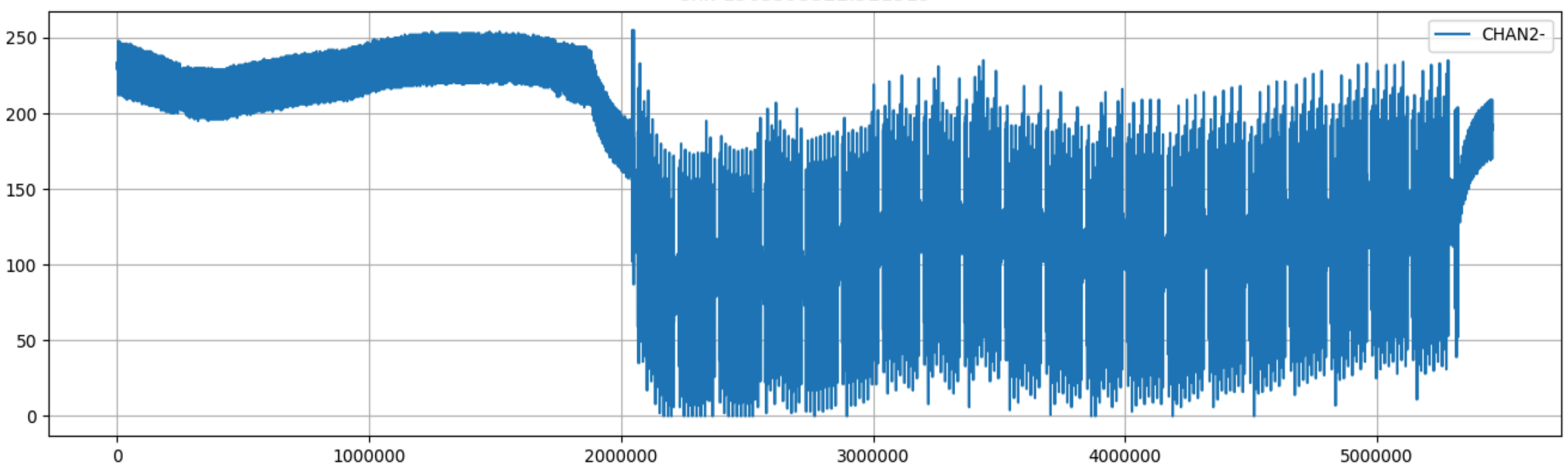
- There is no cryptography used, there is just no room for it
- The Locks load their personality on every single boot before accepting combinations
- Every lock is identical with the exception of their EEPROM contents
- Each type of lock works a bit differently



What exactly is encrypted?

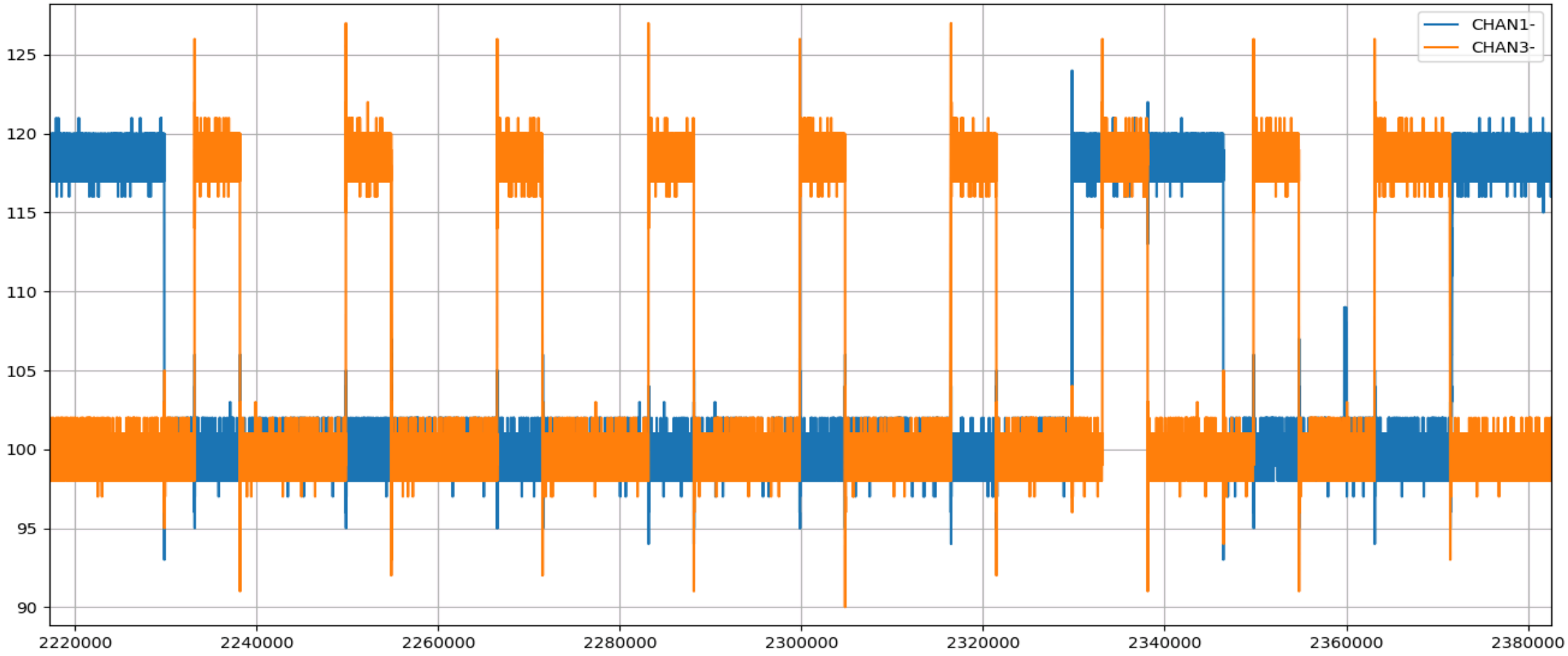
```
Shelving Mode
000000d0: 0000 0087 e006 f006 0000 b105 3103 006a  ............1..j
00000200: 0002 9161 7250 2550 aa55 aa55 aa55 aa55  ...arP%P.U.U.U.U
00000210: 493f a776 0000 0033 44c2 5100 0050 3177  I?.v...3D.Q..P1w
00000220: 4aef a371 0000 003d e841 5000 0058 33ff  J..q...=.AP..X3.
00000230: ffff ffff ffff ffff ffff ffff ffff ffff  ................

Bank Mode
000000d0: 0500 2093 7012 0000 0013 5716 9109 102c  .. .p.....W....,
00000200: 0005 6544 3650 2550 aa55 aa55 aa55 aa55  ..eD6P%P.U.U.U.U
00000210: 4f0b 3c18 0000 0090 c9ea 4800 0002 02ba  F.<.......H.....
00000220: ffff ffff ffff ffff ffff ffff ffff ff88  ................
00000230: 48ff ffff ffff ffff ffff ffff ffff ff74  H..............t
```



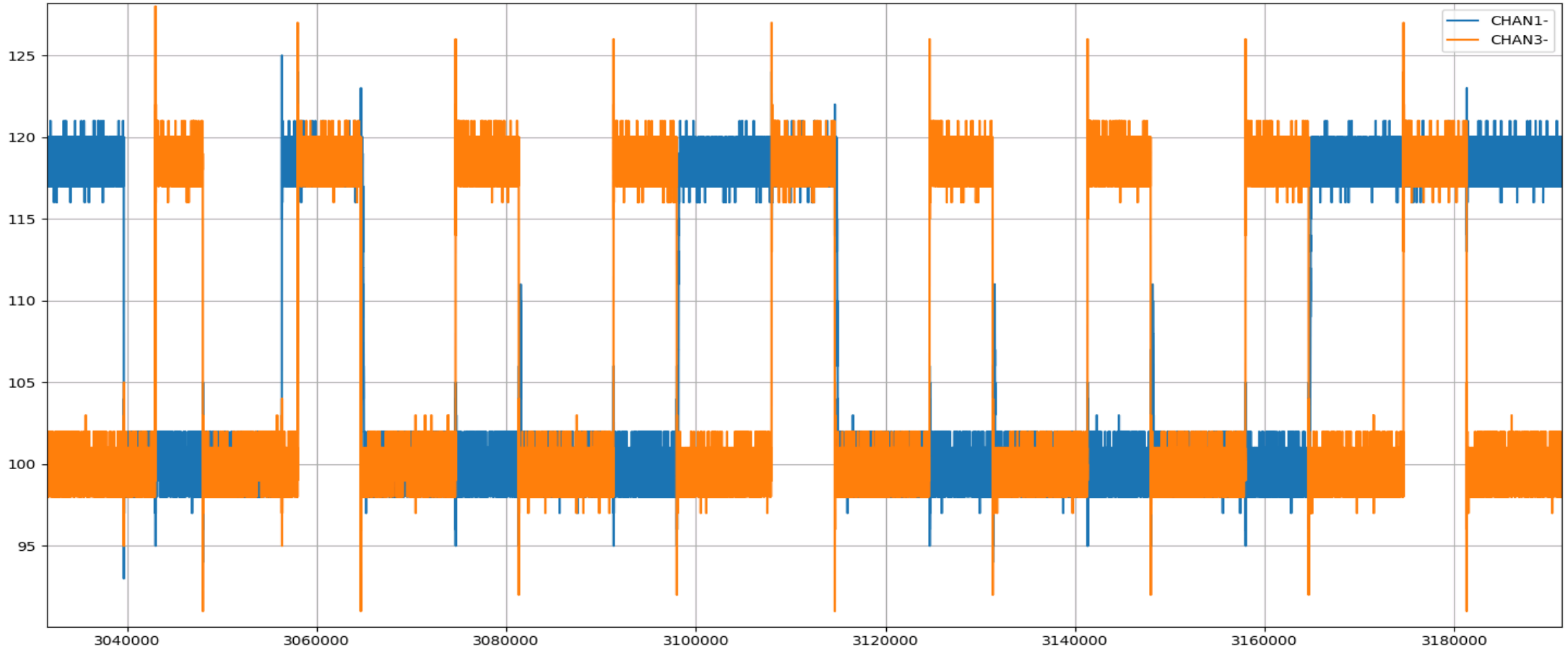
[SOFT I2C REQ] [HARDWARE I2C RESPONSE]

Soft I2C

- 
CHAN1-
CHAN3-
125
120
115
110
105
100
95
90
2220000
2240000
2260000
2280000
2300000
2320000
2340000
2360000
2380000

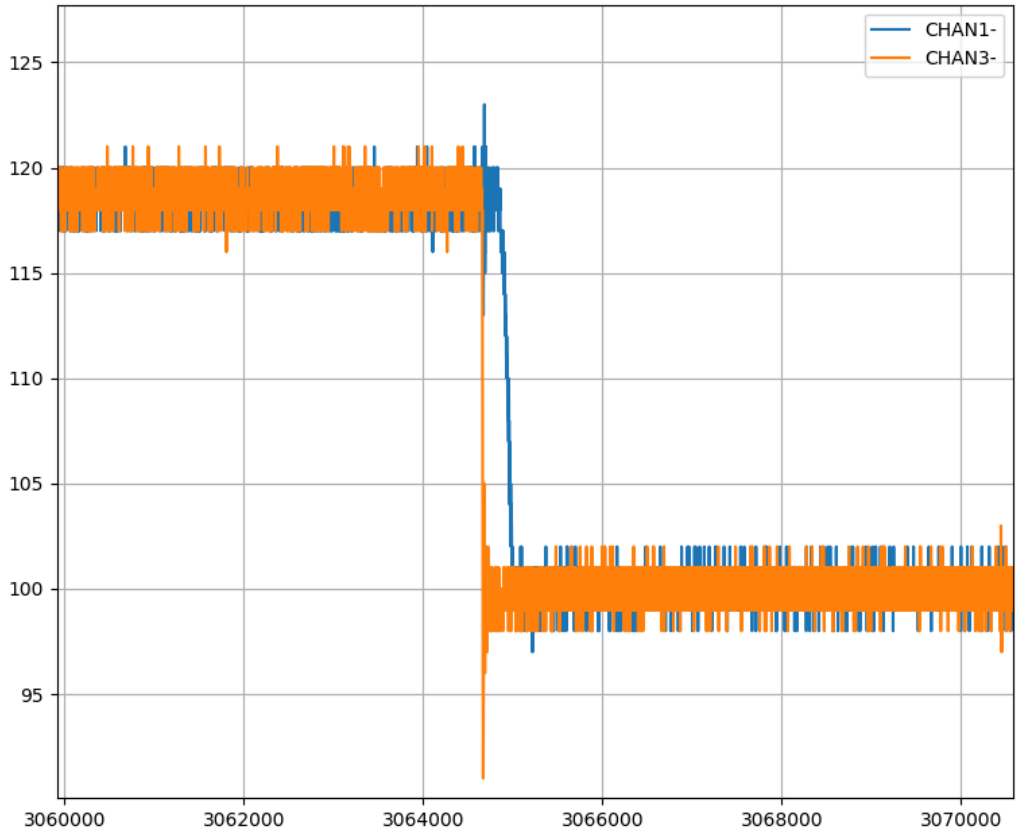
IOActive
Hardware | Software | Wetware
SECURITY SERVICES

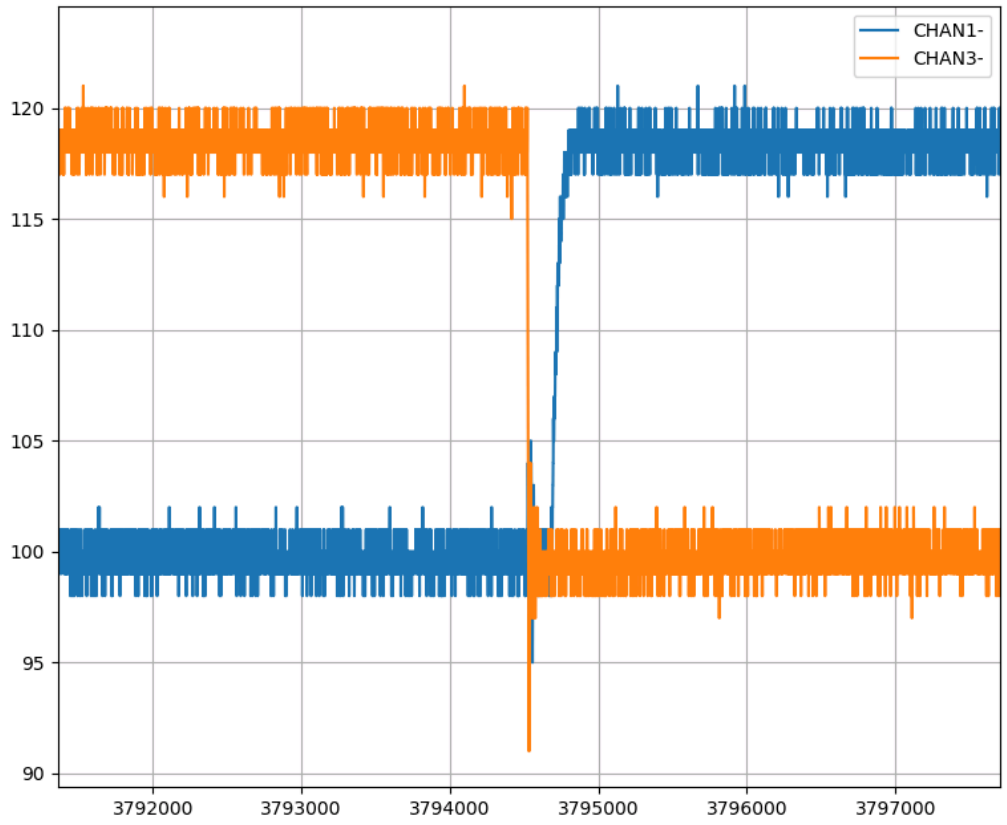
Hardware I2C



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

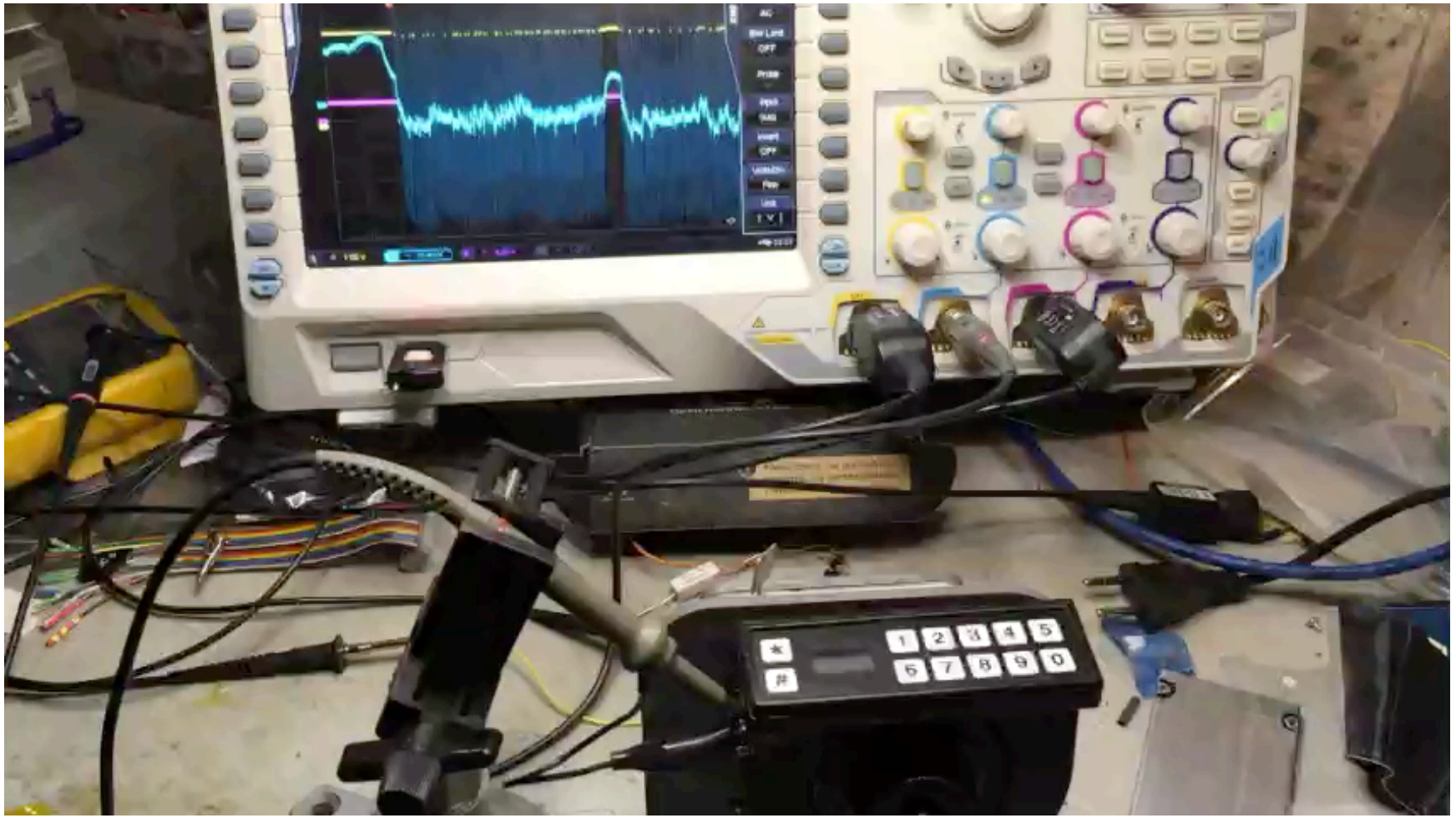
Pop!





IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Demo!



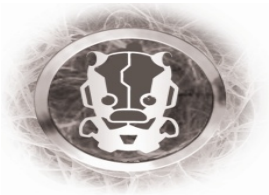
IOActive
Hardware | Software | Wetware
SECURITY SERVICES

"… but what about Gen2?"

"Gen2"

*gen2 is… interesting..

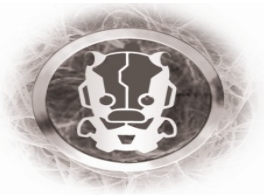
AuditCon



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

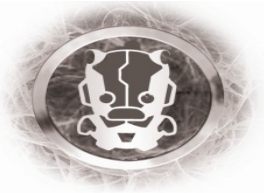
Done Right?

- Write advisory
- Do disclosure
- …DEFCON



Fuuuuuuu.

- Sometimes Kaba != Kaba
- We called the wrong Kaba, but they make locks too!
- From pictures of their locks found online they seem to share the same design pattern
  - (https://www.keypicking.com/viewtopic.php?f=100&t=8680)
- “I believe that you will find that the X-09 design different enough to be much more of a challenge. If you are experimenting on an X-10 lock, you have obtained the lock illegally and whoever from the U.S. provided / sold you the lock will be pursued by U.S. Federal agents.”




© 2013 Kaba Mas LLC. All Rights Reserved.

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

GSA

General Services Administration
Interagency Committee on Security Equipment
Security Equipment and Locking Systems
Washington DC

6 March 2018

Cesar Cerrudo
Chief Technology Officer
IO Active
701 5th Avenue, Suite 7250
Seattle WA 98104

Subject: Authority for the Testing of US Government Combination Locks

Reference: A. Executive Order 13526

B. 32 Code of Federal Regulations (Parts 2001.42)

C. Federal Specification FF-L-2740B

Mr. Cerrudo,

It has come to the attention of the General Services Administration, Interagency Committee on Security Equipment (GSA/IACSE), that your company may be in the process of analyzing electromechanical combination locks approved under Federal Specification FF-L-2740B. These electromechanical combination locks are tested and approved for the protection of classified information by the General Services Administration under the authority derived from the 32 Code of Federal Regulations and Executive Order 13526 signed by the PRESIDENT on 29 December 2009.

Electromechanical combination locks tested and approved under Federal Specification FF-L-2740B are only for use by the US Government and are placed on a Qualified Products List (QPL) with contracts established between the manufacturers and the US Government subject to continued security testing. If at any time it is determined that the locks are no longer as secure as required under the specification the manufacturer can be removed from the QPL with all contracts subject to termination. If your company has any information regarding the security of the products approved under this or any other federal specification involving the protection of classified information it should be held in strict confidence and appropriately reported to GSA.

GSA-approved combination locks are only used by the US Government and its contractors for the protection of classified information. They are not used by any financial institution or the general public therefore; the practice of only notifying the manufacturer of discovered security issues is unacceptable due to the potential impact on the worldwide protection of US Government classified information. In addition, the publication of security information in this case would not serve the public interest; conversely it would put the National Security of the United States at great risk.

Again, if your company has information to report to the US Government regarding combination locks approved under Federal Specification FF-L-2740B please contact GSA, Mr.

Sincerely,

CC: GSA/IACSE Members

General Services Administration, Q1

Information Security Oversight Office, National Archives and Records Administration

National Counterintelligence and Security Center, Office of the Director of National Intelligence

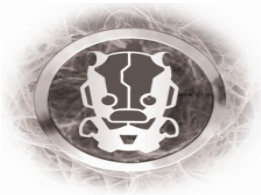
Office of the Undersecretary of Defense for Intelligence

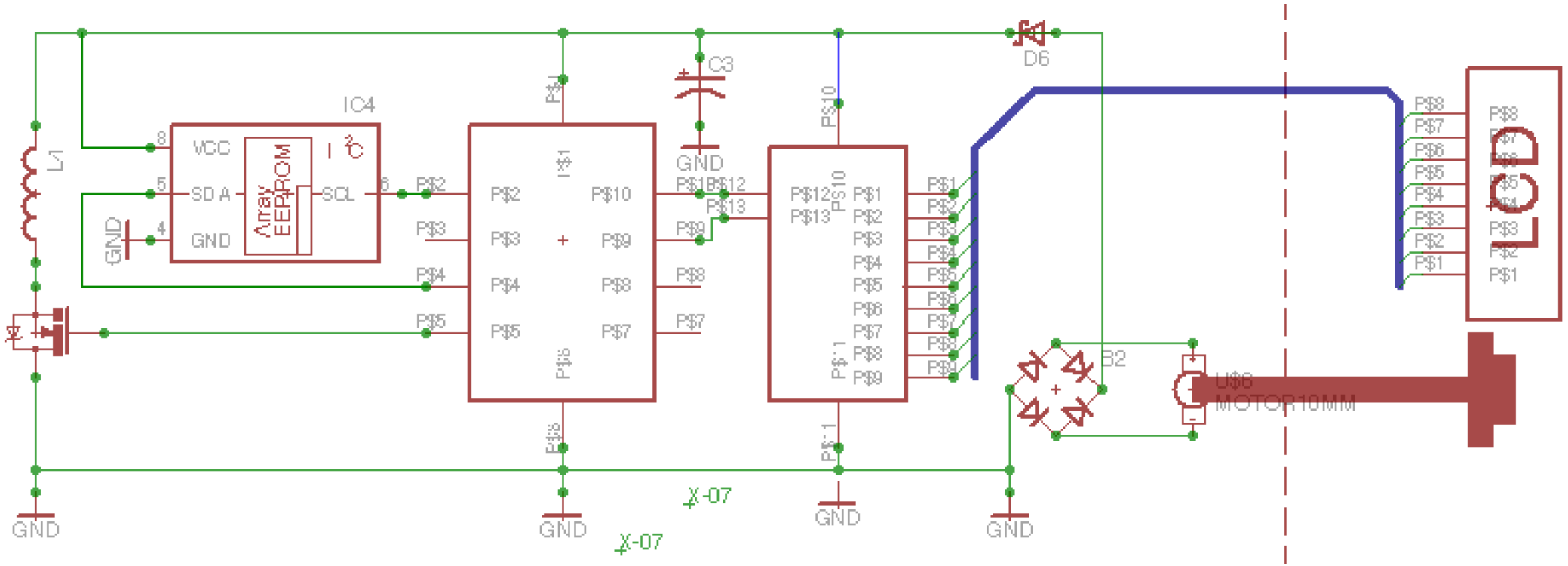
Central Intelligence Agency

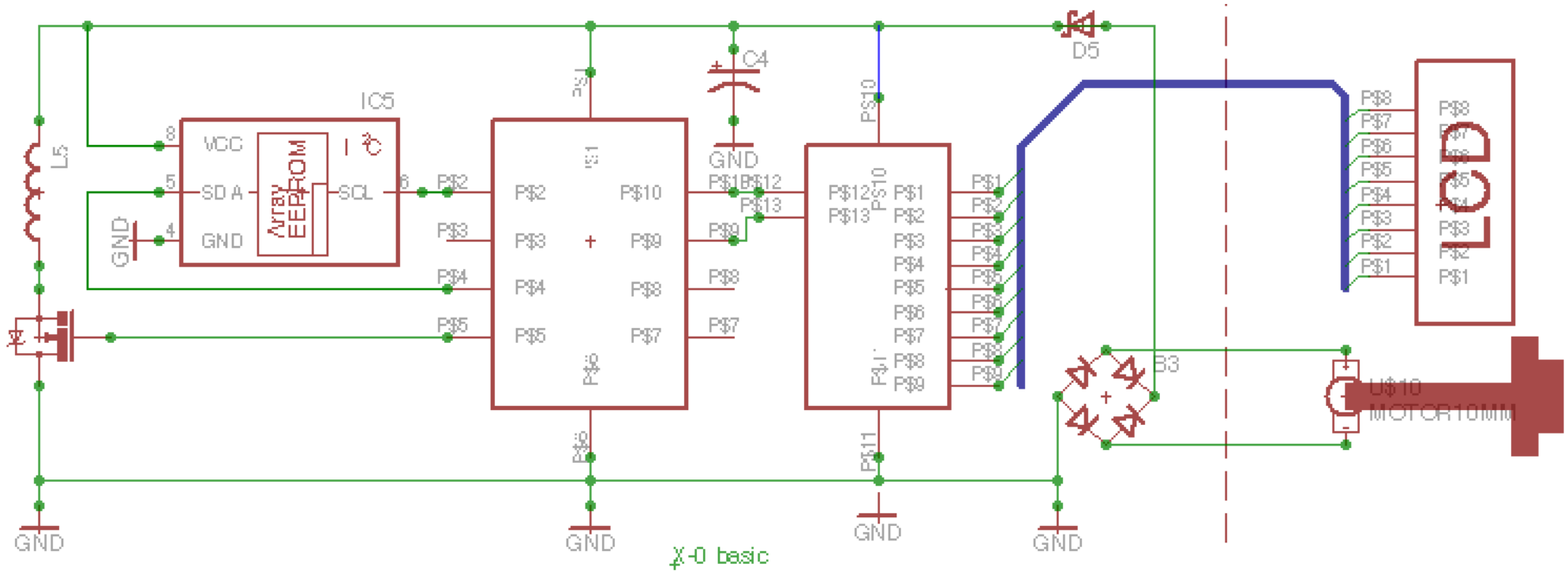
Federal Bureau of Investigation

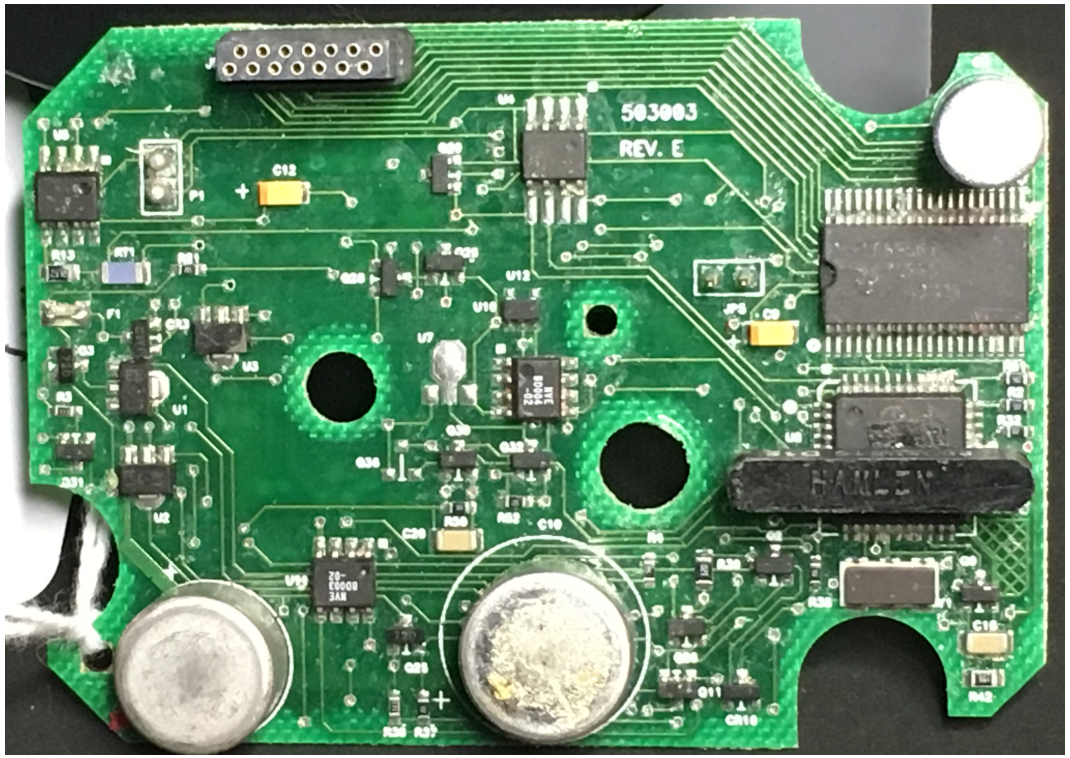
Department of State

National Security Agency

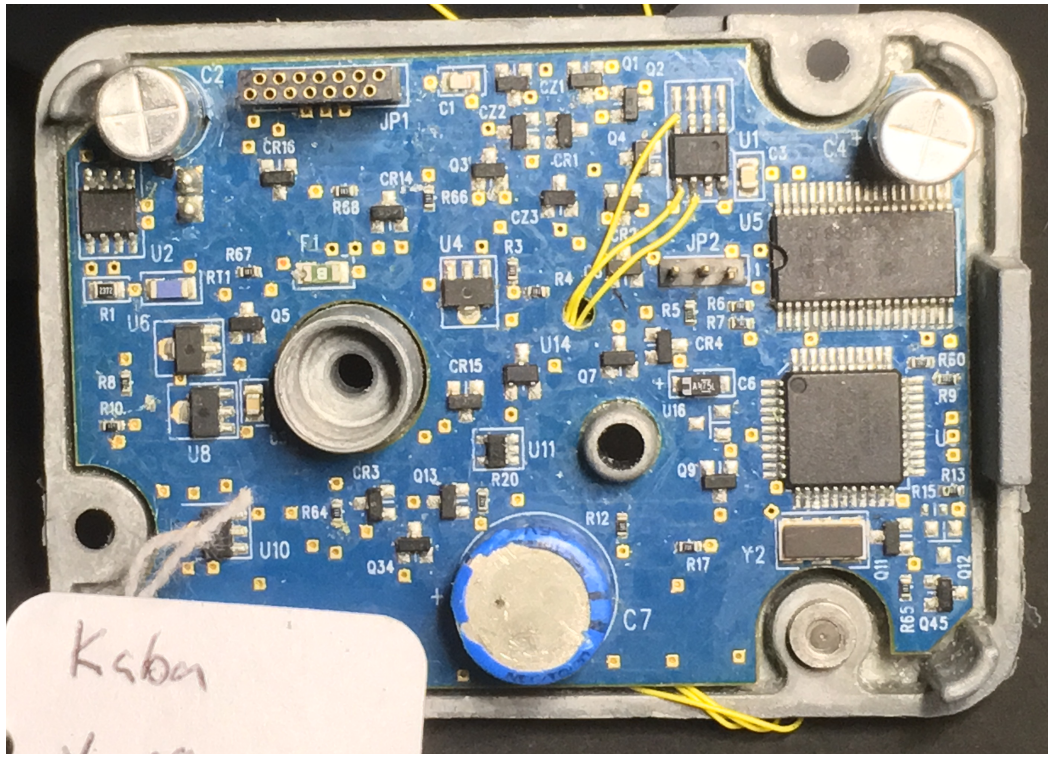



IC4
VCC
SDA
GND
SCL
Array EEPROM
GND
C3
GND
D6
B2
U$6
MOTOR10MM
LCD
GND
GND
GND
GND
X-07
X-07

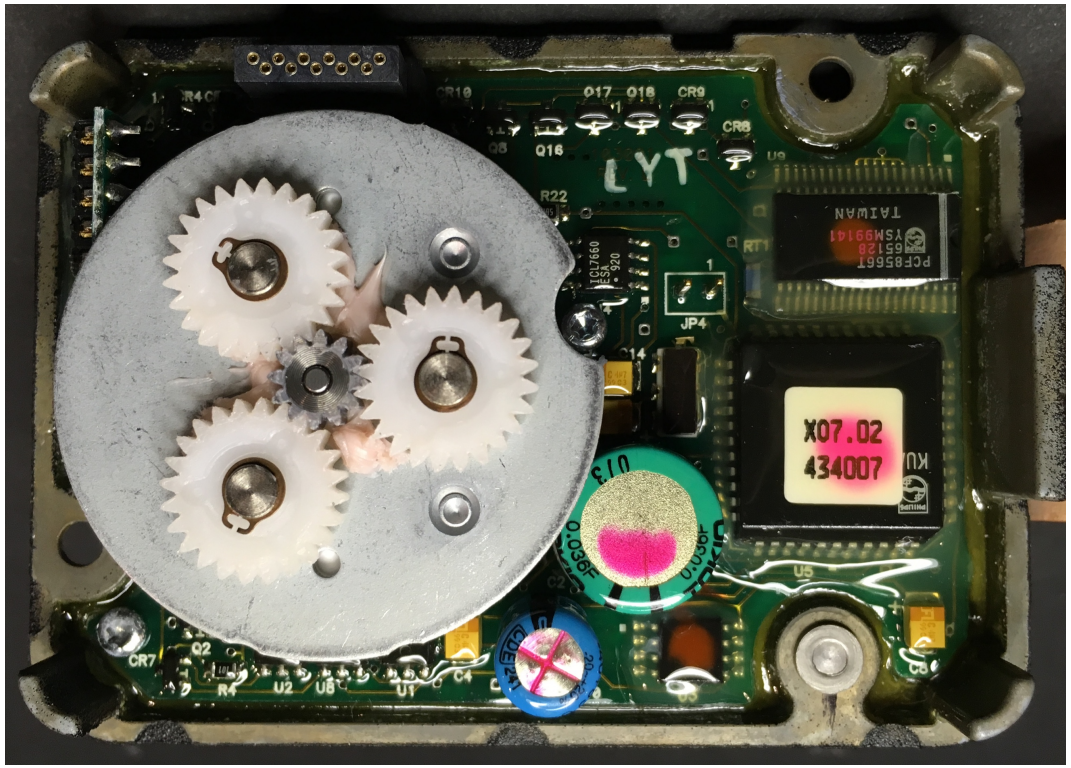

IC5
VCC
SDA
GND
SCL
Array EEPROM
I²C
C4
D5
LCD
B3
U$10
MOTOR10MM
GND
X-0 basic

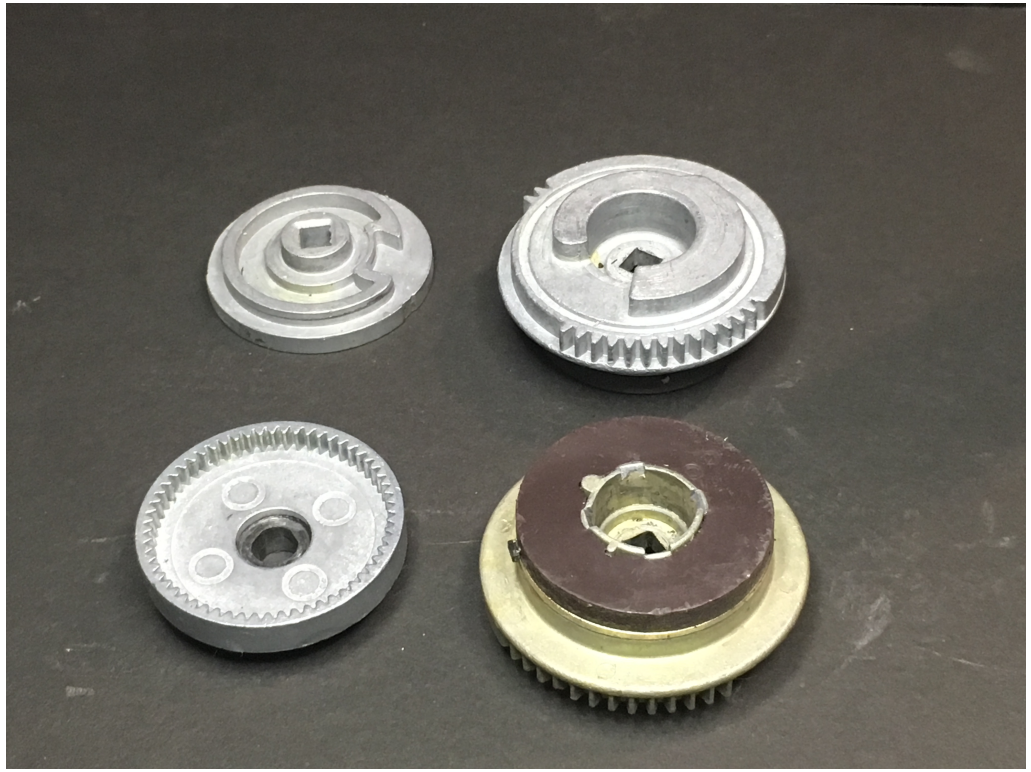


X-08

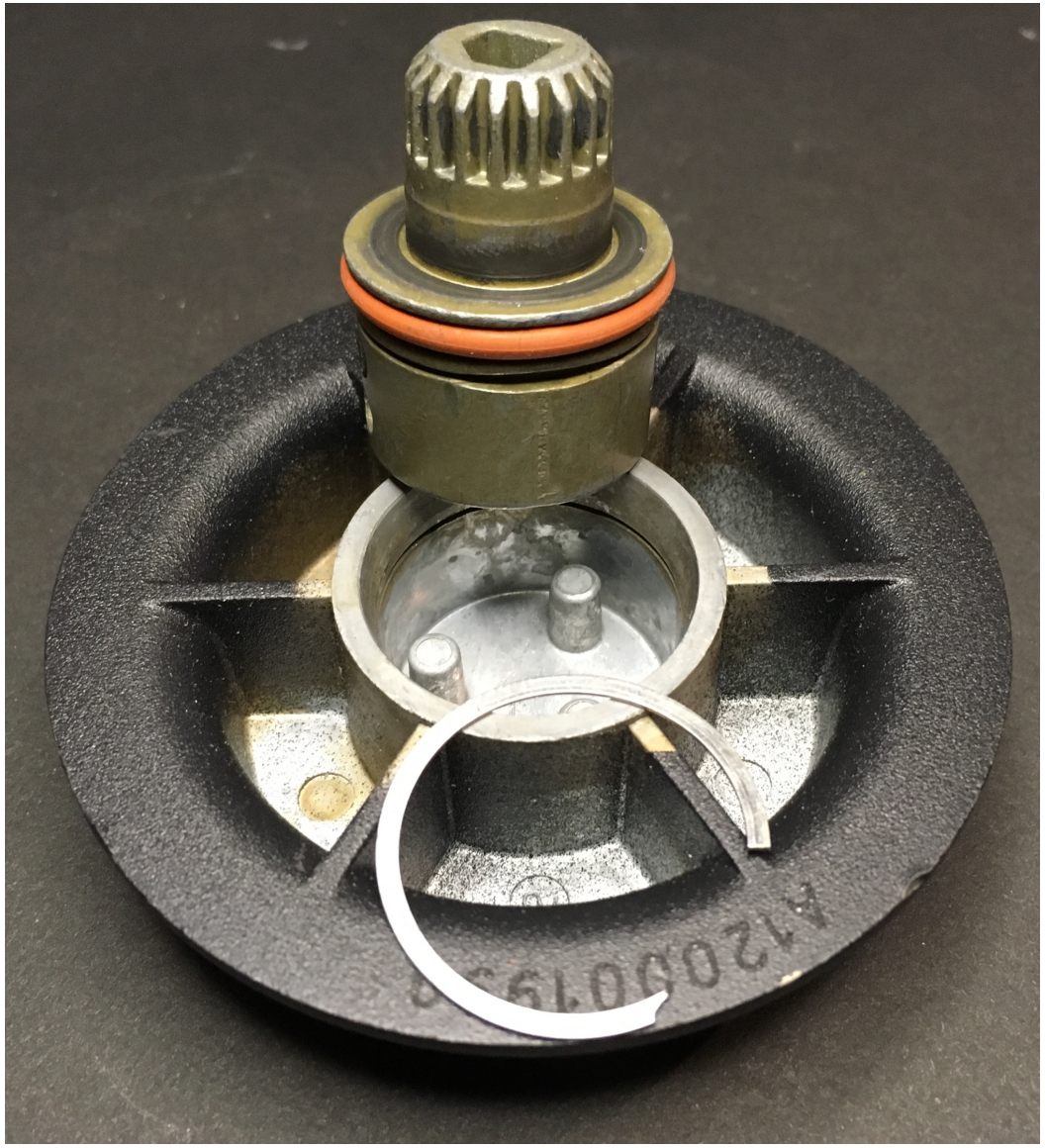


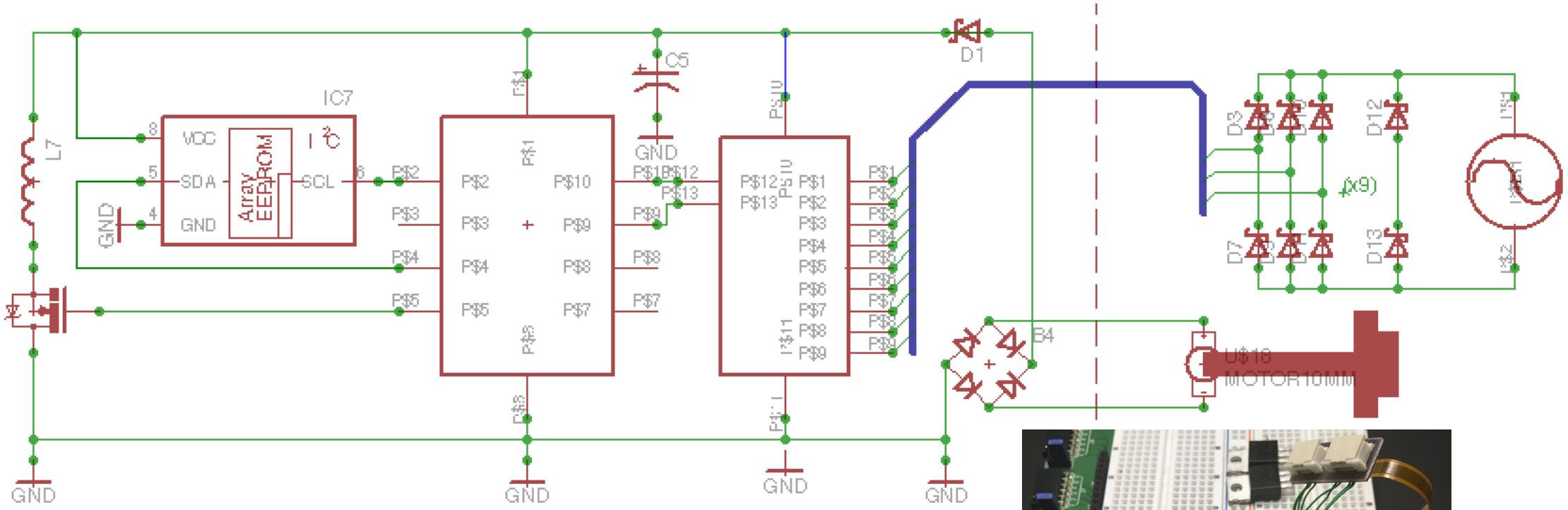
X-09

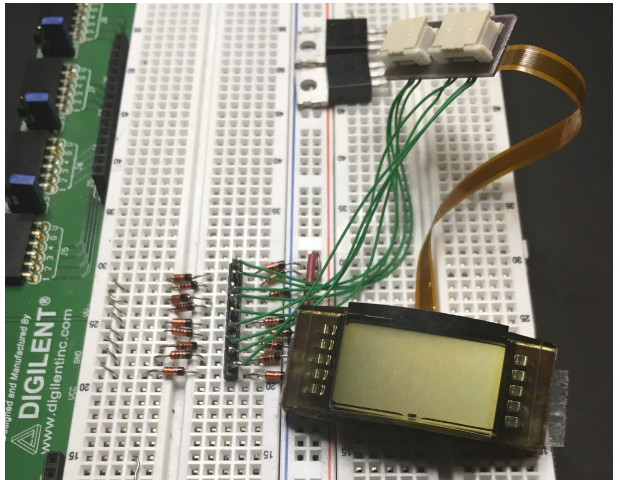

LYT
X07.02
434007
TAIWAN
JP4
U13
CR7
Q2
R4
U2
U8
U1
C4
U5

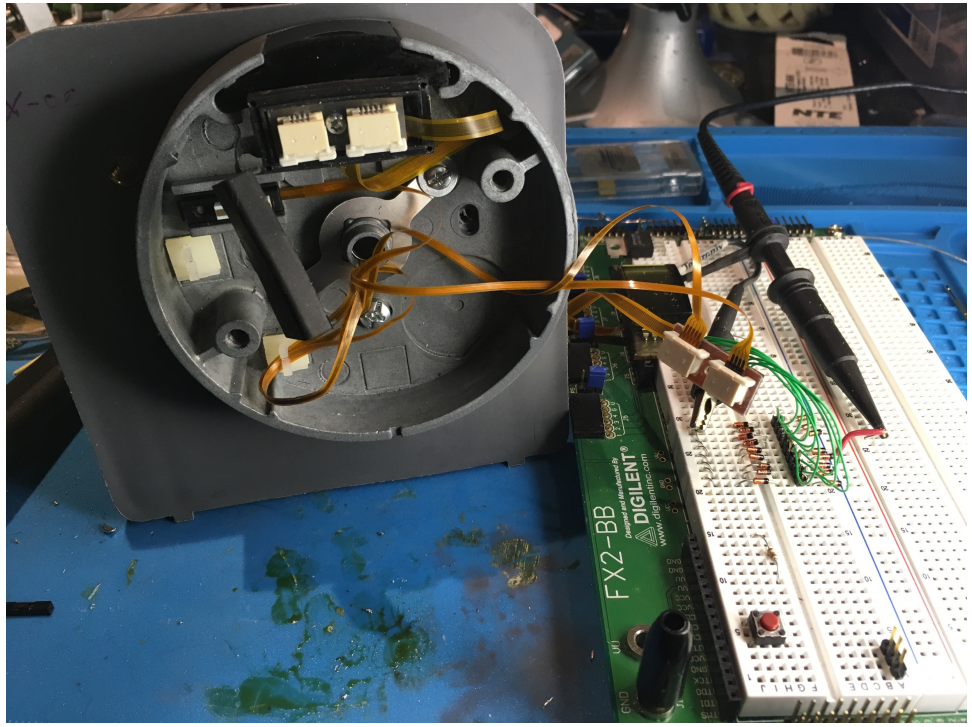


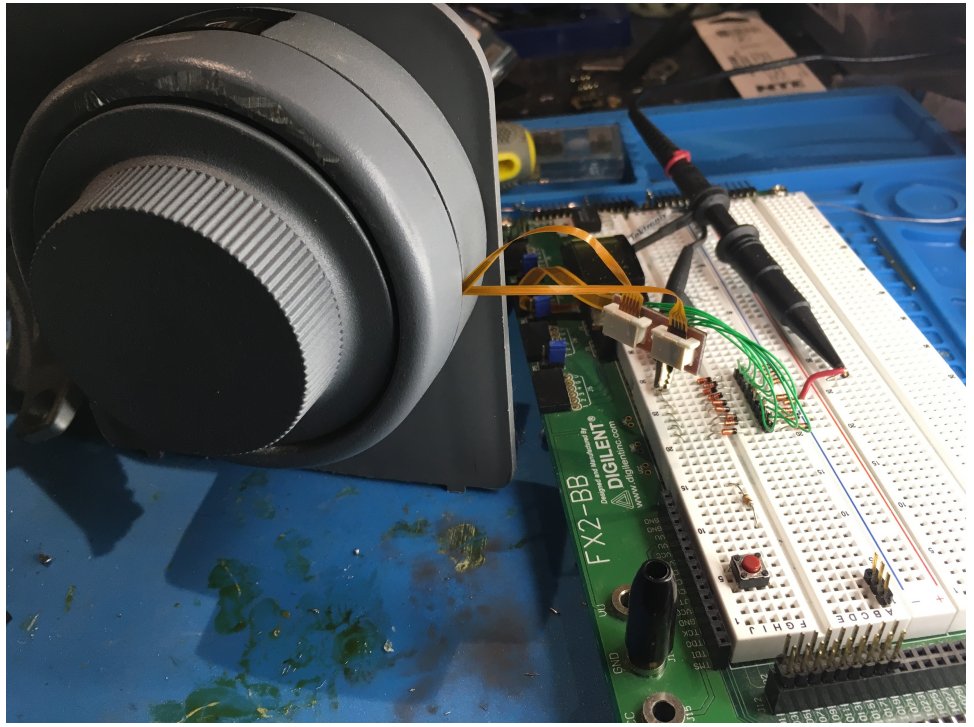
WHY REDUNDANT DESIGN MATTERS..

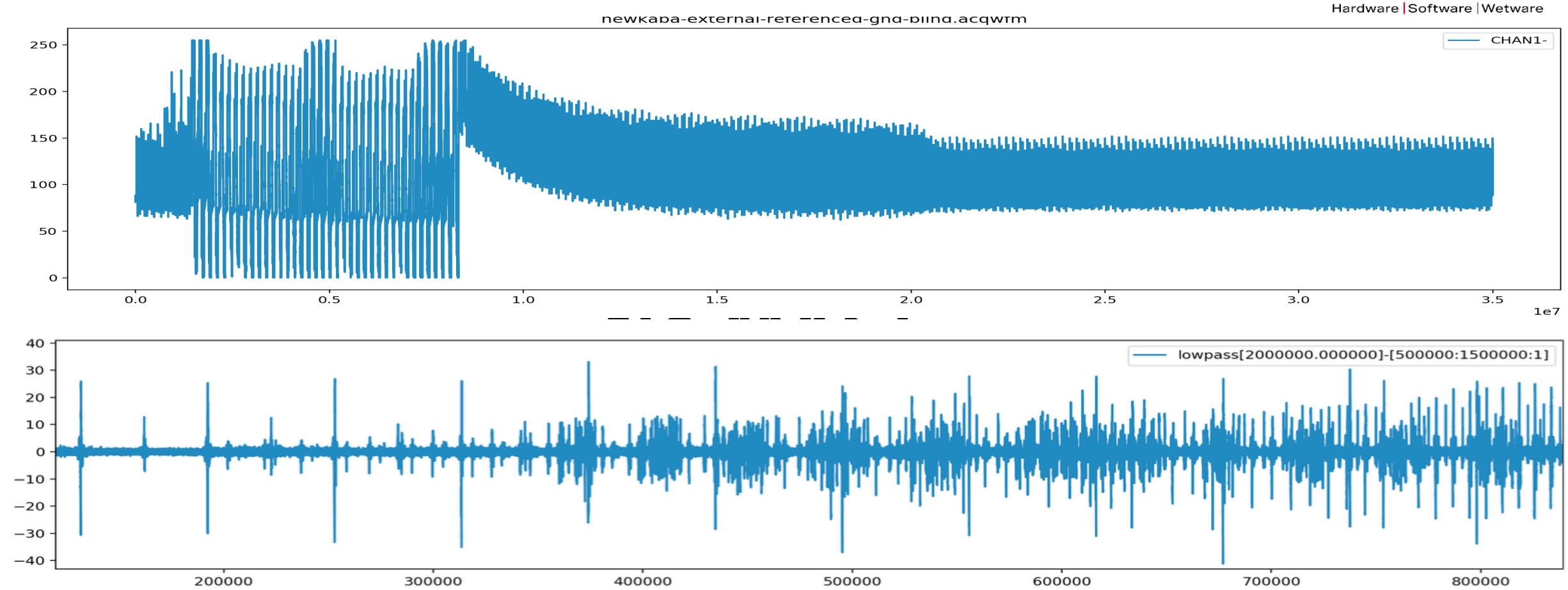


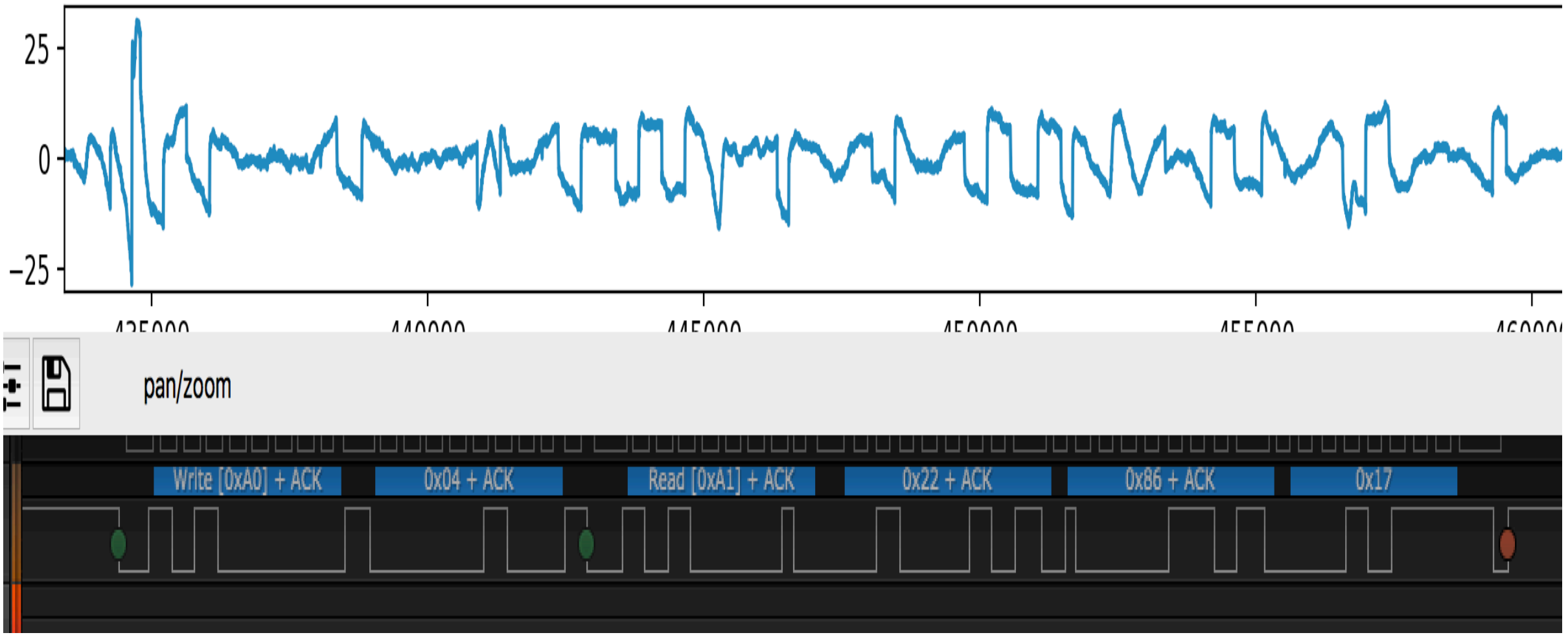

IC7
VCC
SDA
SCL
GND
Array EEPROM
I²C
L7
C5
D1
B4
D3
D12
D7
D13
(x9)
U$18
MOTOR10MM
GND


DIGILENT
www.digilentinc.com


FX2-BB
DIGILENT


FX2-BB
DIGILENT


newkaba-external-referenced-gnd-blind.acqwfm
CHAN1-
250
200
150
100
50
0
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
1e7
lowpass[2000000.000000]-[500000:1500000:1]
40
30
20
10
0
−10
−20
−30
−40
200000
300000
400000
500000
600000
700000
800000
+60 ms
+70 ms
+80 ms
+90 ms
+10 ms

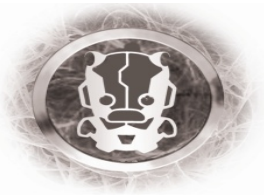

25
0
−25
425000
440000
445000
450000
455000
460000
pan/zoom
Write [0xA0] + ACK
0x04 + ACK
Read [0xA1] + ACK
0x22 + ACK
0x86 + ACK
0x17

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

But… What about the X-10?

"Based on the information presented at the meeting, it does not look like it would be beneficial to spend any time looking at the X-10 model."

- GSA



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Questions?

Did I even leave time for questions?

MDavis@IOActive.com