
Nathan Seidle
Joel Bartlett
Rob Reynolds

Combos in 45
minutes or less!*

*Totes Guaranteed

2002



Credit: Me

New Products

Top Sellers

SparkFun Originals

Spectacle

Sale

Gift Certificates

Arduino

Audio

Books

Breakout Boards

Cables

Components

Development Tools

Dings and Dents

Educators

GPS

Intel® Edison

IoT

Kits

LCDs

Prototyping

Raspberry Pi

Robotics

Sensors

SparkX

Swag

Tools

Way more versatility than
just radio, the bladeRF x 40.

EXPLORE THE REAL RADIO STAR



New Products

See All

PAGE 5 OF 6



**SparkFun micro:climate
kit**

★ KIT-14217

~~\$114.95~~ **\$54.95**



**SparkFun micro:arcade
kit**

★ KIT-14218

~~\$49.95~~ **\$46.78**



SparkFun moto:bit

★ DEV-14213

~~\$14.95~~ **\$11.18**



SparkFun weather:bit

★ DEV-14214

~~\$14.95~~ **\$10.95**

LATEST BLOG POST

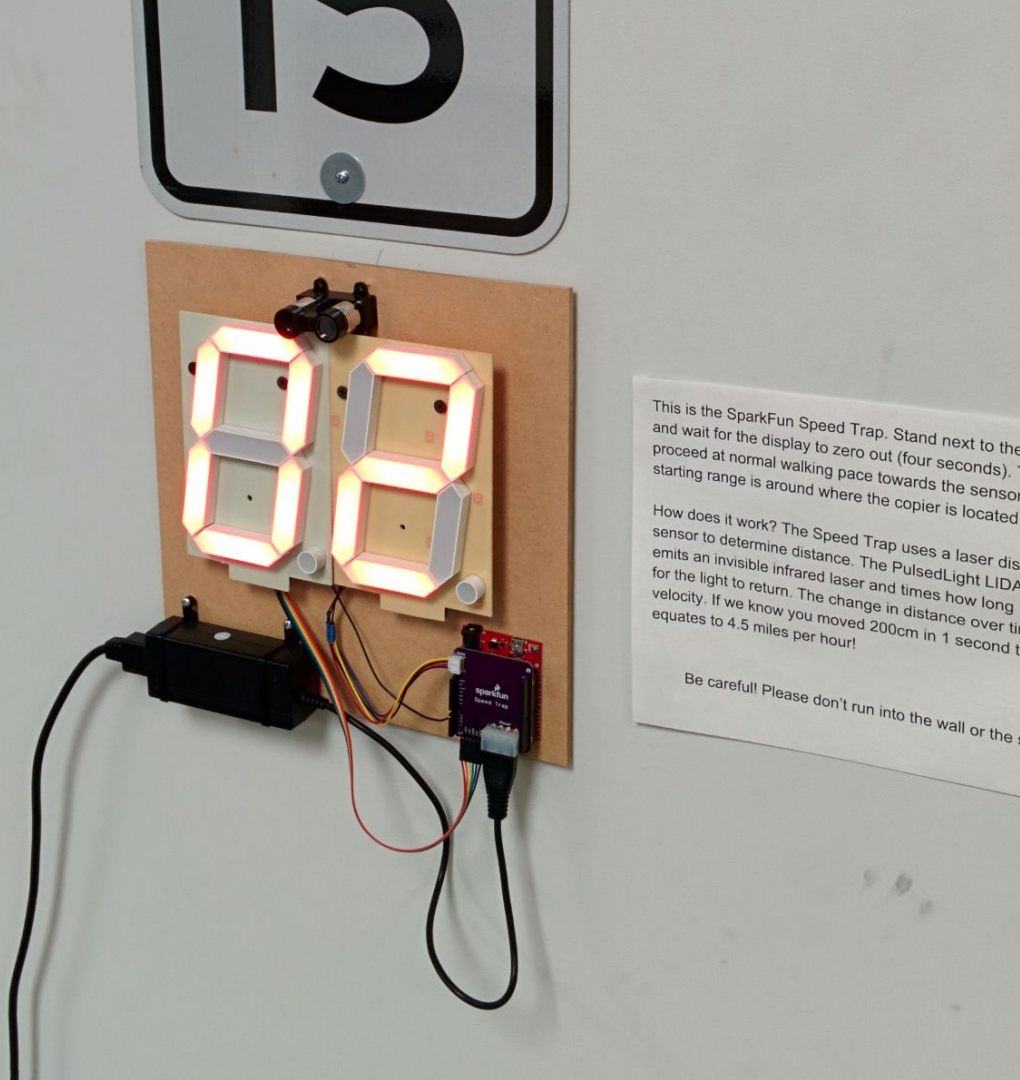
Desk of an Engineer: the Mary Edition



**FREE
SHIPPING**



Credit: Benjamin Rasmussen

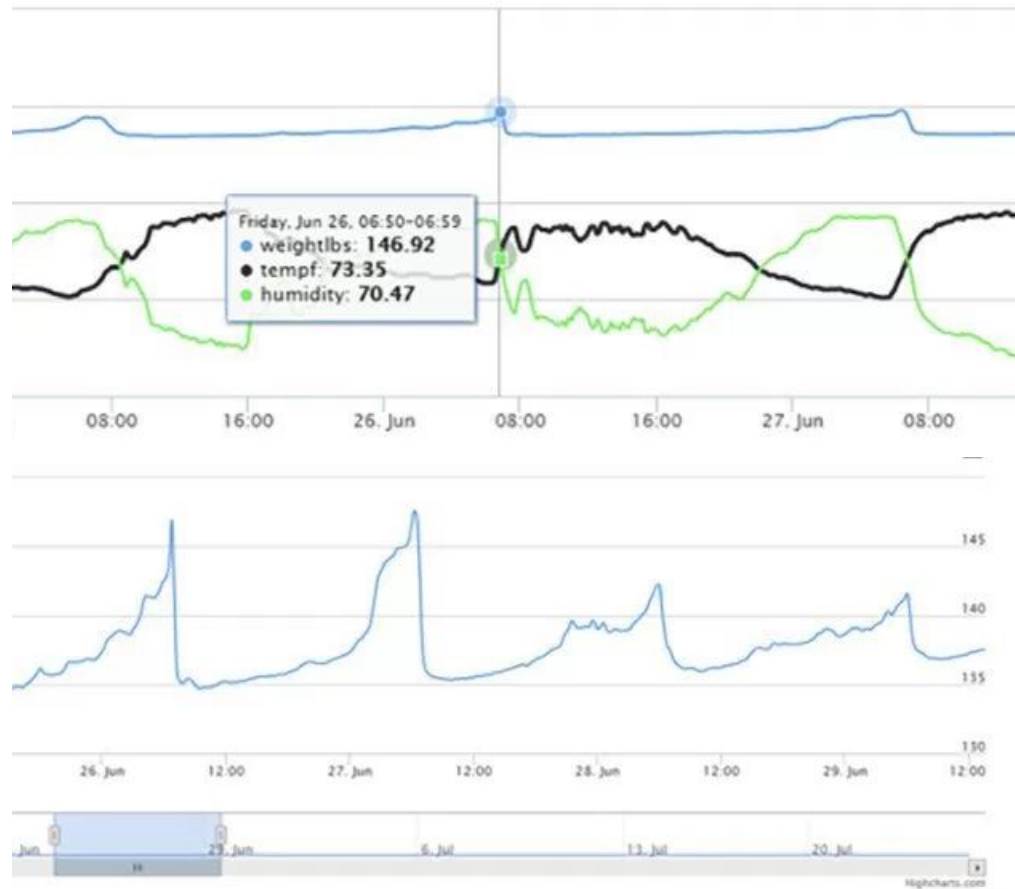
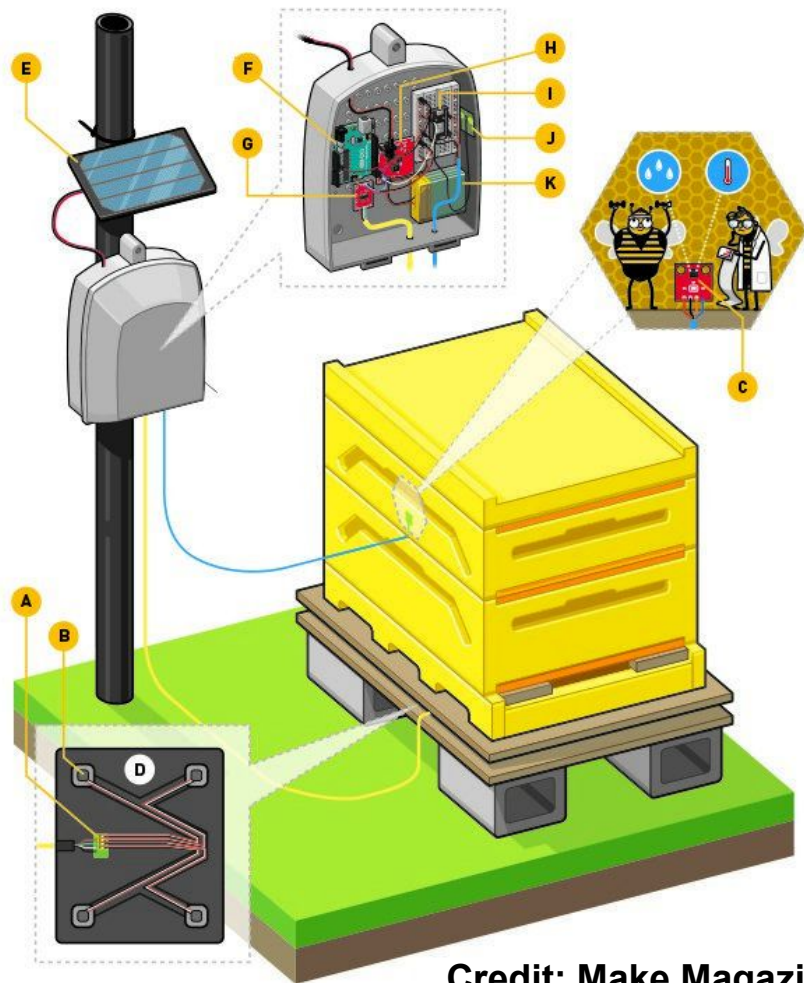


This is the SparkFun Speed Trap. Stand next to the display and wait for the display to zero out (four seconds). Then proceed at normal walking pace towards the sensor. The starting range is around where the copier is located.

How does it work? The Speed Trap uses a laser distance sensor to determine distance. The PulsedLight LIDAR sensor emits an invisible infrared laser and times how long for the light to return. The change in distance over time is velocity. If we know you moved 200cm in 1 second that equates to 4.5 miles per hour!

Be careful! Please don't run into the wall or the sensor.





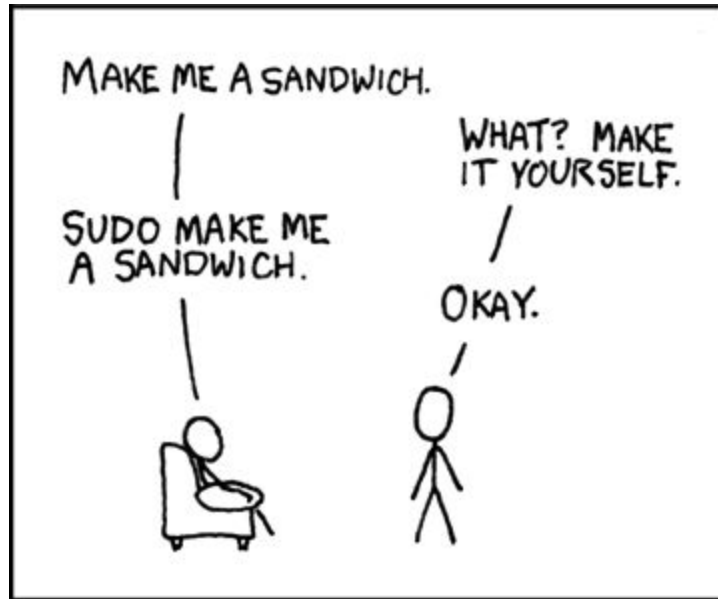
Credit: Make Magazine



Credit: SparkFun



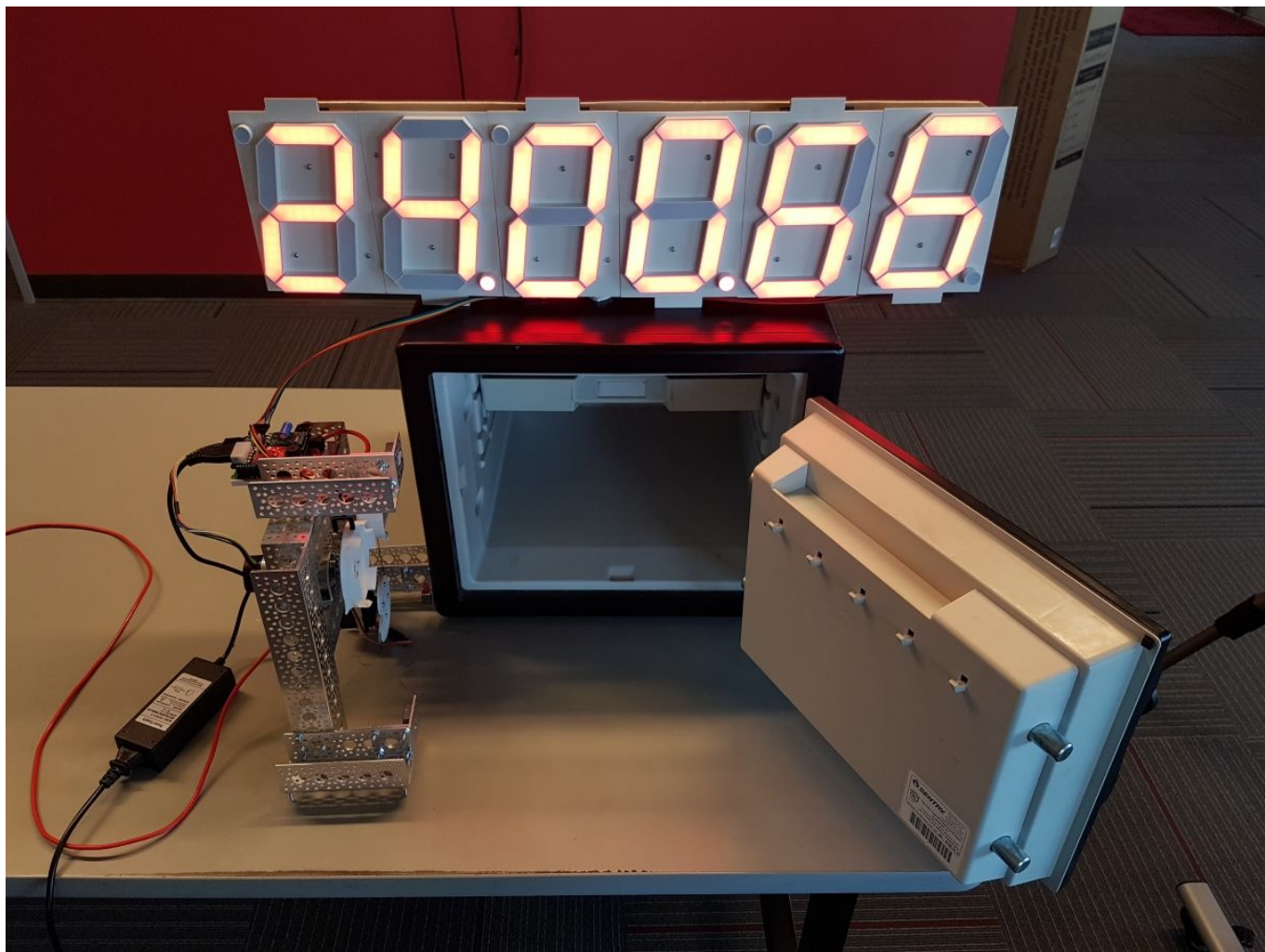
Credit: SparkFun

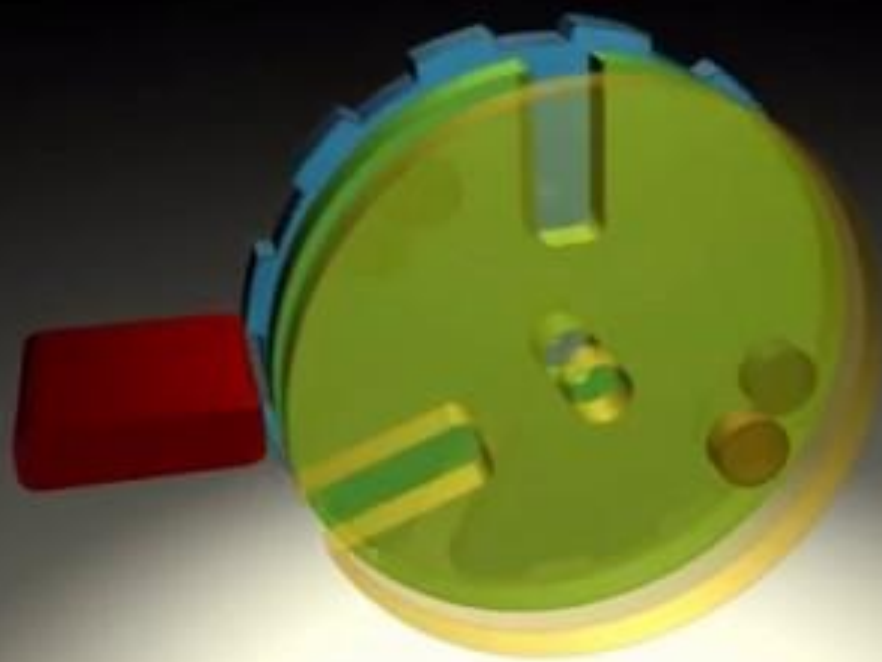


Credit: xkcd



Credit: SentrySafe / Liberty Safes





Handle puller

Servo with feedback

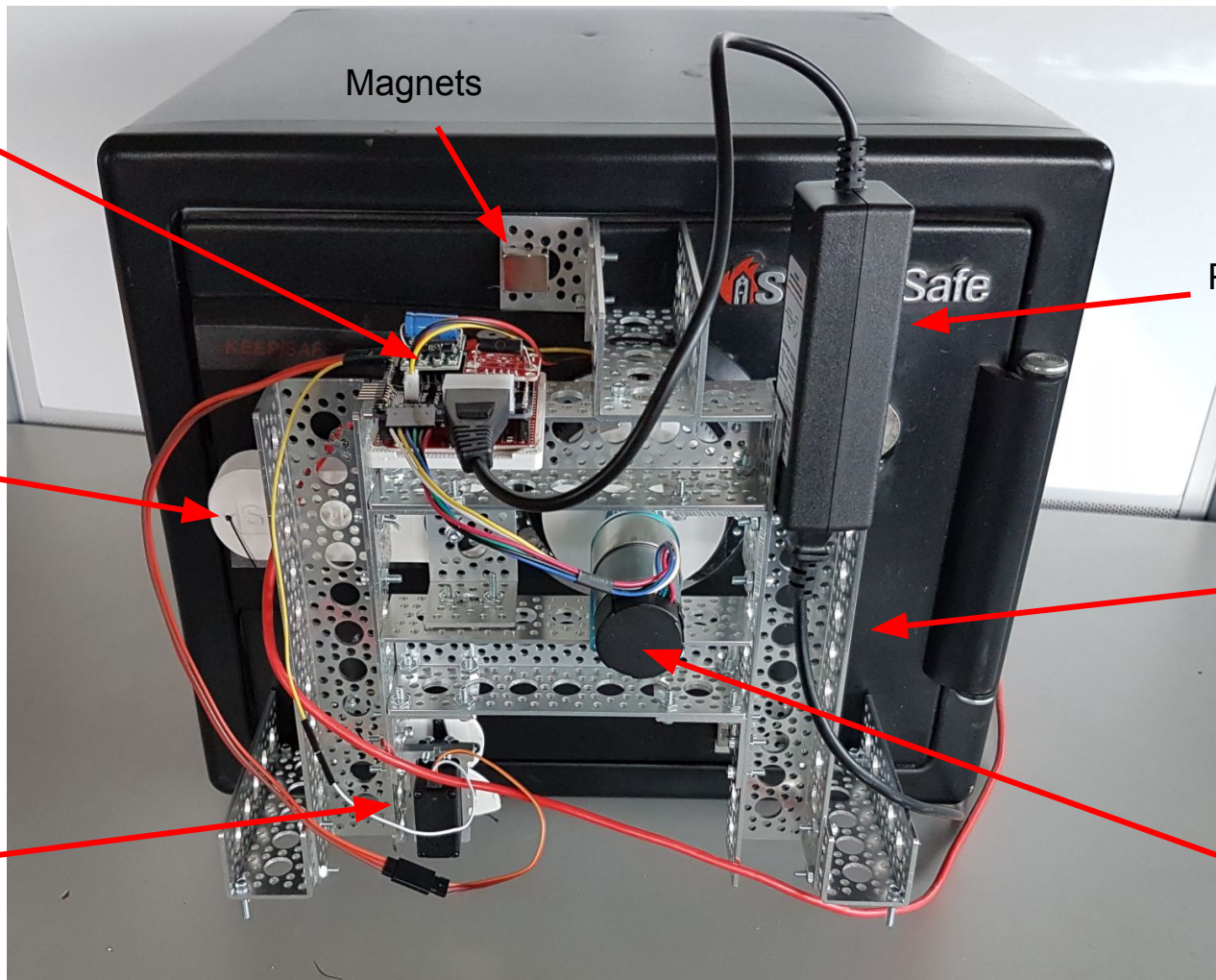
Arduino

Magnets

Power!

Erector set
(Actobotics)

Motor with 8400
tick encoder



Arduino

Handle puller

Servo with
feedback



Power!

Erector set
(Actobotics)

Motor with 8400
tick encoder

Credit: Pololu

Handle puller

Servo with feedback

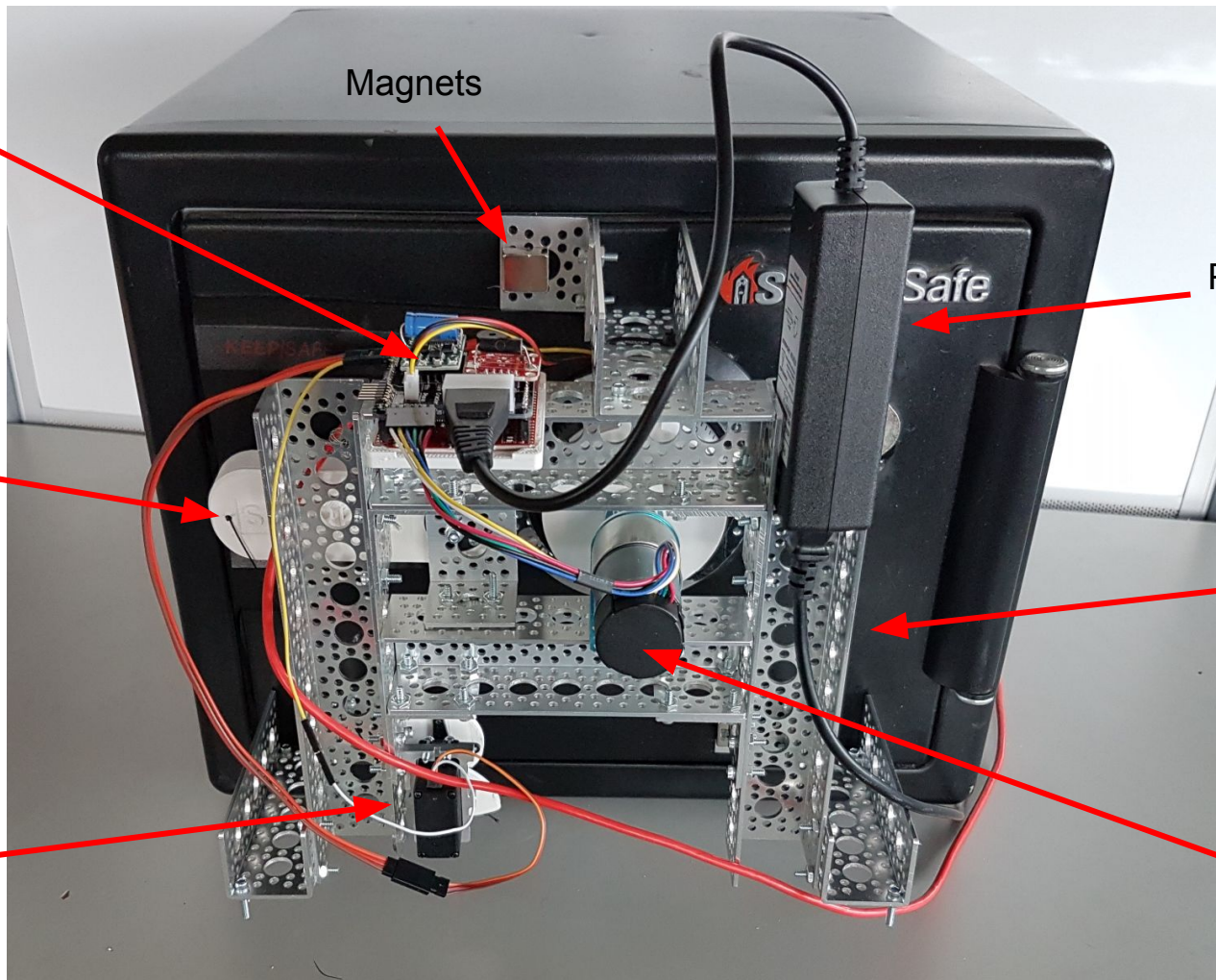
Arduino

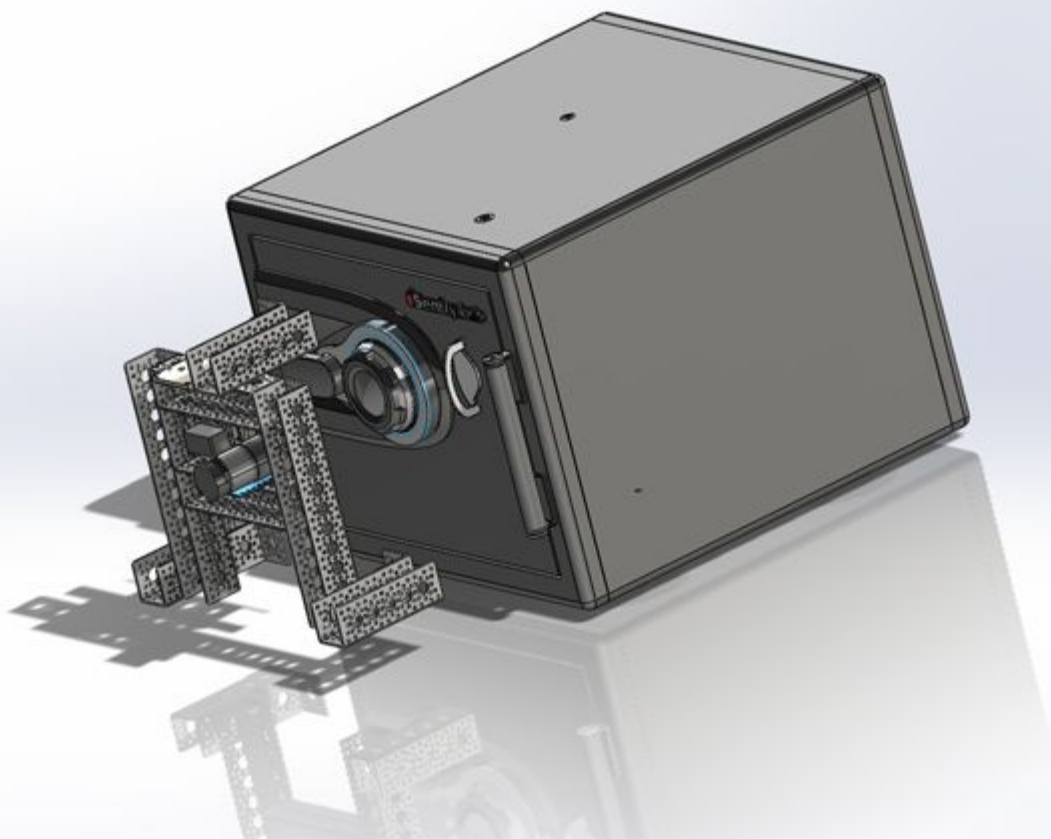
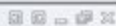
Magnets

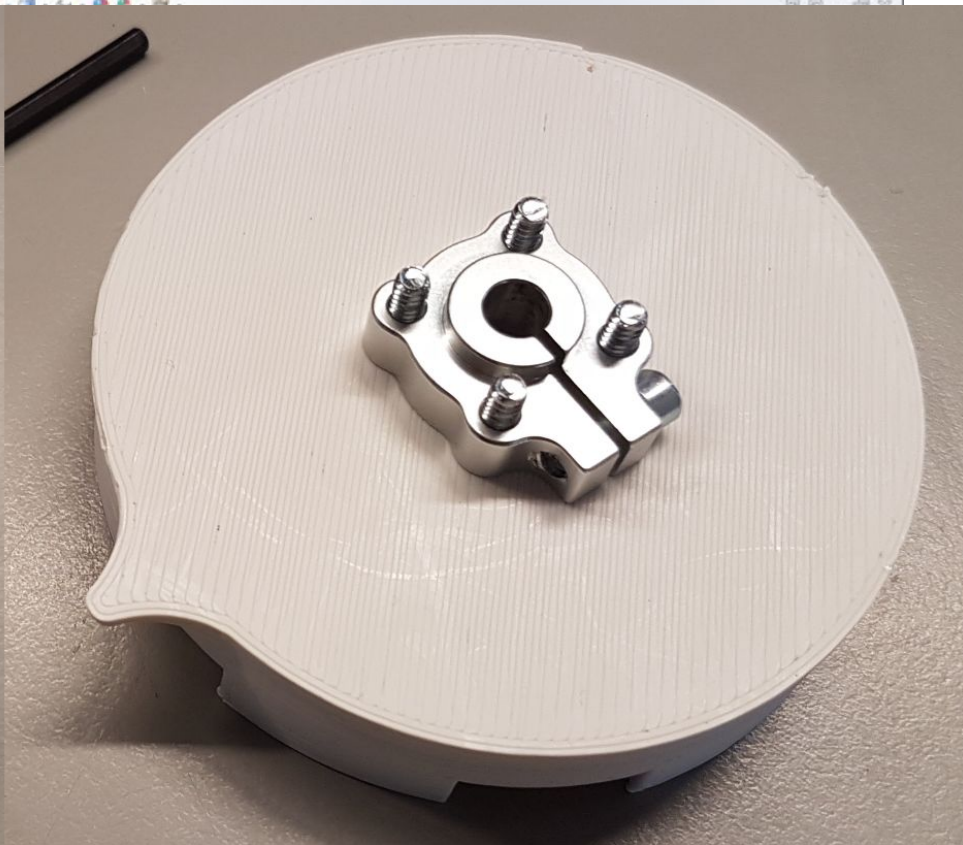
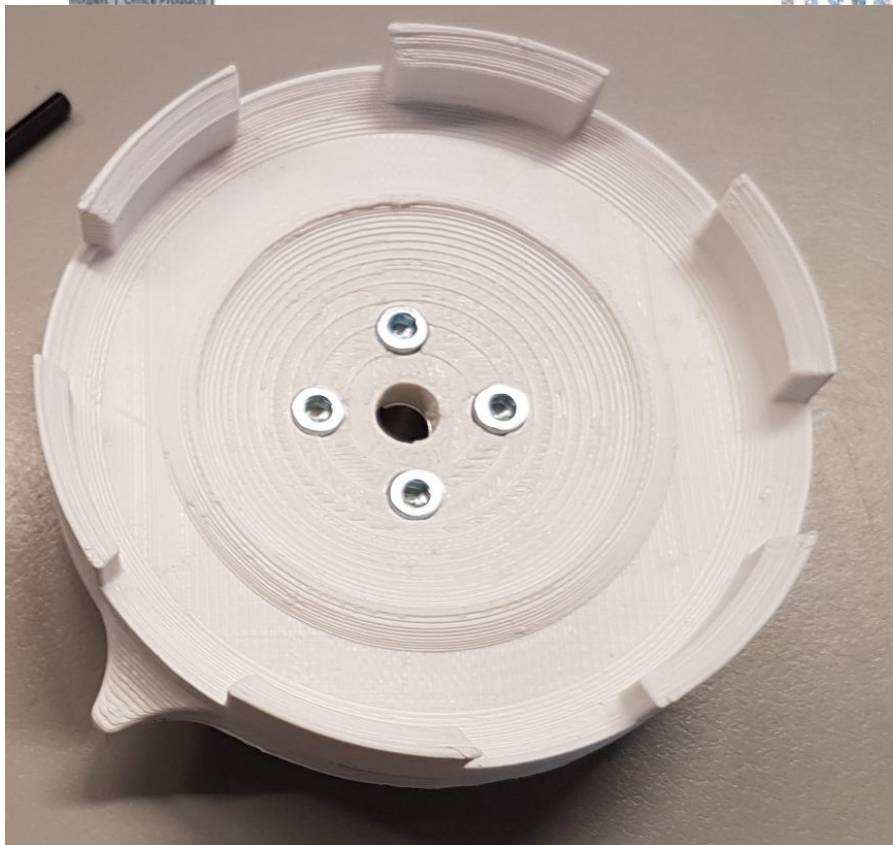
Power!

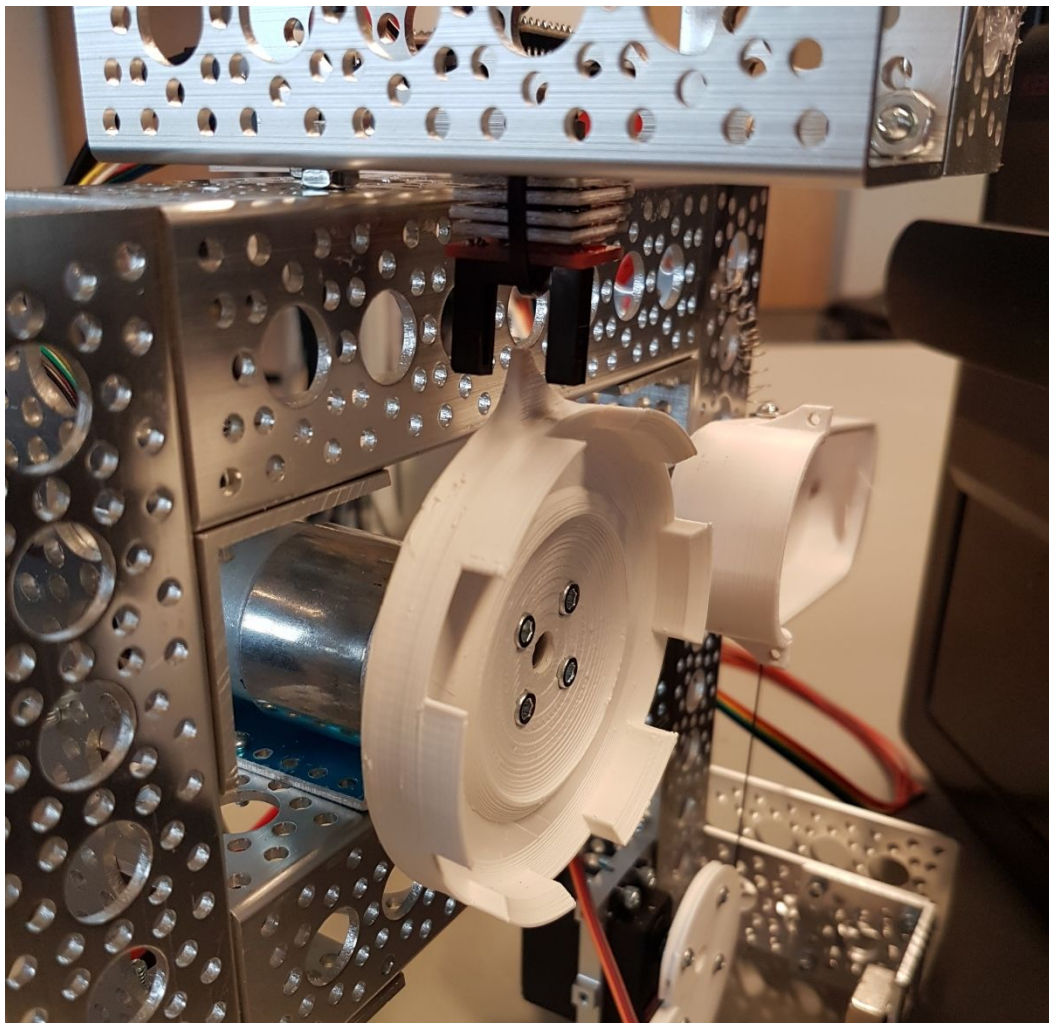
Erector set
(Actobotics)

Motor with 8400
tick encoder







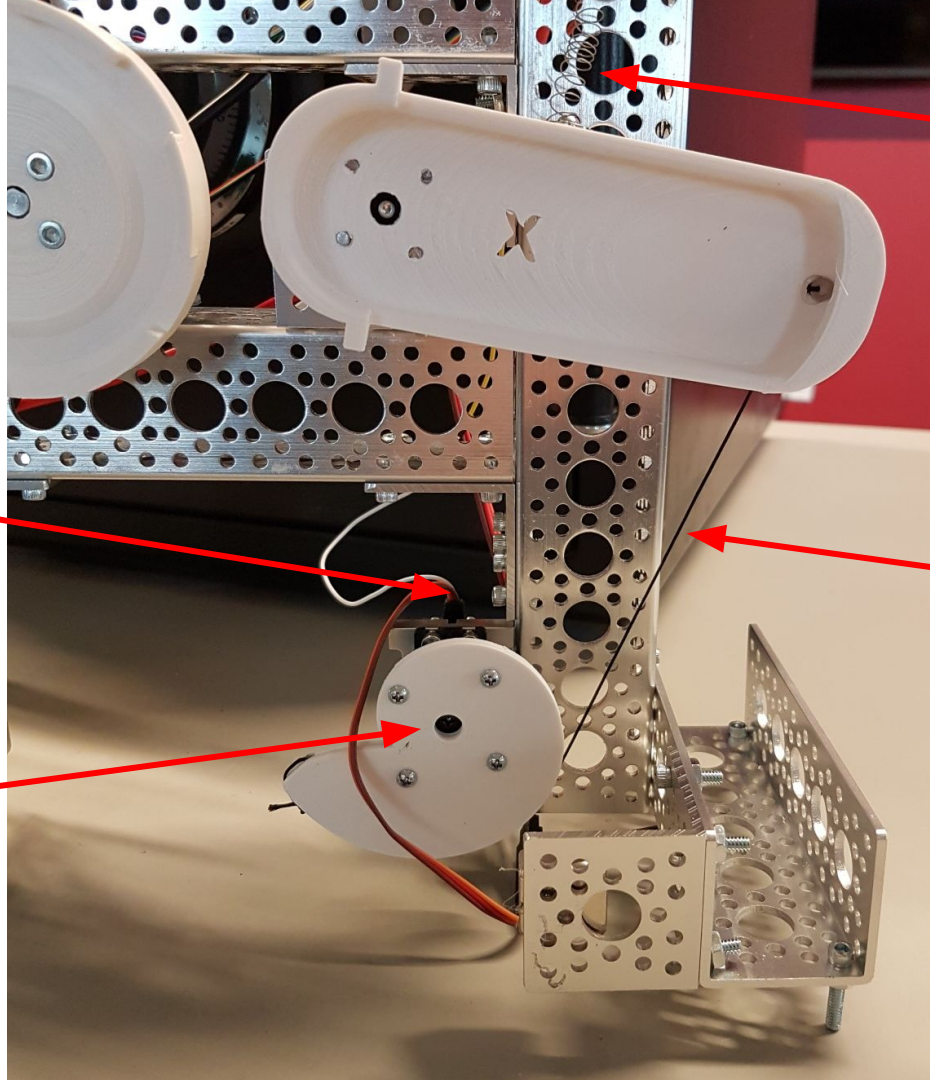


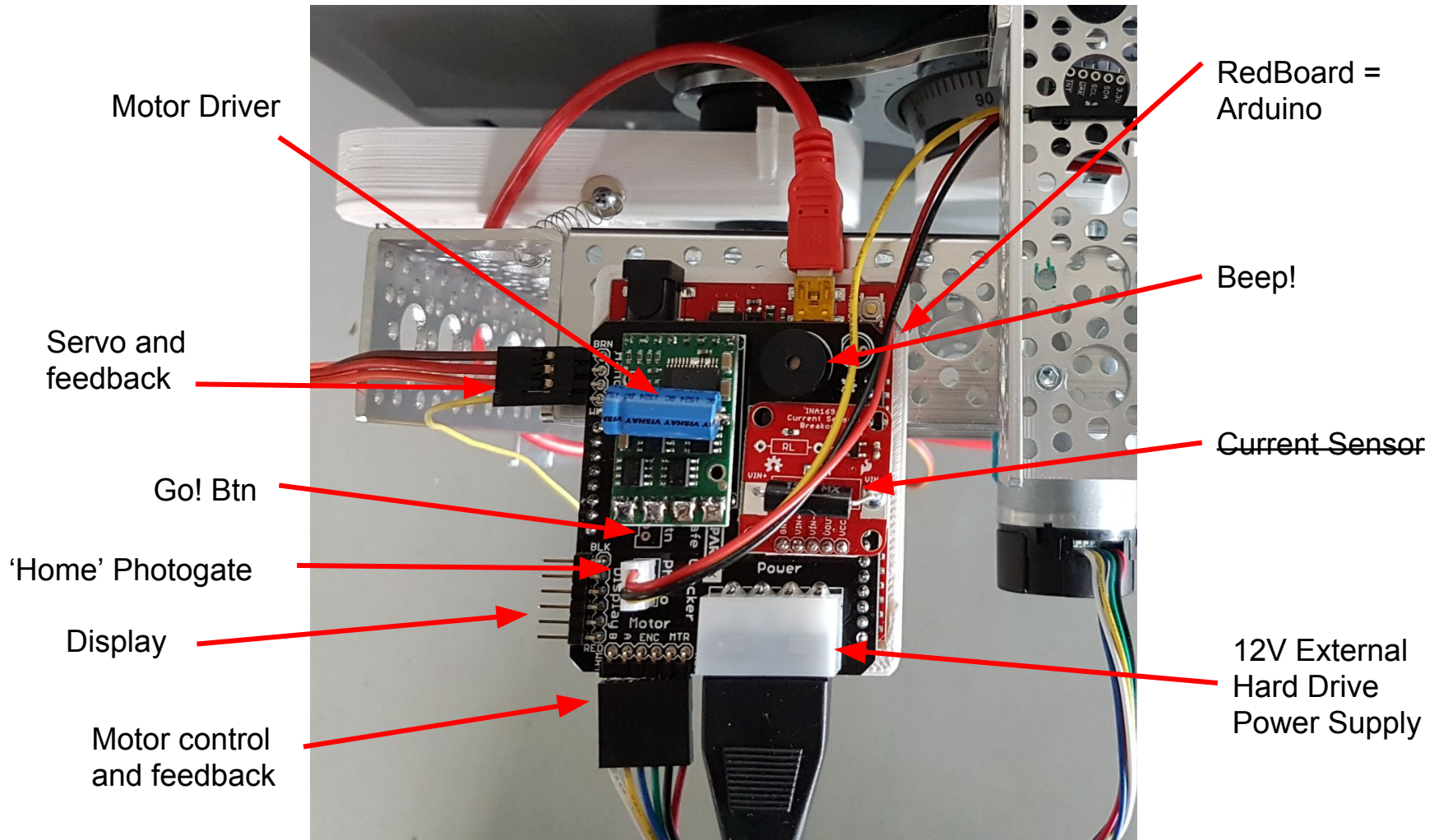
Standard servo with analog
feedback hack

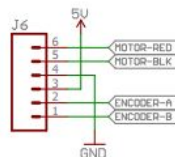
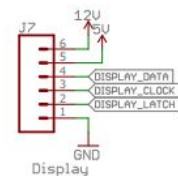
'Come back here'
spring

Very fancy string

The super freaking amazing
nautilus gear that made this all
work

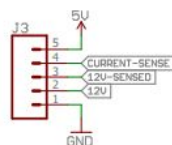




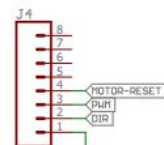


Power

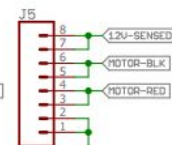
Motor Connect



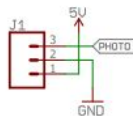
Current Sense



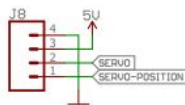
Motor Control



Motor Controller Output



Dial Zero



Handle Servo



Released under the Creative Commons
Attribution Share-Alike 4.0 License
<https://creativecommons.org/licenses/by-sa/4.0/>

TITLE: Safe Cracker Shield

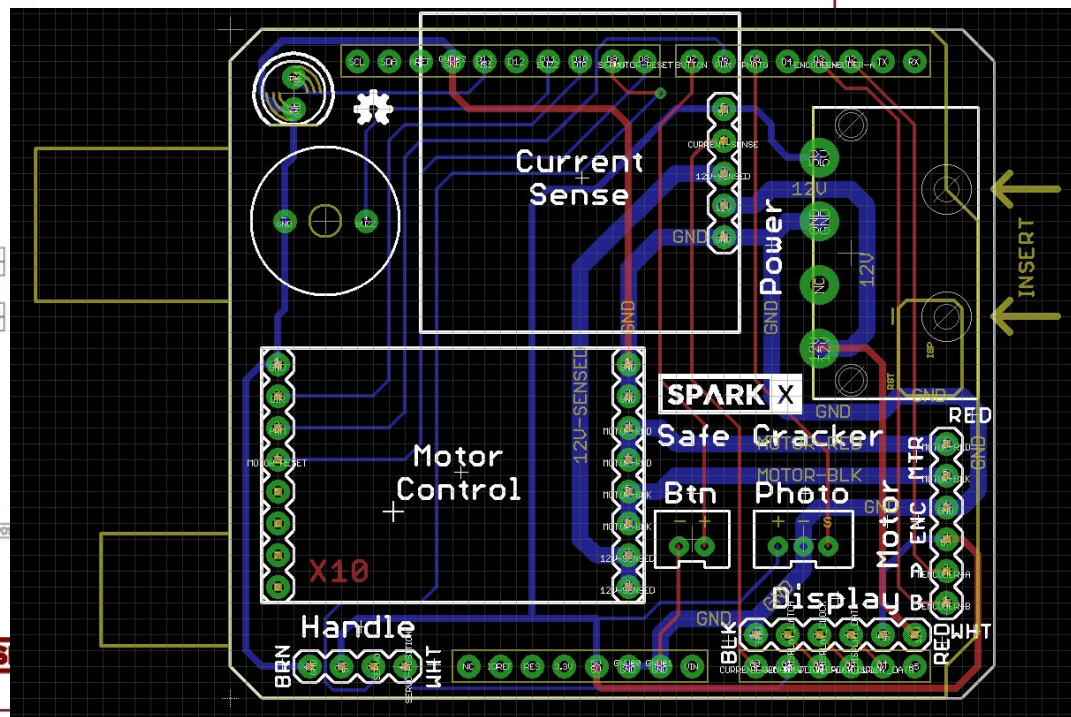
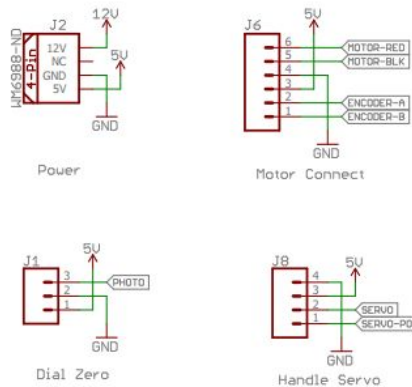
Design by: N. Seidle

REV:
X10

Date: 3/28/2017 8:23 AM

Sheet: 1/1





Problem Domain:

100^3 combinations

10 seconds per test

115 days (worst case)

Combinations:
 100^3 combinations

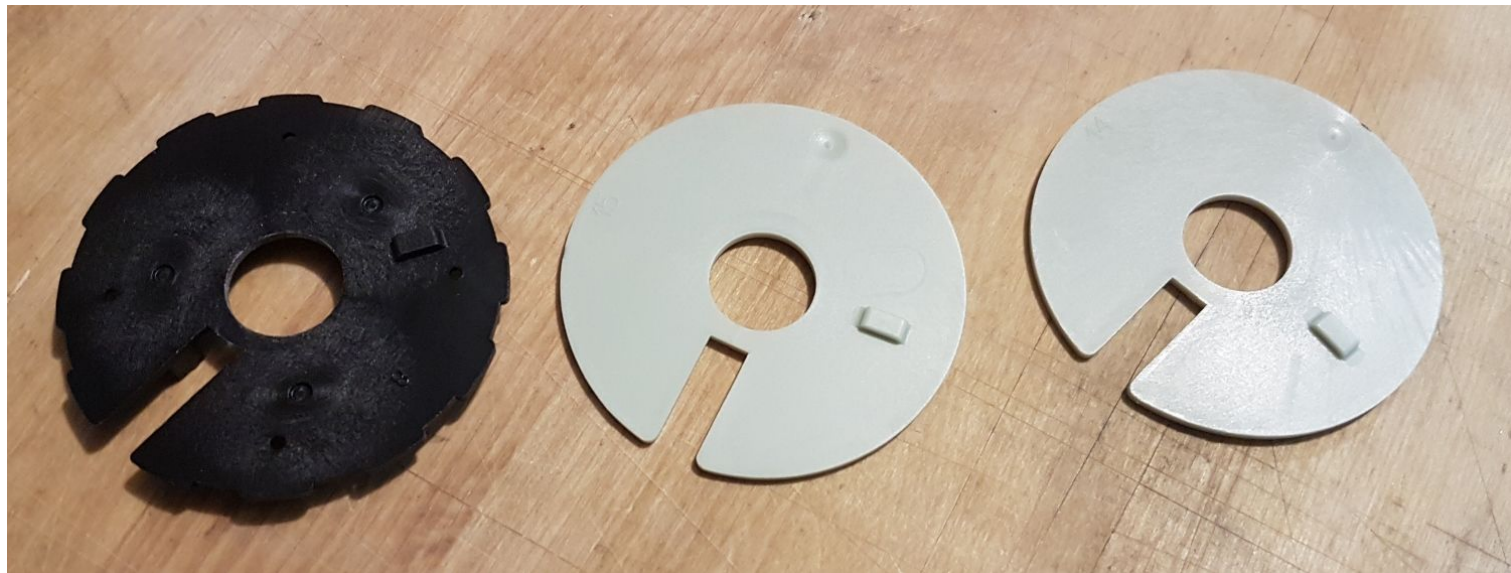
Exploits

Combinations:

~~**100^3 combinations**~~

33^3 combinations = 4.15 days

Exploits



Exploits

Combinations:

~~100^3 combinations~~

~~33^3 combinations = 4.15 days~~

Disc C has 12 indents

$33^2 * 12 = 1.5$ days

Exploits



Disc C:

Outer diameter: 2.815" (71.5mm)

Width of solution slot: 0.239"

Width of 11 indents: 0.249" +/- 0.002"

8.84" (Circumference) / 8400 ticks

0.001" / tick

~10 ticks smaller

Exploits

Combinations:

~~100^3 combinations~~

~~33^3 combinations = 4.15 days~~

~~Disc C has 12 indents~~

~~$33^2 * 12 = 1.5$ days~~

Disc C has a skinny indent

$33^2 * 1 = 3$ hours

Exploits





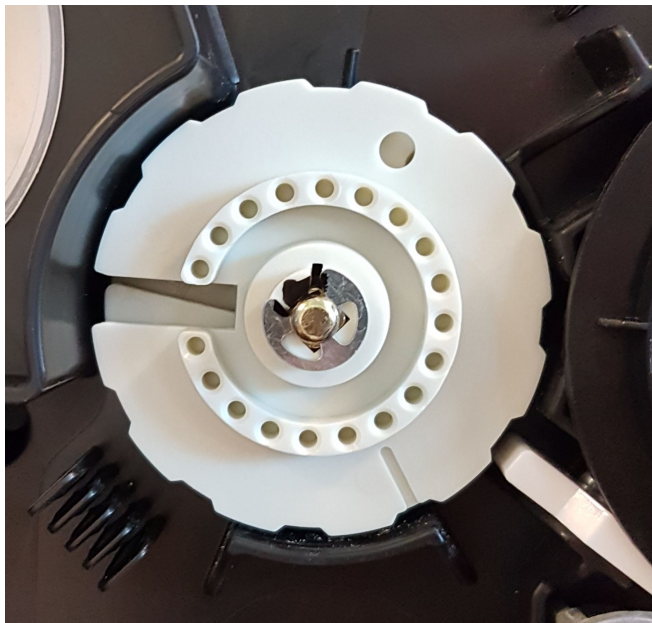












'New' Disc C:

Outer diameter: 2.456" (62.4mm)

Width of solution slot: 0.250"

Width of 11 indents: 0.201" +/- 0.002"

7.72" (Circumference) / 8400 ticks

0.00092" / tick

**~54 ticks LARGER
(5 times easier to hack)**

Exploits



File Edit Setup Control Window Help

6) Set starting combos

7) Calibrate handle servo

8) Test handle button

9) Test indent centers

s) Start cracking

How many measurements would you like to take? (Start with 1)1

Test 1 of 1. IndentNum[0] Encoder[8049] / Dial[96] / Width[474] / Depth[0]

Test 1 of 1. IndentNum[1] Encoder[354] / Dial[4] / Width[485] / Depth[0]

Test 1 of 1. IndentNum[2] Encoder[1051] / Dial[13] / Width[468] / Depth[0]

Test 1 of 1. IndentNum[3] Encoder[1758] / Dial[21] / Width[503] / Depth[0]

Test 1 of 1. IndentNum[4] Encoder[2458] / Dial[29] / Width[478] / Depth[0]

Test 1 of 1. IndentNum[5] Encoder[3153] / Dial[38] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[6] Encoder[3848] / Dial[46] / Width[535] / Depth[0]

Test 1 of 1. IndentNum[7] Encoder[4534] / Dial[54] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[8] Encoder[5248] / Dial[62] / Width[495] / Depth[0]

Test 1 of 1. IndentNum[9] Encoder[5943] / Dial[71] / Width[490] / Depth[0]

Test 1 of 1. IndentNum[10] Encoder[6638] / Dial[79] / Width[484] / Depth[0]

Test 1 of 1. IndentNum[11] Encoder[7344] / Dial[87] / Width[481] / Depth[0]

Largest indent number: 6

Largest indent is now set to test

Indent locations recorded to EEPROM

Press key to continue

File Edit Setup Control Window Help

6) Set starting combos

7) Calibrate handle servo

8) Test handle button

9) Test indent centers

s) Start cracking

How many measurements would you like to take? (Start with 1)1

Test 1 of 1. IndentNum[0] Encoder[8049] / Dial[96] / Width[474] / Depth[0]

Test 1 of 1. IndentNum[1] Encoder[354] / Dial[4] / Width[485] / Depth[0]

Test 1 of 1. IndentNum[2] Encoder[1051] / Dial[13] / Width[468] / Depth[0]

Test 1 of 1. IndentNum[3] Encoder[1758] / Dial[21] / Width[503] / Depth[0]

Test 1 of 1. IndentNum[4] Encoder[2458] / Dial[29] / Width[478] / Depth[0]

Test 1 of 1. IndentNum[5] Encoder[3153] / Dial[38] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[6] Encoder[3848] / Dial[46] / Width[535] / Depth[0]

Test 1 of 1. IndentNum[7] Encoder[4534] / Dial[54] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[8] Encoder[5248] / Dial[62] / Width[495] / Depth[0]

Test 1 of 1. IndentNum[9] Encoder[5943] / Dial[71] / Width[490] / Depth[0]

Test 1 of 1. IndentNum[10] Encoder[6638] / Dial[79] / Width[484] / Depth[0]

Test 1 of 1. IndentNum[11] Encoder[7344] / Dial[87] / Width[481] / Depth[0]

Largest indent number: 6

Largest indent is now set to test

Indent locations recorded to EEPROM

Press key to continue

File Edit Setup Control Window Help

6) Set starting combos

7) Calibrate handle servo

8) Test handle button

9) Test indent centers

s) Start cracking

How many measurements would you like to take? (Start with 1)1

Test 1 of 1. IndentNum[0] Encoder[8049] / Dial[96] / Width[474] / Depth[0]

Test 1 of 1. IndentNum[1] Encoder[354] / Dial[4] / Width[485] / Depth[0]

Test 1 of 1. IndentNum[2] Encoder[1051] / Dial[13] / Width[468] / Depth[0]

Test 1 of 1. IndentNum[3] Encoder[1758] / Dial[21] / Width[503] / Depth[0]

Test 1 of 1. IndentNum[4] Encoder[2458] / Dial[29] / Width[478] / Depth[0]

Test 1 of 1. IndentNum[5] Encoder[3153] / Dial[38] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[6] Encoder[3848] / Dial[46] / Width[535] / Depth[0]

Test 1 of 1. IndentNum[7] Encoder[4534] / Dial[54] / Width[496] / Depth[0]

Test 1 of 1. IndentNum[8] Encoder[5248] / Dial[62] / Width[495] / Depth[0]

Test 1 of 1. IndentNum[9] Encoder[5943] / Dial[71] / Width[490] / Depth[0]

Test 1 of 1. IndentNum[10] Encoder[6638] / Dial[79] / Width[484] / Depth[0]

Test 1 of 1. IndentNum[11] Encoder[7344] / Dial[87] / Width[481] / Depth[0]

Largest indent number: 6

Largest indent is now set to test

Indent locations recorded to EEPROM

Press key to continue

Combinations:

~~100^3 combinations~~

~~33^3 combinations = 4.15 days~~

~~Disc C has 12 indents~~

~~$33^2 * 12 = 1.5$ days~~

Disc C has a large indent

$33^2 * 1 = 3$ hours

Exploits

Test Time:

Resetting Dials = 10s / test

Exploits

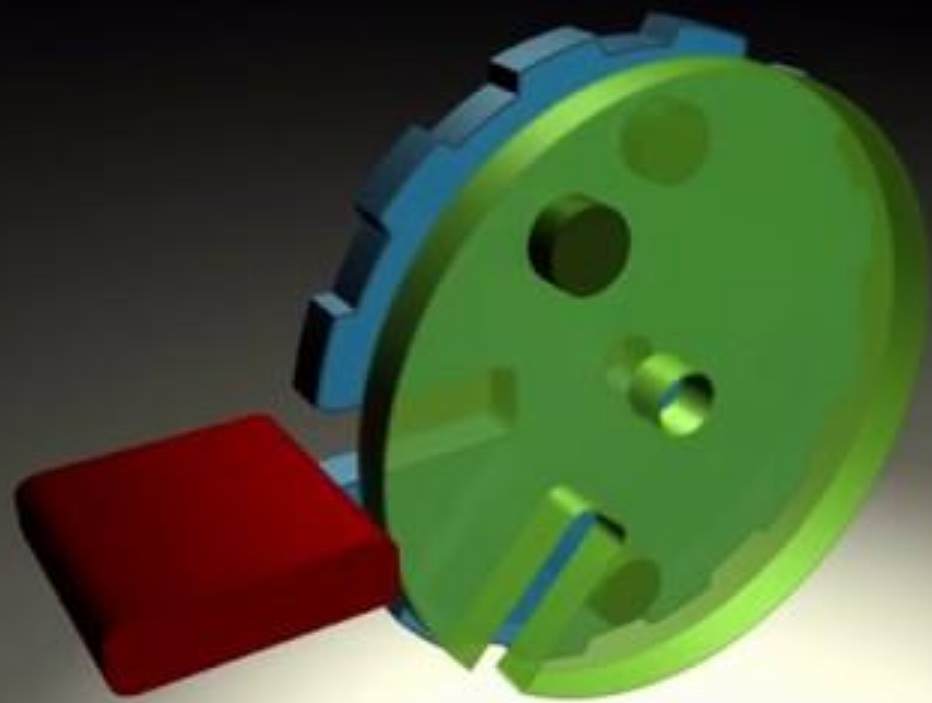
Test Time:

~~**Resetting Dials = 10s / test**~~

'Set testing' = 4s / test

1.2 hours

Exploits





Test Time:

~~Resetting Dials = 10s / test~~

~~'Set testing' = 4s / test~~

~~1.2 hours~~

45 minutes!

~~Exploits~~ **Luck**

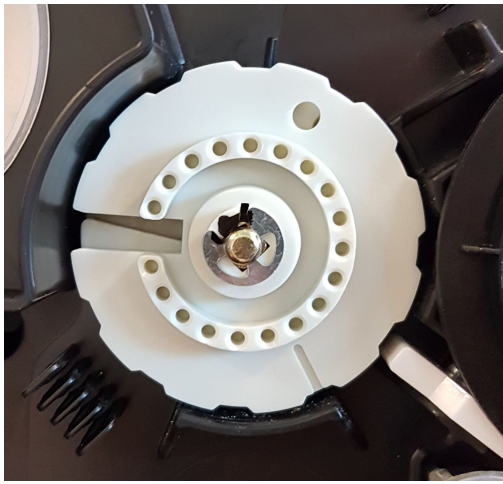
How do I protect myself!?



Credit: starwarsblog.starwars.com



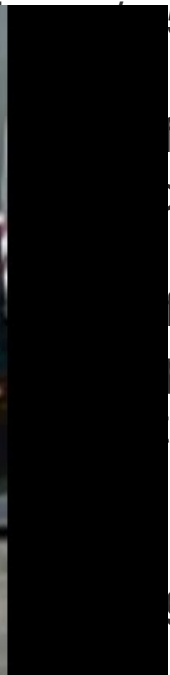
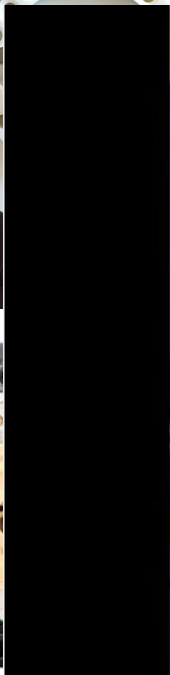
One of these is not like the others...



“The S&G 6730 ... has only a $\pm .5$ dialing tolerance, essentially giving a 1 digit window to hit. While many locksmiths might prefer the S&G 6730, it can be notoriously difficult to open and very unforgiving to human error. In addition, slight alterations to the lock (for example, if the dial or the dial ring was bumped during shipping) can shift the combination, rendering the lock unusable.”

-Hayman Safes: Lock Ratings





5 dialing
window to
fer the S&G
o open and
dition, slight
f the dial or
opping) can
he lock

gs



Future Research

Measuring complete

Smallest to largest width [Width]/[Depth]

Indent 8: [1911] / [1130]

Indent 1: [1925] / [1122]

Indent 3: [1953] / [1091]

Indent 0: [1955] / [1099]

Indent 11: [1966] / [1105]

Indent 2: [1992] / [1100]

Indent 9: [1994] / [1126]

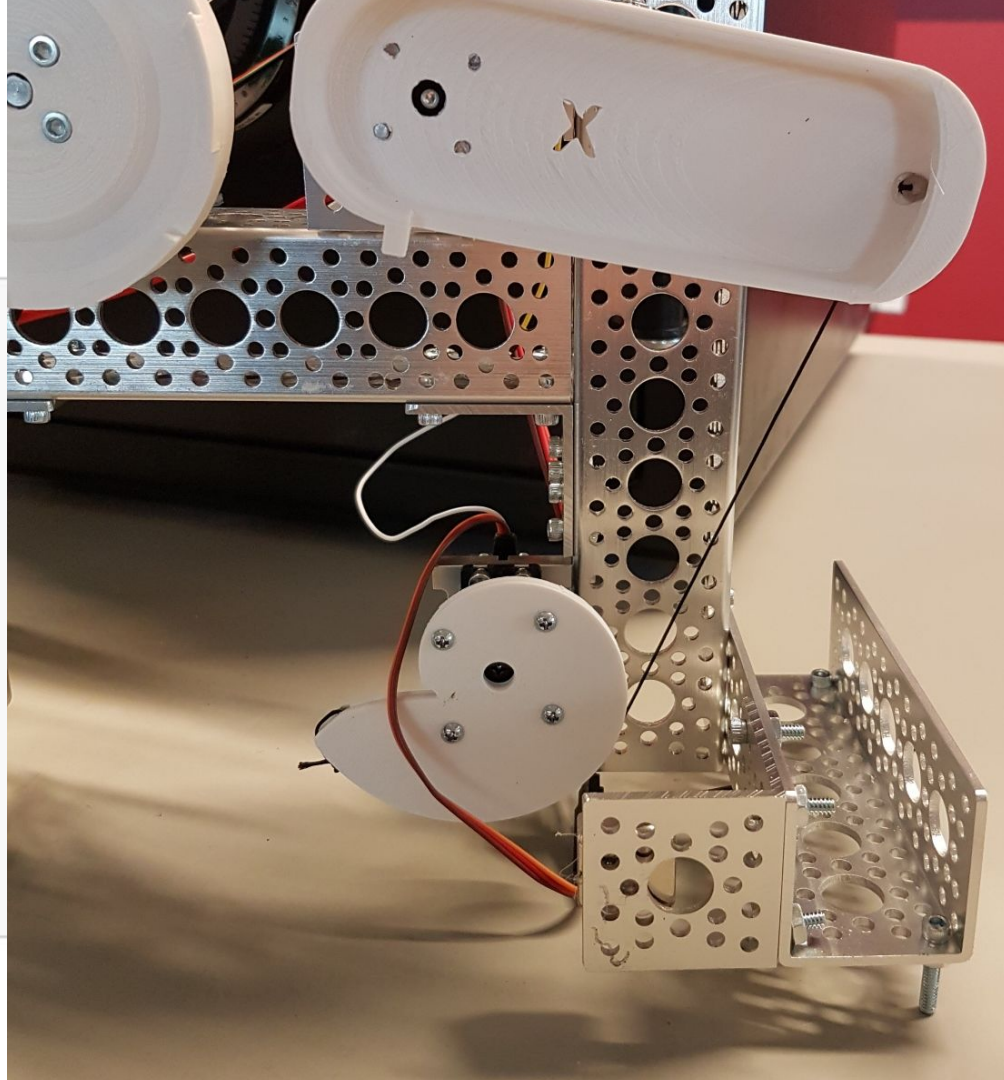
Indent 7: [2011] / [1098]

Indent 10: [2036] / [1096]

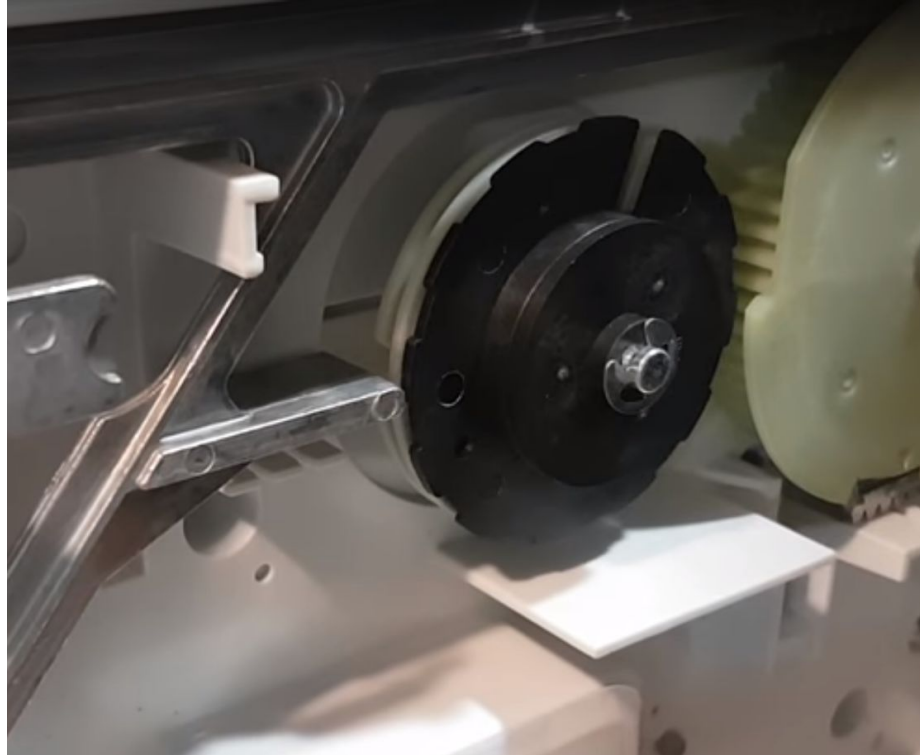
Indent 4: [2077] / [1109]

Indent 5: [2083] / [1100]

Indent 6: [2114] / [1096]



Future Research



Future Research



Credit: iRobot

Future Research



Is it open yet?



nathan@sparkfun.com



Demo fail!