CUTTING TIES OF A VINYL CUTTER

LE HACK
KERNEL PANIC!

virtualabs@mamot.fr

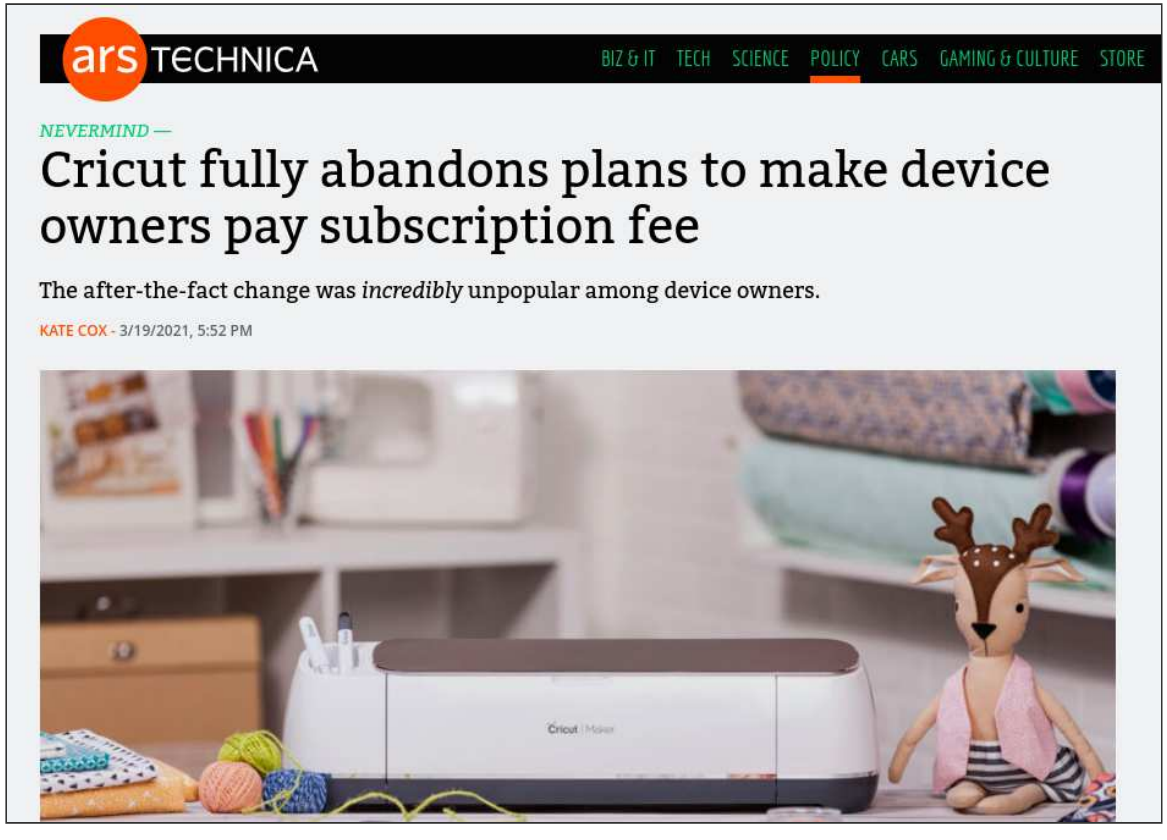
/ME

- Security engineer @ **Quarkslab**
- **Hardware/software reverse-engineering**
- **Streamer** on

WHERE IT ALL BEGAN

CRICUT MAKER

CRICUT MADE A BAD CALL



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

NEVERMIND —

Cricut fully abandons plans to make device owners pay subscription fee

The after-the-fact change was *incredibly* unpopular among device owners.

KATE COX - 3/19/2021, 5:52 PM

source: Ars Technica

AND ROLLED BACK ASAP

The Verge / Tech / Reviews / Science / Entertainment / More +

TECH / CREATORS

Cricut promises unlimited lifetime uploads for existing crafting machines after user backlash

/ Machines registered before December 31st will have unlimited uploads without paying extra

source: The Verge

E-WASTE

r/cricut • 2 yr. ago
by melliferamel

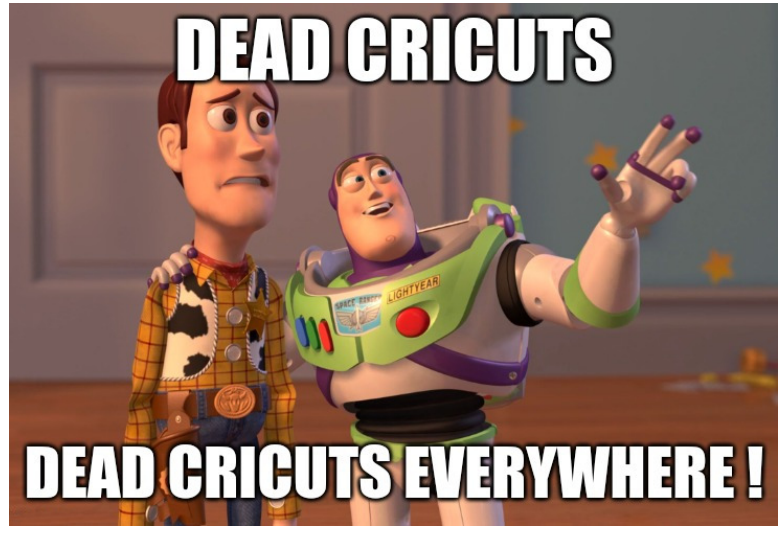
Join

Cricut deactivated machine and tell me to throw it away!

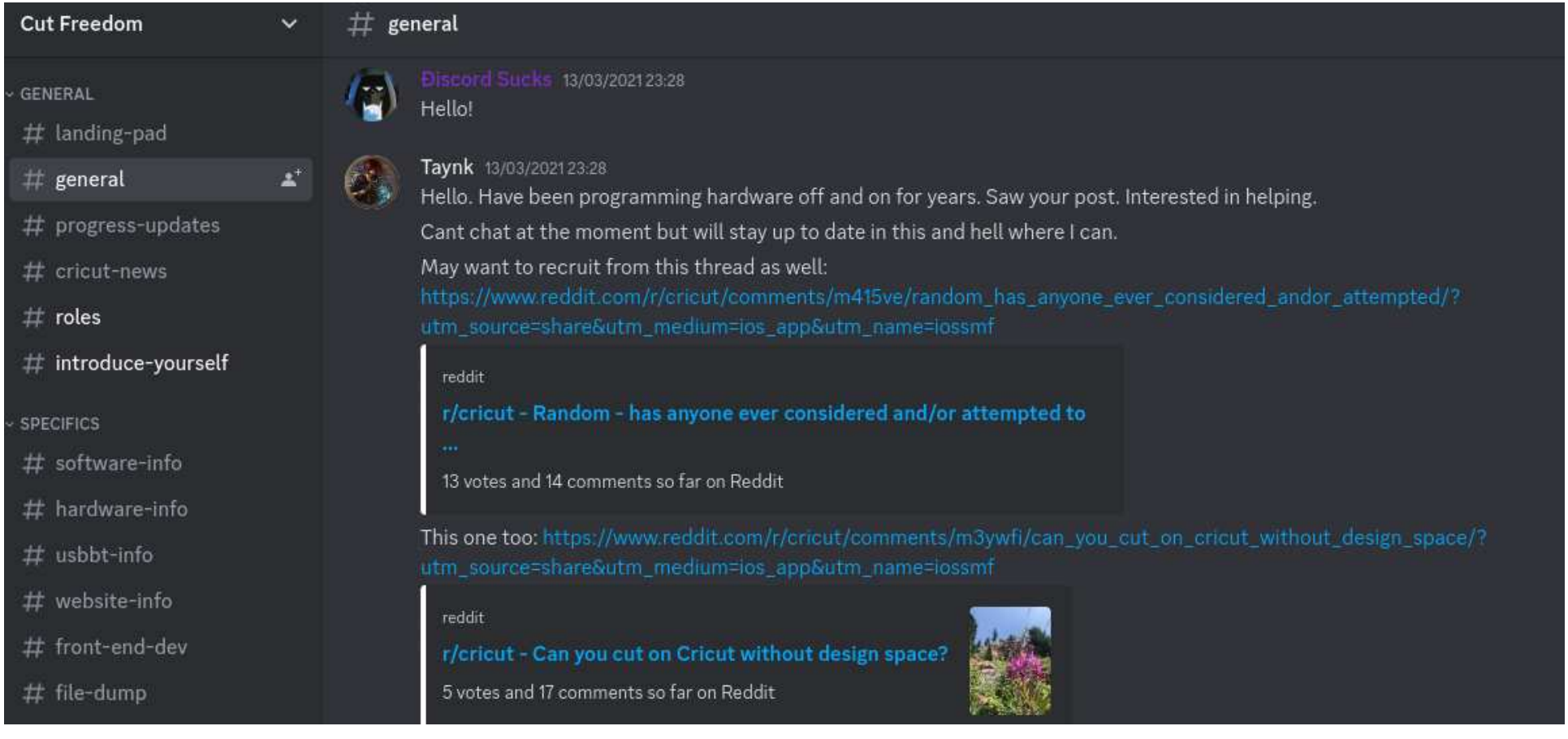
Major vent here about Cricut's customer and environmental policy. I got a Maker from my husband for Christmas and have really enjoyed using it for making cards. Early this month I tried to make some stickers with print and cut and was having so many problems. Recalibrated dozens of times and it would just be randomly off every time.

So I contact customer support and send them a video of my machine working, they deem it a faulty sensor and are sending me a replacement. Hooray! Right?

It takes a few weeks for replacement to be sent and ordered, my machine actually works fine for cutting and I keep making cards up until a couple of days ago when my machine suddenly stops working. I get a message saying "This machine has been deactivated" because it is faulty. Wtf? So they have used a DRM to lock me out of a functioning machine.



BUT IN THE MEANTIME ...



Same motor setup for the mat movement

SoftestVoid 15/03/2021 11:41

@crenn6977 @Brodie hq board picies incoming!

WILSON SONSINI

Wilson Sonsini Goodrich & Rosati
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050

July 29, 2021

Via Online Dissemination

Re: Legal Notice from Cricut to "Freedom from Cricut" Discord Server Participants

Dear "Cut Freedom" (FKA "Freedom From Cricut") Server Participants:

This law firm represents Cricut, Inc. and helps Cricut protect its computer systems, software, and intellectual property from unauthorized intrusions, misuse, infringement, and similar threats. We have learned that certain individuals participating in the discussions on this server are engaged in unlawful activity that poses a cybersecurity and infringement threat to Cricut's systems and intellectual property. To avoid any confusion on your part about what activities are unlawful, we hereby give legal notice to you, and anyone acting on your behalf, to immediately cease and desist from the following unlawful activities that have been discussed on this server:

HOW TO HACK DESIGN SPACE FOR 30€

THE PLAN

TWO OPTIONS

- **Keep the Cricut firmware** and create a **new open-source client**

- Create a **custom firmware** compatible with **existing cutting software**

OPTION #1: KEEPING THE FW

😡 Communication is encrypted with **a secret key (IP)**

Cricut **can update** the protocol **at any time**

😡 We cannot develop **new features**

DMCA STRIKE

This is an open letter to Cricut Inc.

Hello, and thanks for checking out this project!

I built this project to help with my specific use case: First: I wanted to easily use my Cricut offline, without any account. Second, I wanted to more easily itterate on cutting SVG-based files rather than repeatedly re-uploading to Design Space.

This project is not a threat to your services business model. To use this software, somebody has to download it from Github (which is not non-programmer friendly), figure out how to extract AES keys, accept the "doom and gloom" warnings this software presents, navigate this software's weird UI (which I deliberately made dark and vaguely hacker-y), and supply SVGs that they've created in some other software package (Some of this might improve over time, but it won't improve by much). And that's assuming that this program doesn't crash first. **The demographic who will tolerate all this is not the same as the demographic who is going to pay you a subscription for services.** This is software for tinkerers and people with ideological opinions about free software. It is not designed to compete with your services business (It's also GPL licensed, which is a poison pill for anybody *else* looking to use this commercially).

OPTION #2: OPENSOURCE FW

🤩 No encrypted communication protocol

We control everything

We can implement new features !

🤔 Programming interface must be available

NEXT STEPS

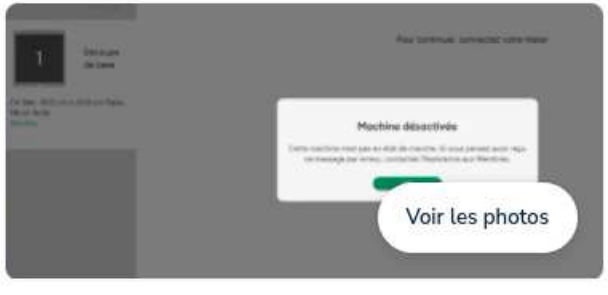
1. Reverse-engineer the **printed circuit boards**

2. Find a way to **program the micro-controller**

3. **Write some code** to drive motors, LEDs, buttons and sensors

4. **Customize GRBL** to fit the board

OH, AND I NEED A CRICUT MAKER



L

Lily
12 annonces
★★★★★ (42)

Profil recommandé

Répond généralement en 30 minutes

Acheter

Message

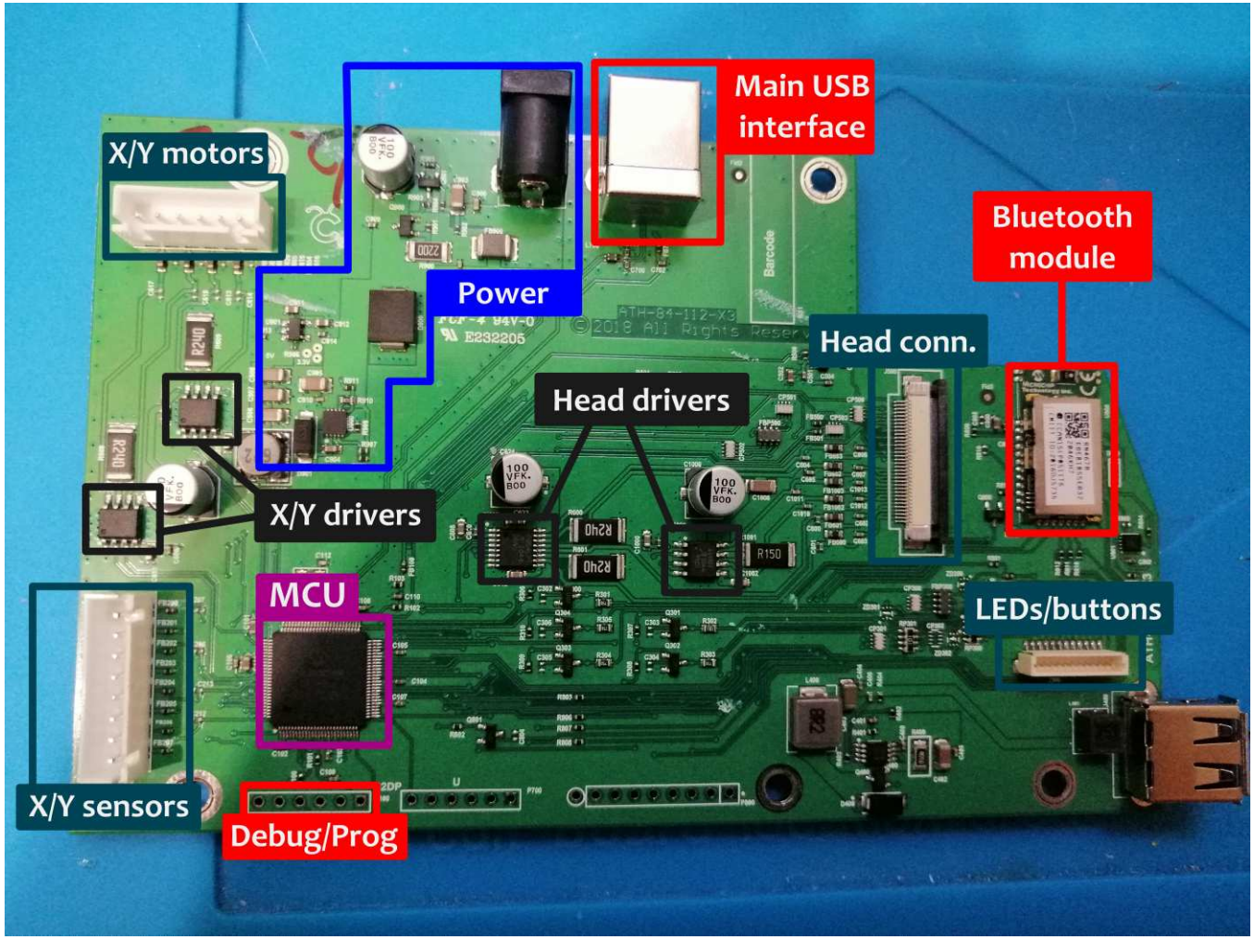
Machine Cricut Maker désactivée

100 € Livraison : à partir de 10,99 €

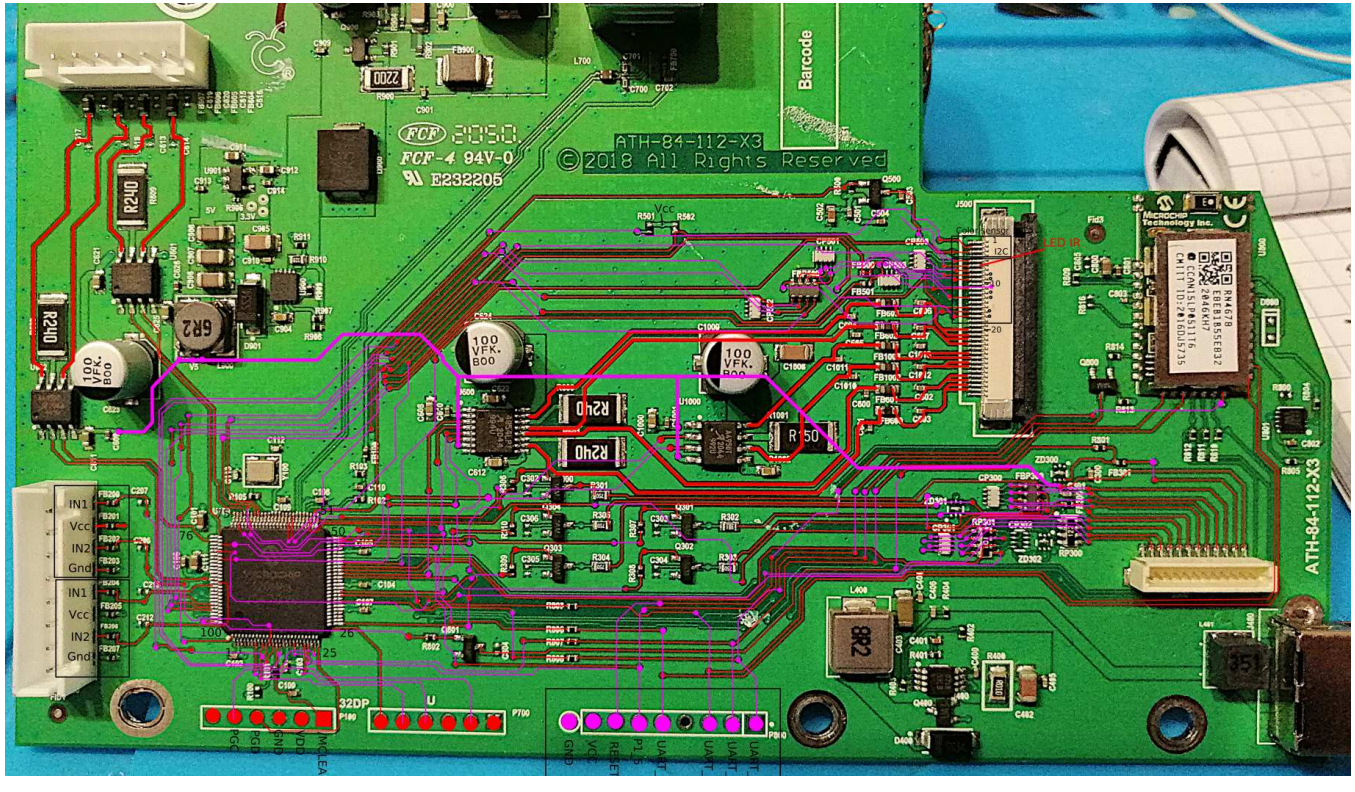
20/05/2023 à 11:22

REVERSE-ENGINEERING

PCB BREAKDOWN



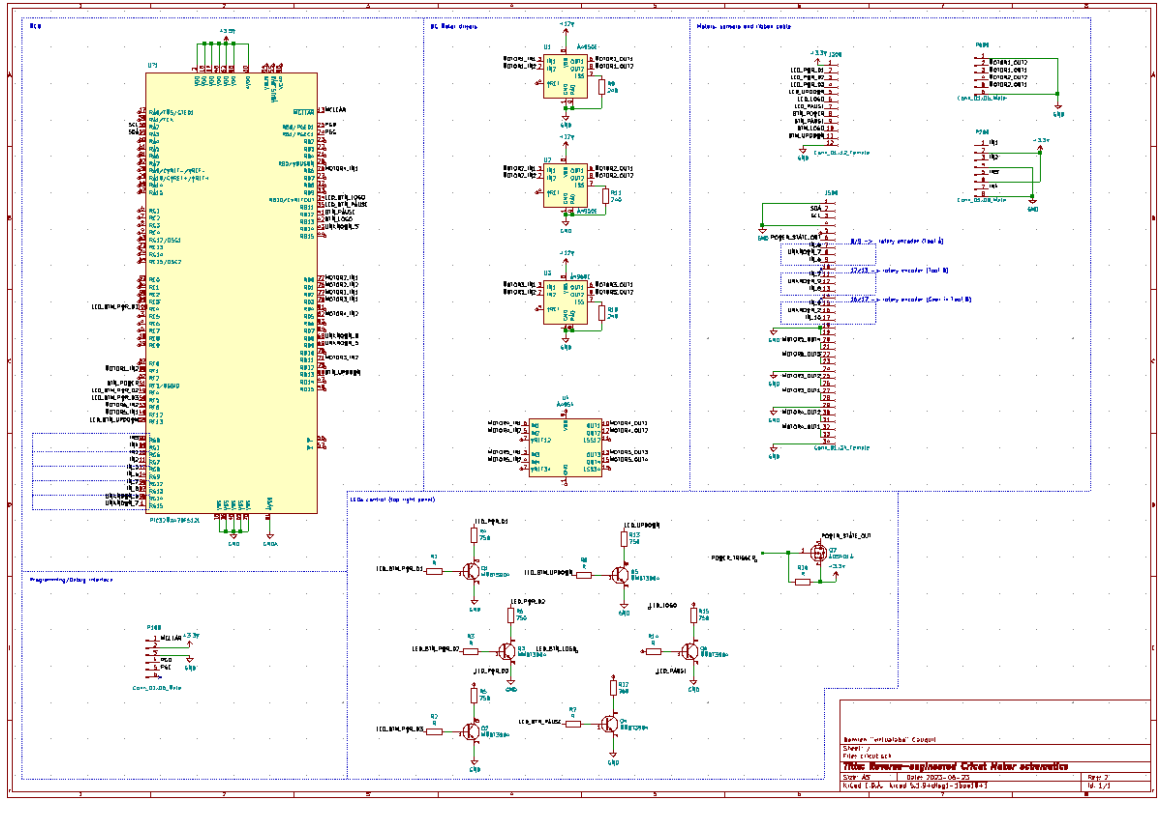
RECOVER ALL THE TRACKS !



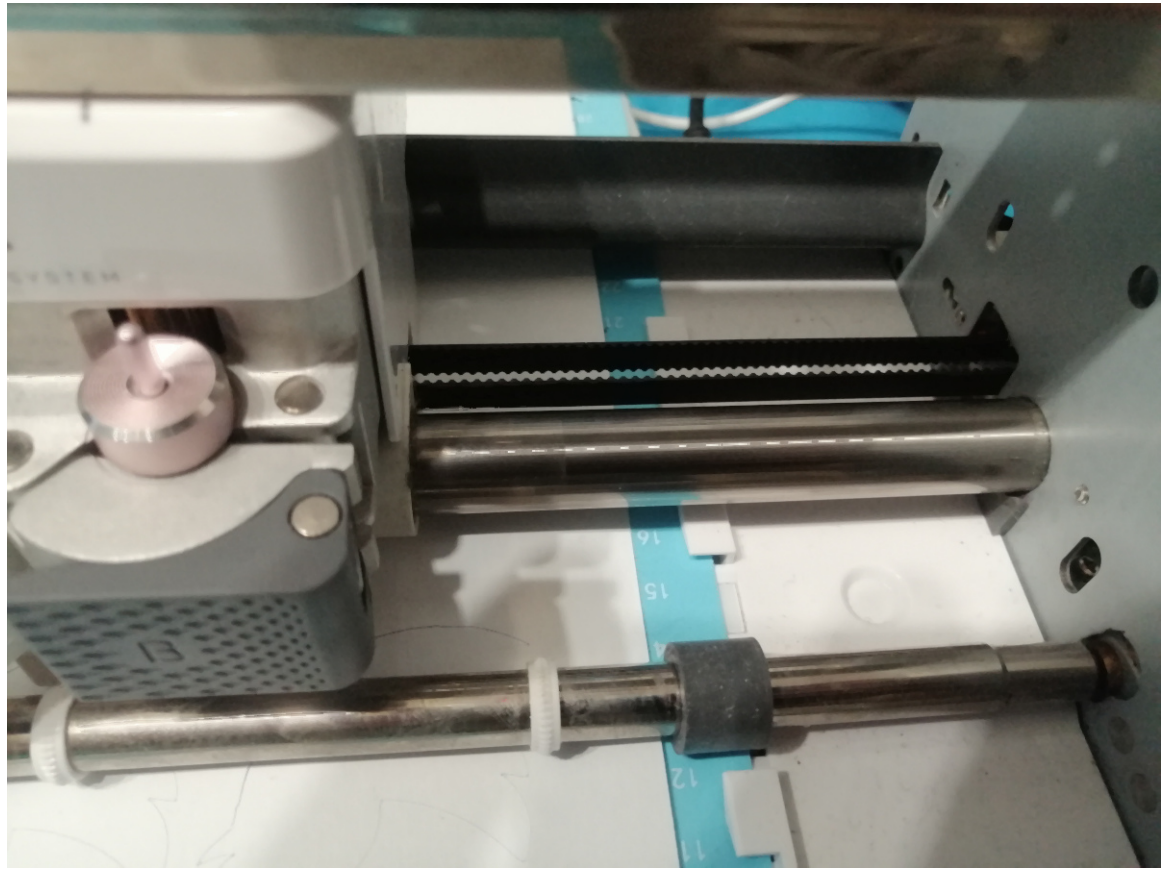
MCU IDENTIFICATION

- **Custom markings**
- Discord server mentionned a **PIC32**
- Matching MCU: **PIC32MX470F512L**

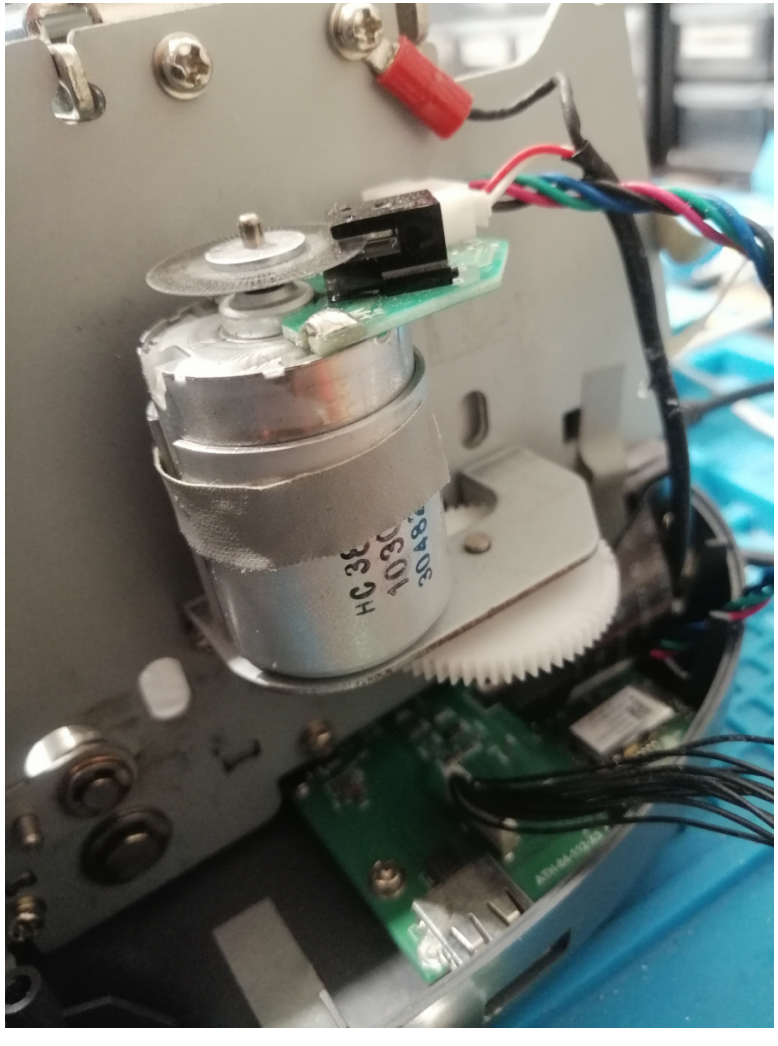
SCHEMATICS (PARTLY) RECOVERED

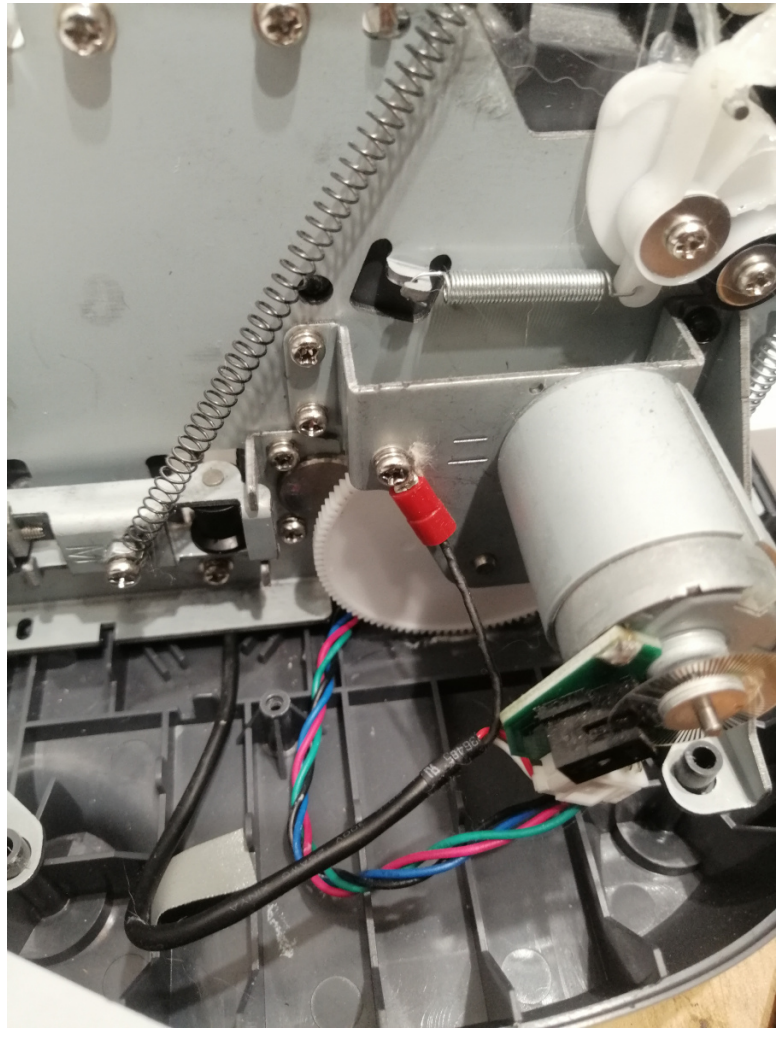


GEARS, BELT AND MOTORS

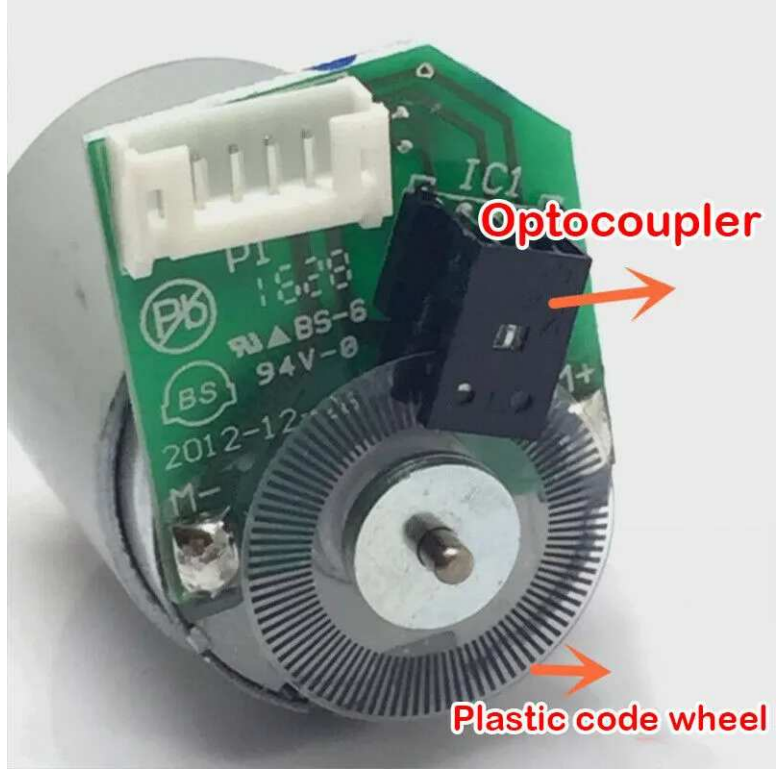


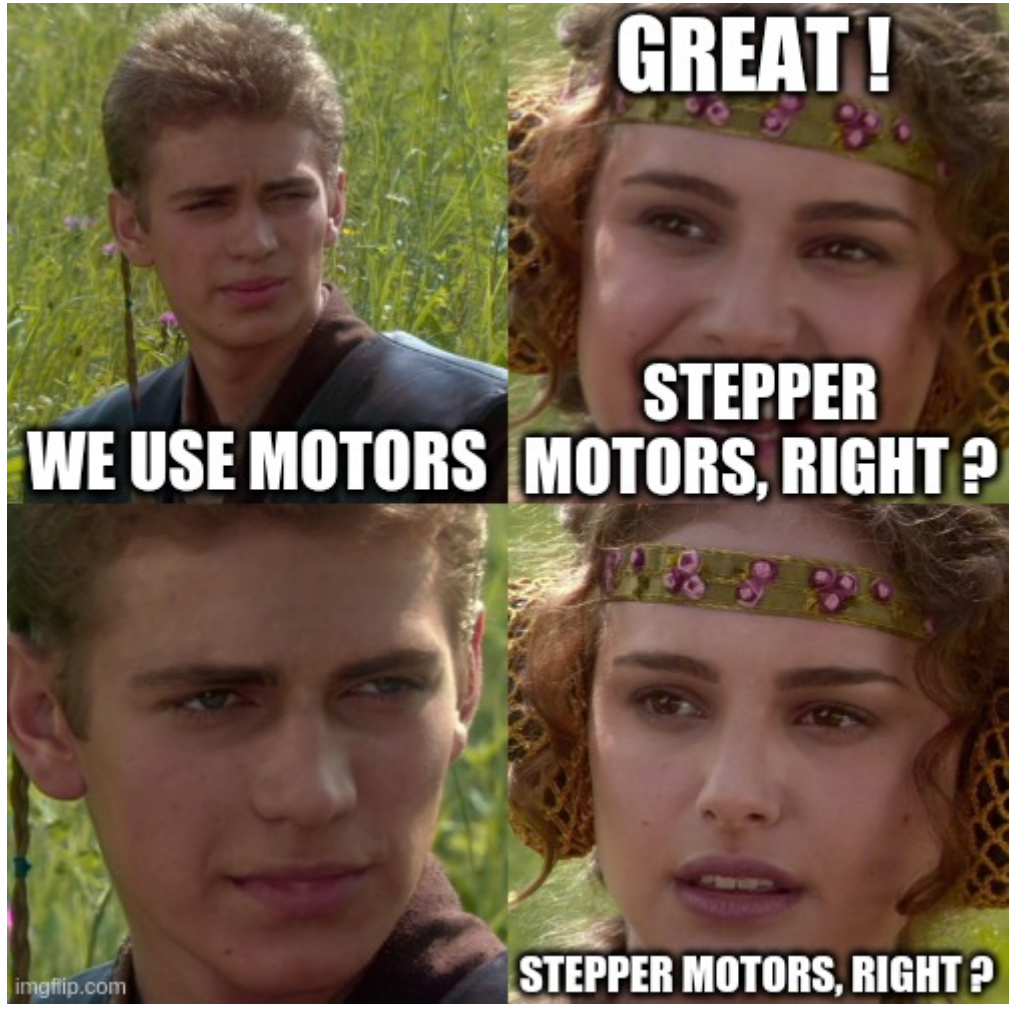
GEARS, BELT AND MOTORS



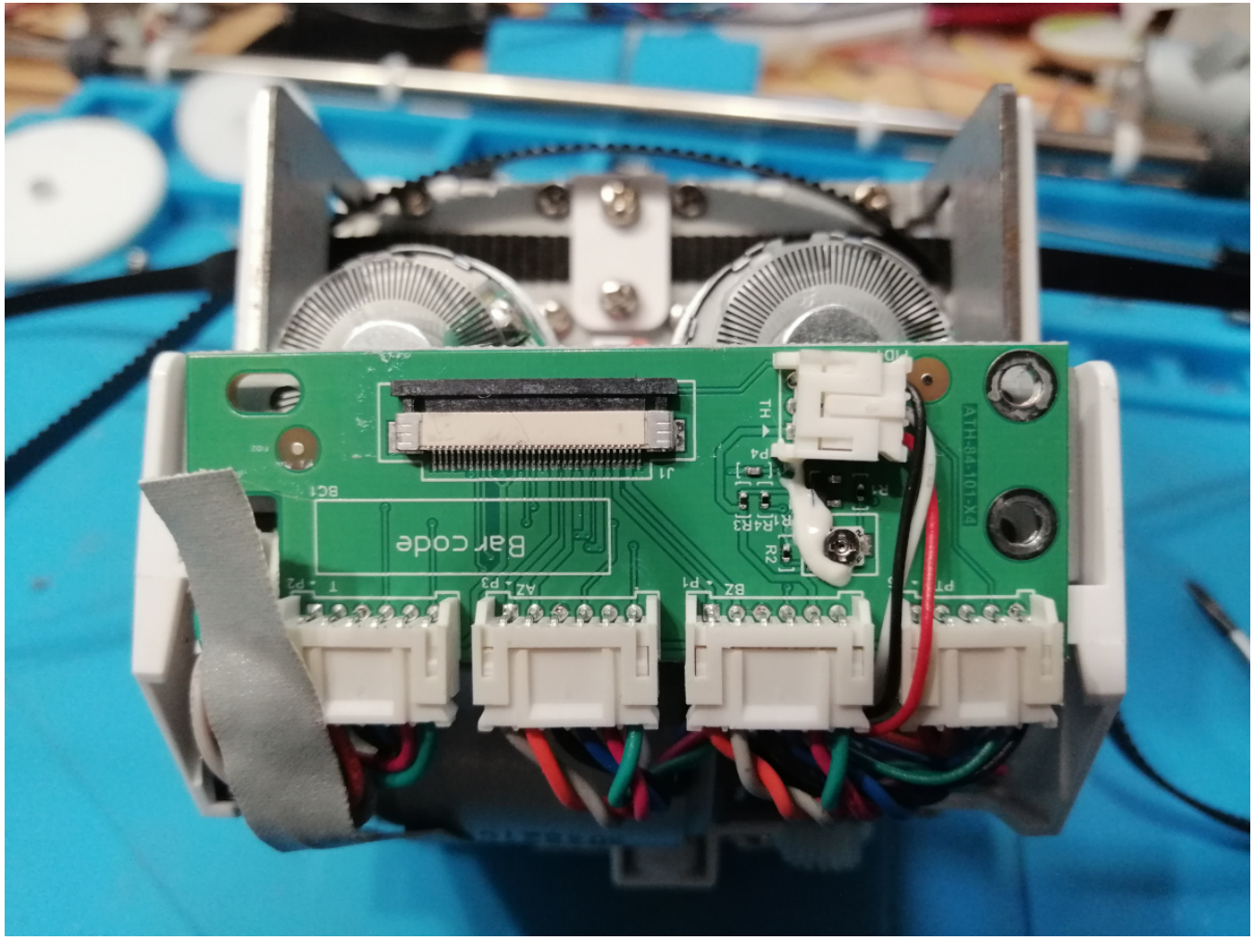


MOTORS




WE USE MOTORS
GREAT !
STEPPER MOTORS, RIGHT ?
STEPPER MOTORS, RIGHT ?
imgflip.com

TOOL HEAD PCB

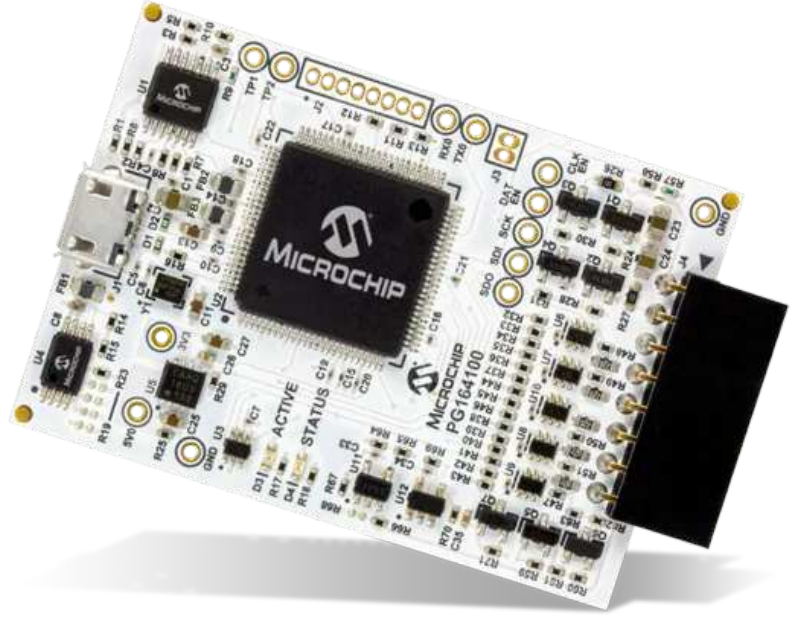


WE KNOW THINGS

- How **electronics work** on the Maker
- How **X and Y axes** are driven
- How the **tool head** works

PUTTING GRBL INSIDE THE MAKER

PROGRAMMING/DEBUGGING



PORTING GRBL TO OUR PIC32

- **GRBL** supports almost everything
- Multiple **challenges** 😨
- **Designed for AVR**, not PIC32

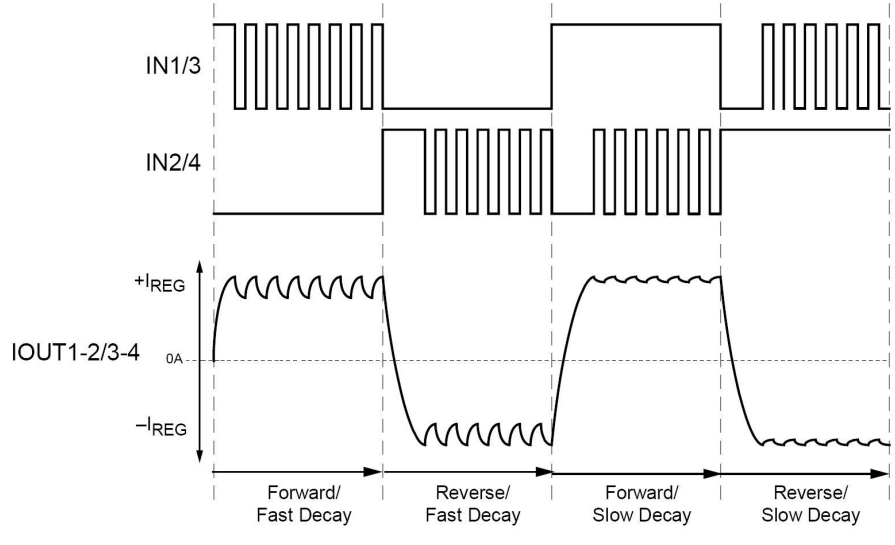
SERIAL COMMUNICATION

- Microchip **USB CDC ACM example** is a PITA

- Did **some hacks** to interface with existing **AVR's UART code**
- Works pretty fine and **allows easy debugging**

DRIVING MOTORS

- PWM frequency is **20 kHz** to avoid **weird buzzing**
- Driven through **PWM in slow decay mode**

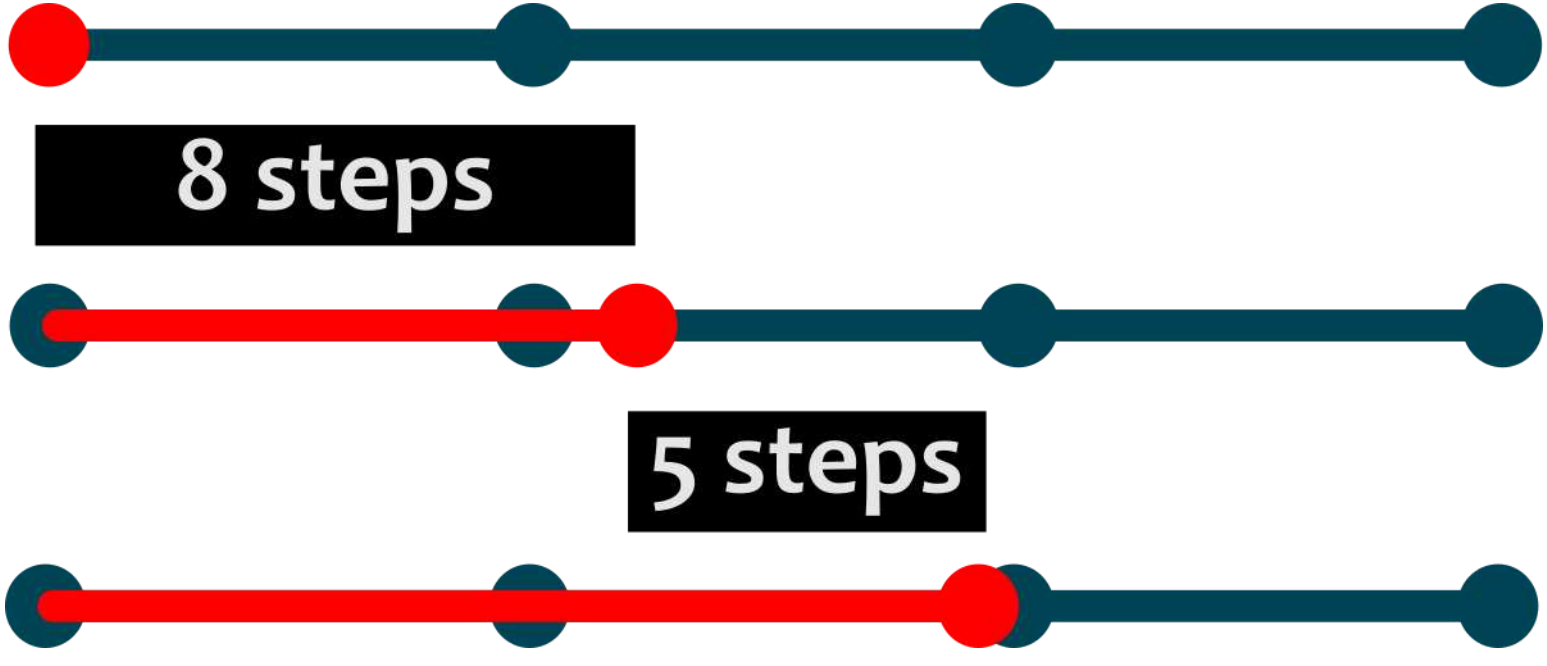


DC MOTORS AS STEPPERS

- Force **small moves (steps)** with DC motors
- We have to deal with **inertia**
- **Precision is pretty bad** (not real stepper motors 🤬)

POSITION HACK FTW

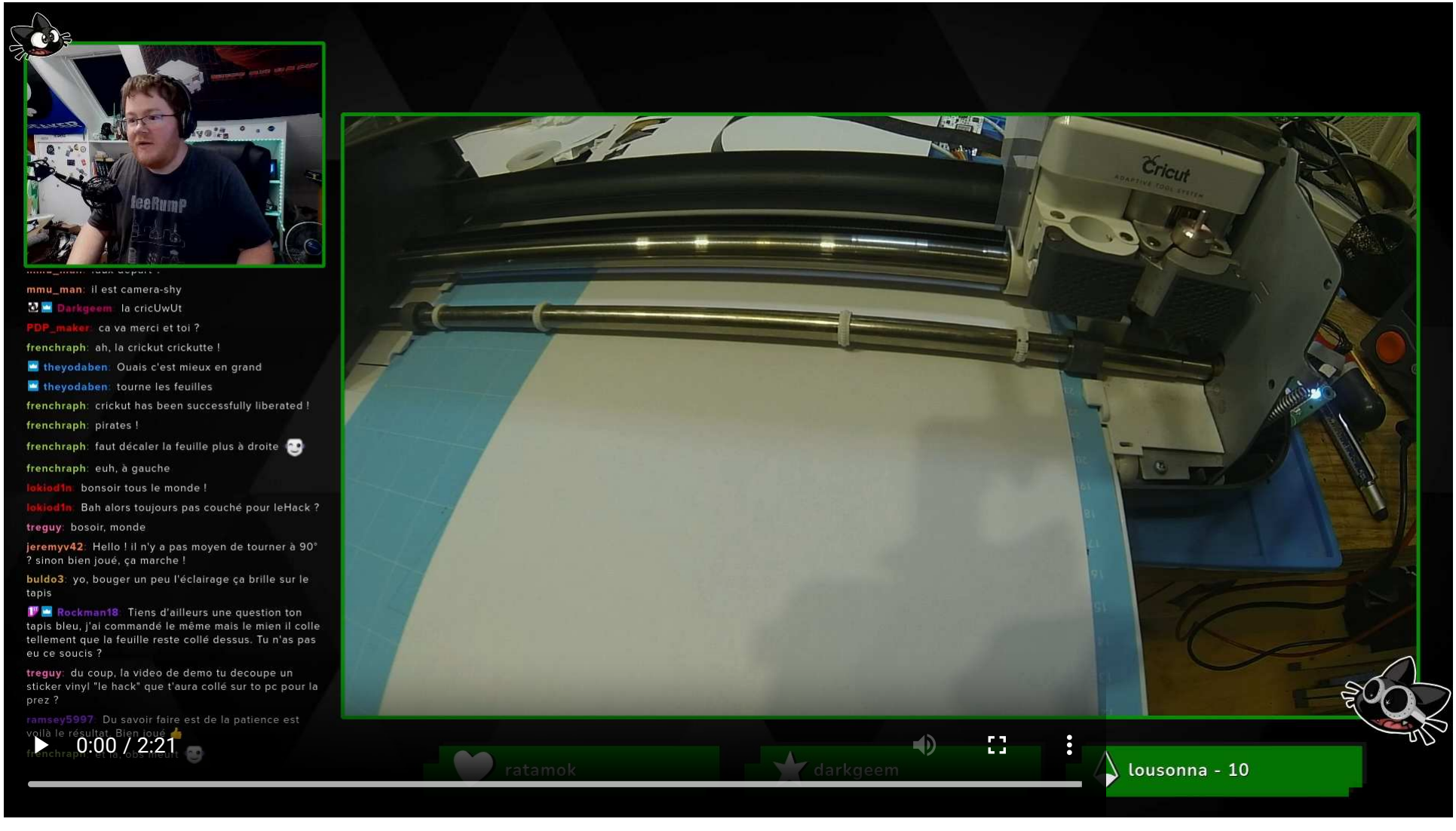
(POOR MAN'S PID)



DETECTING MOTOR STALL

- **No endstops**, deal with it
- We have **quadrature encoders**, that's neat 👍

AFTER COUNTLESS HOURS ...



A MATTER OF TIME

- Roughly **100 hours** spent on this project
- Streamed **live on Twitch**
- A lot of **fails** 😅

FREE ALL THE HARDWARE !

WE BUY, WE OWN !

boulanger

Magasin Compte Panier

Produits

Rechercher...

Accueil > Informatique - Tablette

Machine de découpe **Cricut** Pack Maker 3 + 3 lames

Réf. 1190380

Produit neuf

(0)

549,99€

0.90€ d'éco-part.

Ajouter au panier

Ou payer en plusieurs fois par carte bancaire.

En savoir plus

3x 4x Apport de **150.37€** puis **3x137.5€**. Coût du financement: **12.87€**. TAEG Fixe de 21.01%.

Consulter la disponibilité en magasin

✓ Retrait magasin ou drive - offert

Choisir mon magasin

✓ Livraison chez vous **dès lundi 03 juillet**

Vérifier mes options de livraison

LOCKING USERS IN

- Vendor can **remotely deactivate** any machine
- Machine is **damn expensive**
- Users must use some kind of **crappy software**
- This is **deliberate**, users are not well informed

VENDORS,
WHAT YOU SHOULD BE DOING

- Sell **hardware** that uses **well-known protocols**
- Provide your official (**optional**) application
- Sell **quality** supplies and accessories

HARDWARE HACKERS, WHAT YOU SHOULD BE DOING

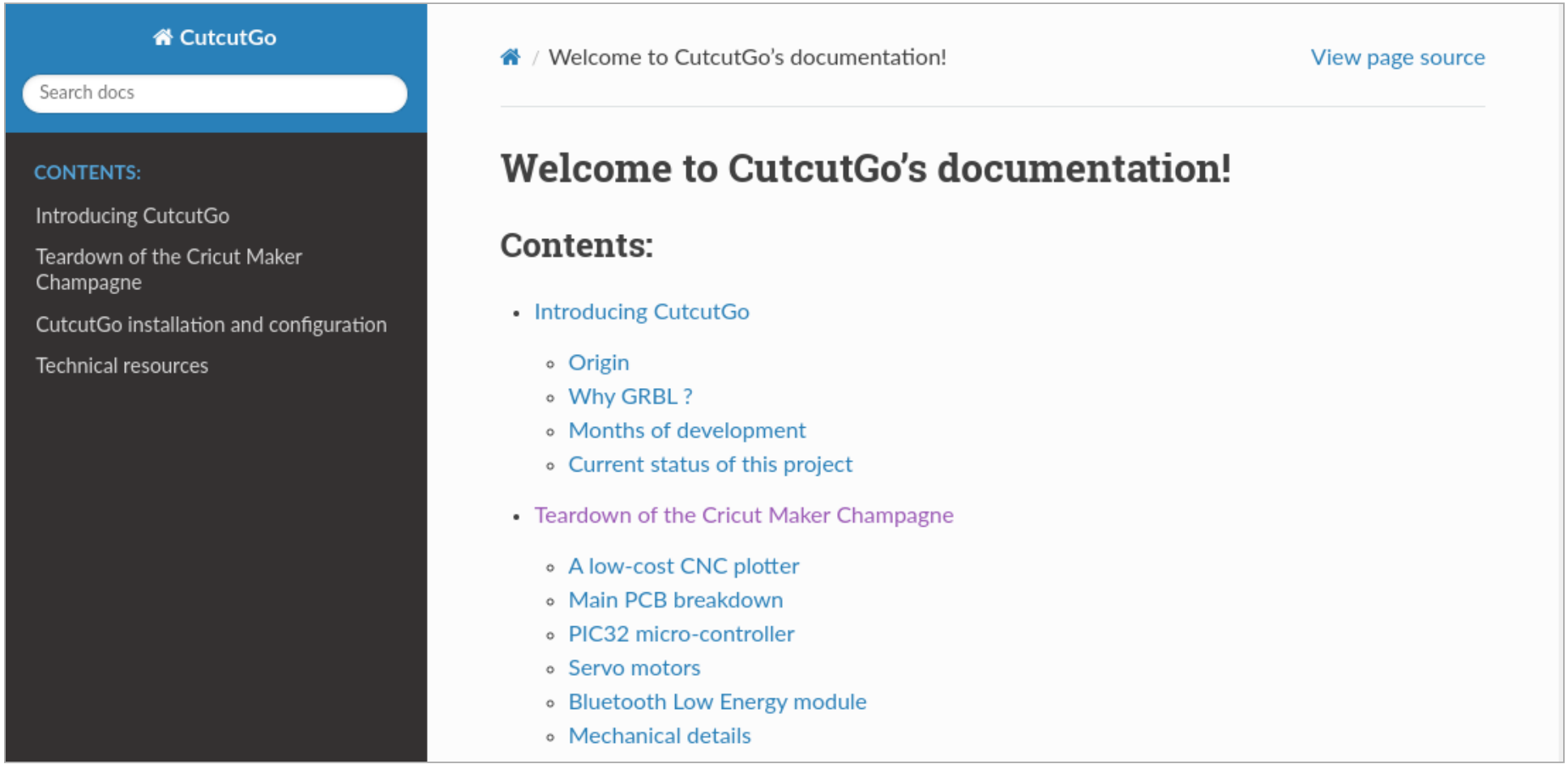
- **Reverse** popular closed-source hardware
- **Create and publish** compatible open-source firmware
- Use and improve **well-known communication protocols**

CONCLUSION

THE MAKER IS (ALMOST) FREE !

- Can be used **offline**, without subscription
- Could work on **Linux/Windows/Mac**
- **Community-driven** features and software

DOCUMENTATION / SOFTWARE



https://virtualabs.github.io/cutcutgo/

STILL A LOT OF WORK

- Modified version of **InkCut** in the pipe
- USB-based **firmware upgrade**
- **Bluetooth Low Energy module** support
- **Front LEDs and buttons** support

CONTRIBUTE !

REMEMBER:

HACK ALL THE THINGS !

THANKS, QUESTIONS ?

@virtualabs@mamot.fr

@virtualabs (DM only)

virtualabs