Hardware Reverse Engineering 101

By John Norman
LayerOne 2013

Basic Principles

- Reverse engineering is the process of figuring how something works, “ the rules of the game”
- We must understand the rules of the game before we can modify them.

Basic Principles

- This information used to be published (schematics, repair guides, etc.)
- These are now considered “Intellectual Property” and usually not disclosed.

What can we do with this?

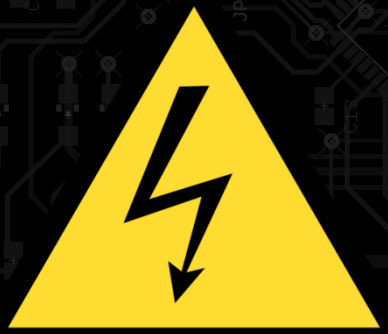
- Repair otherwise non-repairable items
- Modify our stuff
- Cheaply source parts
- Learn better ways to design our own projects.

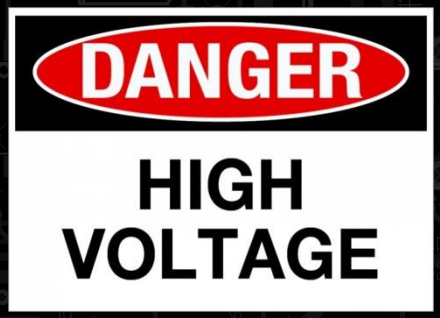
Safety

- High voltage is our greatest danger
  - >50V on dry skin is dangerous
  - Wet or broken skin much more dangerous
  - Possibility of shock, electrocution, arc burns

Safety

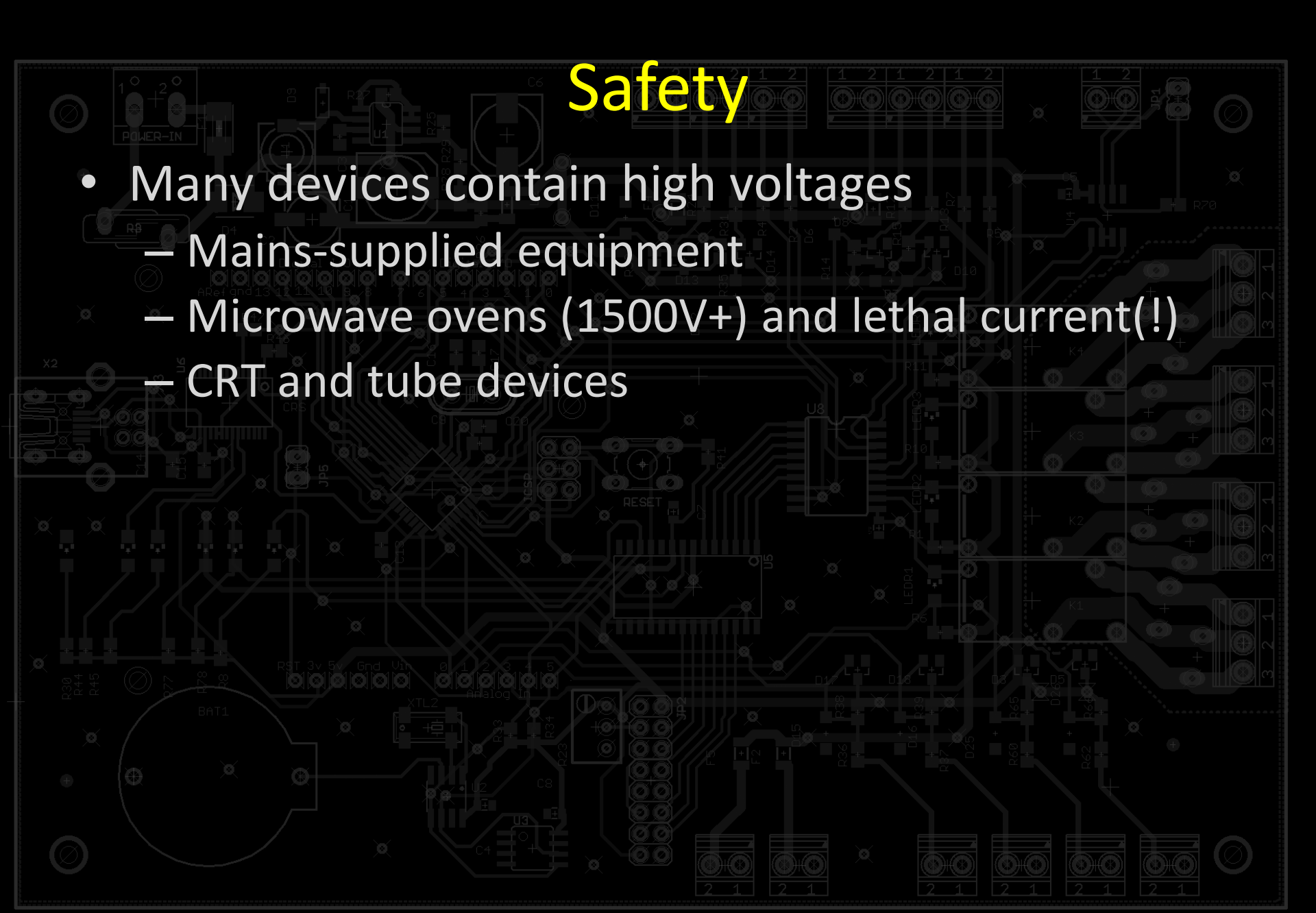
- Things to watch out for
  - Warning labels
  - Thick insulation
  - Shielding





Safety

- Many devices contain high voltages
  - Mains-supplied equipment
  - Microwave ovens (1500V+) and lethal current(!)
  - CRT and tube devices



Safety

- Power off equipment and discharge capacitors
- Wear rubber-soled shoes
- Keep one hand in pocket at all times
- Use insulated tools

Tools of the Trade

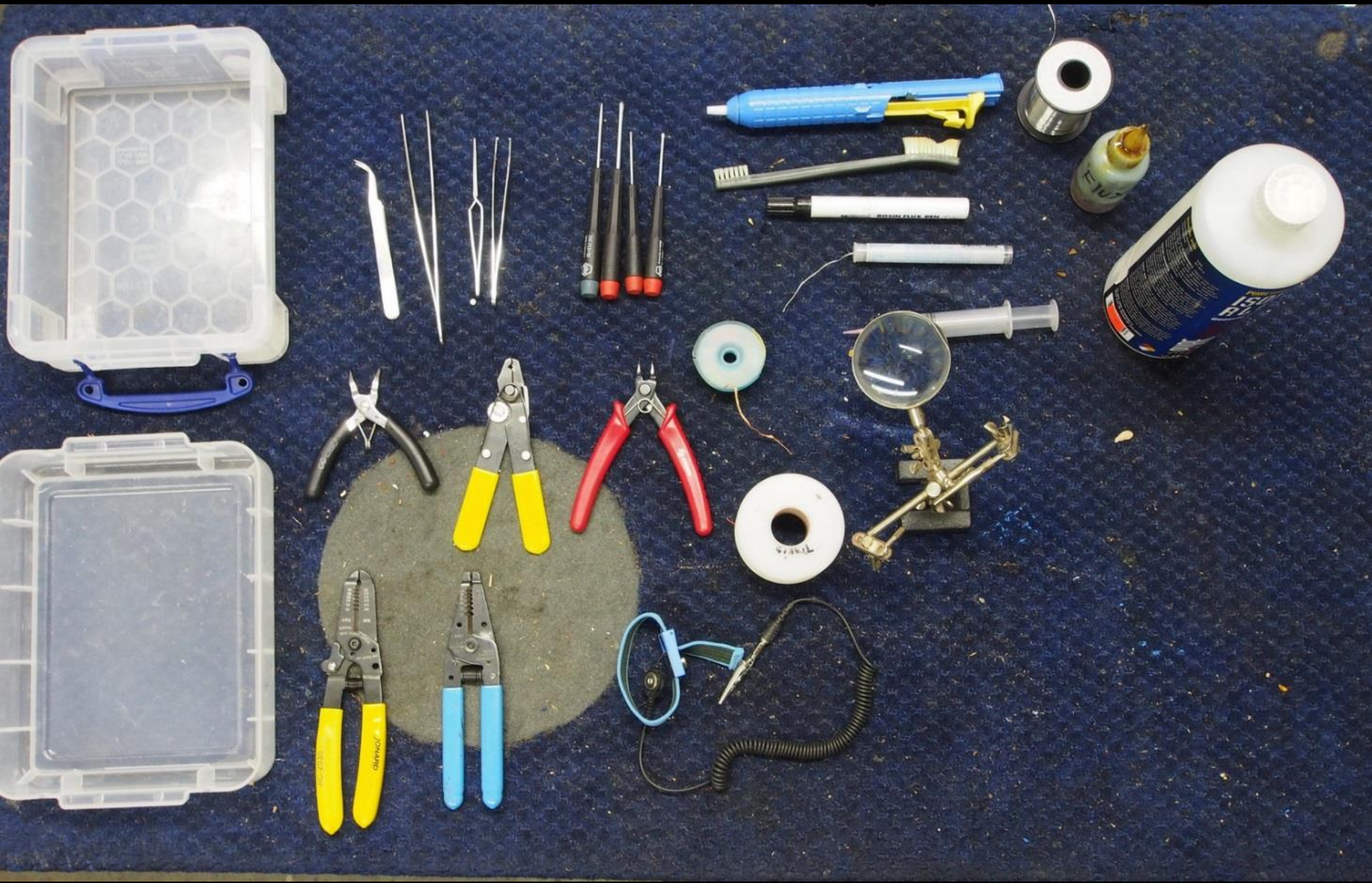
- Disassembly/Assembly
  - Standard screwdrivers
    - Philips #1-#3
    - Flat-blade
  - Small screwdrivers
  - Security driver set (torx, security hex, etc)

Tip: Buy high-quality tools! (Klein, Wiha, etc.)

Tools of the Trade

- Disassembly, modding,
  - Guitar picks , saw blade (case spreading)
  - Sockets/drivers/wrenches
  - Pliers, tweezers
  - Wire strippers (gauge-specific)

Tip: Use a heat gun to soften glue



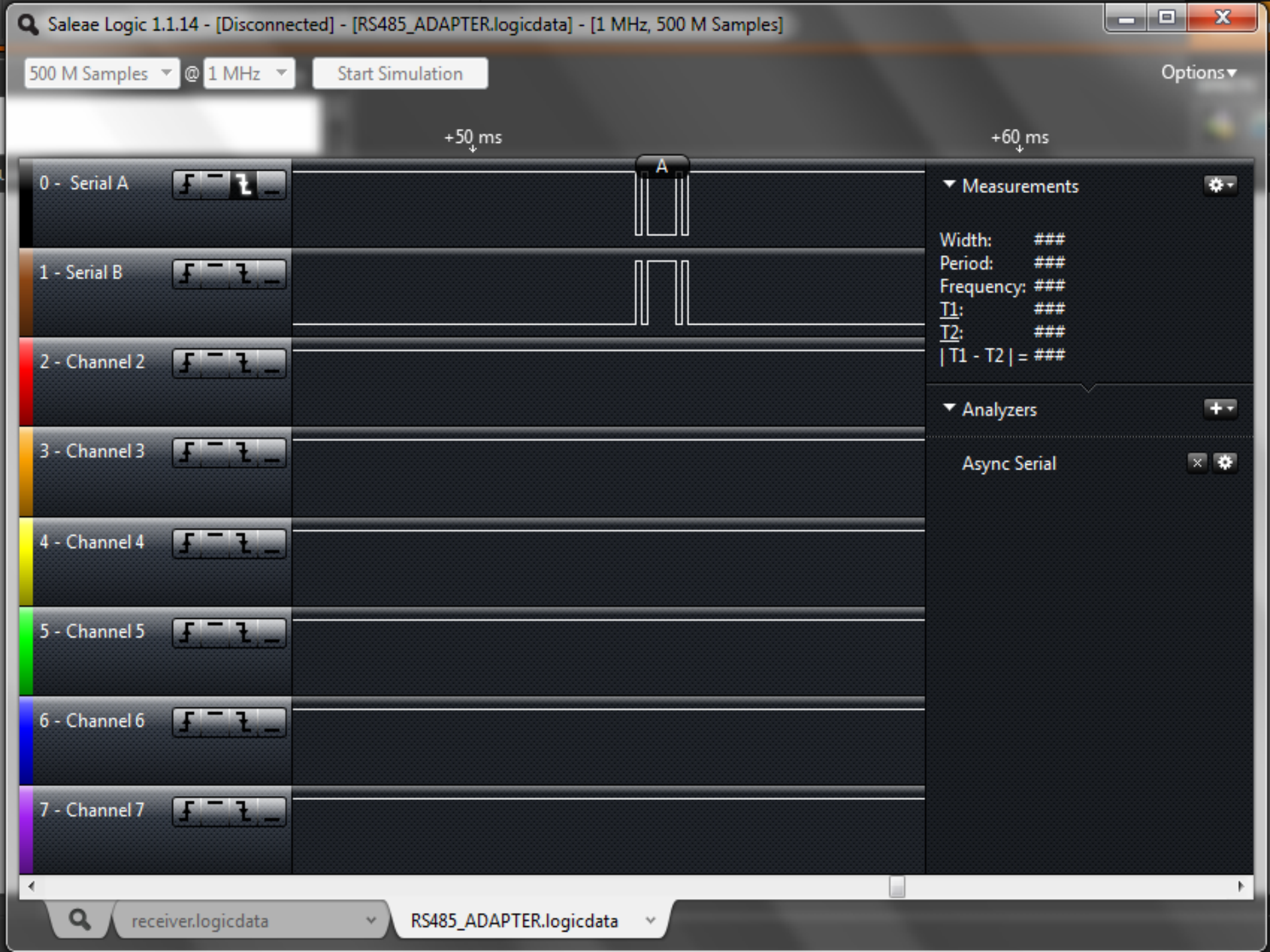
Tools of the Trade

- Test and Measurement
  - Multimeter
    - Measure AC/DC voltage, continuity, resistance
    - Cost: $10-$200
  - ESR Meter
    - Test capacitors in-circuit (#1 cause of dead gear!)
    - Cost: $50-$500


GoldStar
04.99

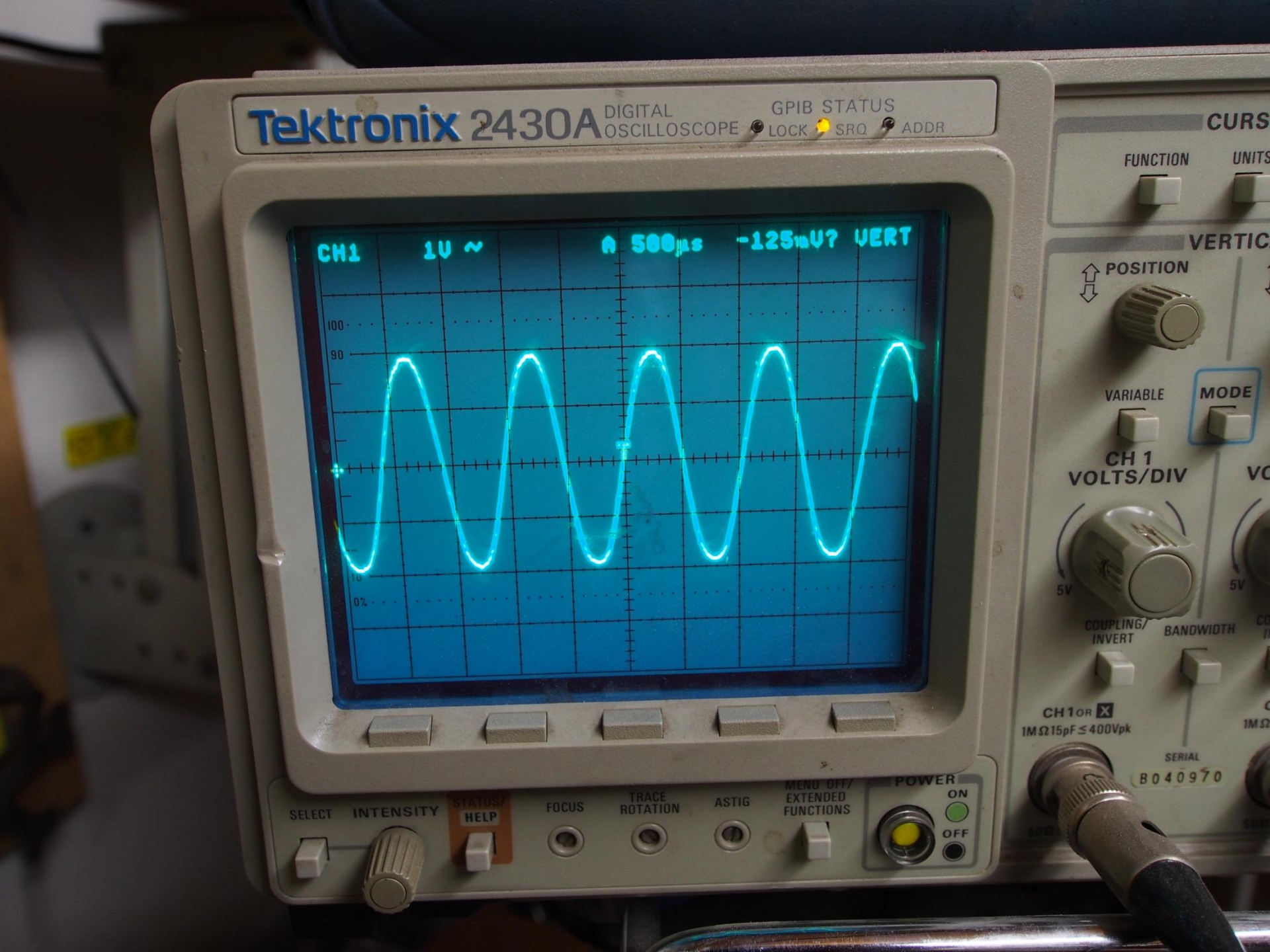
Tools of the Trade

- Test and Measurement
  - Logic analyzer
    - Perform detailed analysis and decoding of signals
    - Does not show wave forms
    - Cost: $50-$10K+


Saleae Logic 1.1.14 - [Disconnected] - [RS485_ADAPTER.logicdata] - [1 MHz, 500 M Samples]
500 M Samples
@
1 MHz
Start Simulation
Options
+50 ms
+60 ms
A
0 - Serial A
1 - Serial B
2 - Channel 2
3 - Channel 3
4 - Channel 4
5 - Channel 5
6 - Channel 6
7 - Channel 7
Measurements
Width: ###
Period: ###
Frequency: ###
T1: ###
T2: ###
| T1 - T2 | = ###
Analyzers
Async Serial
receiver.logicdata
RS485_ADAPTER.logicdata

Tools of the Trade

- Test and Measurement
  - Oscilloscope
    - See fast signal changes, wave forms
    - Measure voltages, amplitudes, etc.
    - Cost: $50-$10K+


Tektronix 2430A DIGITAL OSCILLOSCOPE
GPIB STATUS
LOCK SRQ ADDR
CH1 1V ~
A 500µs -125mV? VERT
100
90
0%
CURS
FUNCTION
UNITS
VERTIC
POSITION
VARIABLE
MODE
CH 1
VOLTS/DIV
5V
COUPLING/
INVERT
BANDWIDTH
CH1 OR X
1MΩ15pF ≤ 400Vpk
SERIAL
B040970
SELECT
INTENSITY
STATUS/
HELP
FOCUS
TRACE
ROTATION
ASTIG
MENU OFF/
EXTENDED
FUNCTIONS
POWER
ON
OFF


allwallpapersfree.blogspot.com

Tools of the Trade

- Soldering
  - High-quality Soldering Iron
    - Must have temperature control, variety of tips
    - Cost: $50-1000
  - Hot air rework station
    - Great for removing components
    - Cost: $50-1000

Tip: Practice on junk electronics first!


W.E.R 858D
METCAL
The SolderMill
www.zeph.com

Tools of the Trade

- Device Programmers
  - Microchip Pickit
    - Program and read Microchip PIC chips
    - Cost: $35
  - Atmel AVR-ISP Mk II
    - Program and read Atmel AVR chips
    - Cost: $35
  - JTAG Debugger
    - Program, read, debug various 32-bit ARM chips
    - Cost: $30-$500+
    - Often require device-specific software/config files
  - EPROM burner
    - Program, read, modify various ROMs
    - Cost: $30-150


MICROCHIP
PICkit 3
POWER
ACTIVE
STATUS
USB
J-link
SEGGER
JTAG

Tools of the Trade

- Magnification
  - Stereo microscope (awesome!)
    - Cost: $100-1000+
  - 5-20X jeweler's loupe
    - Cost: $10-20

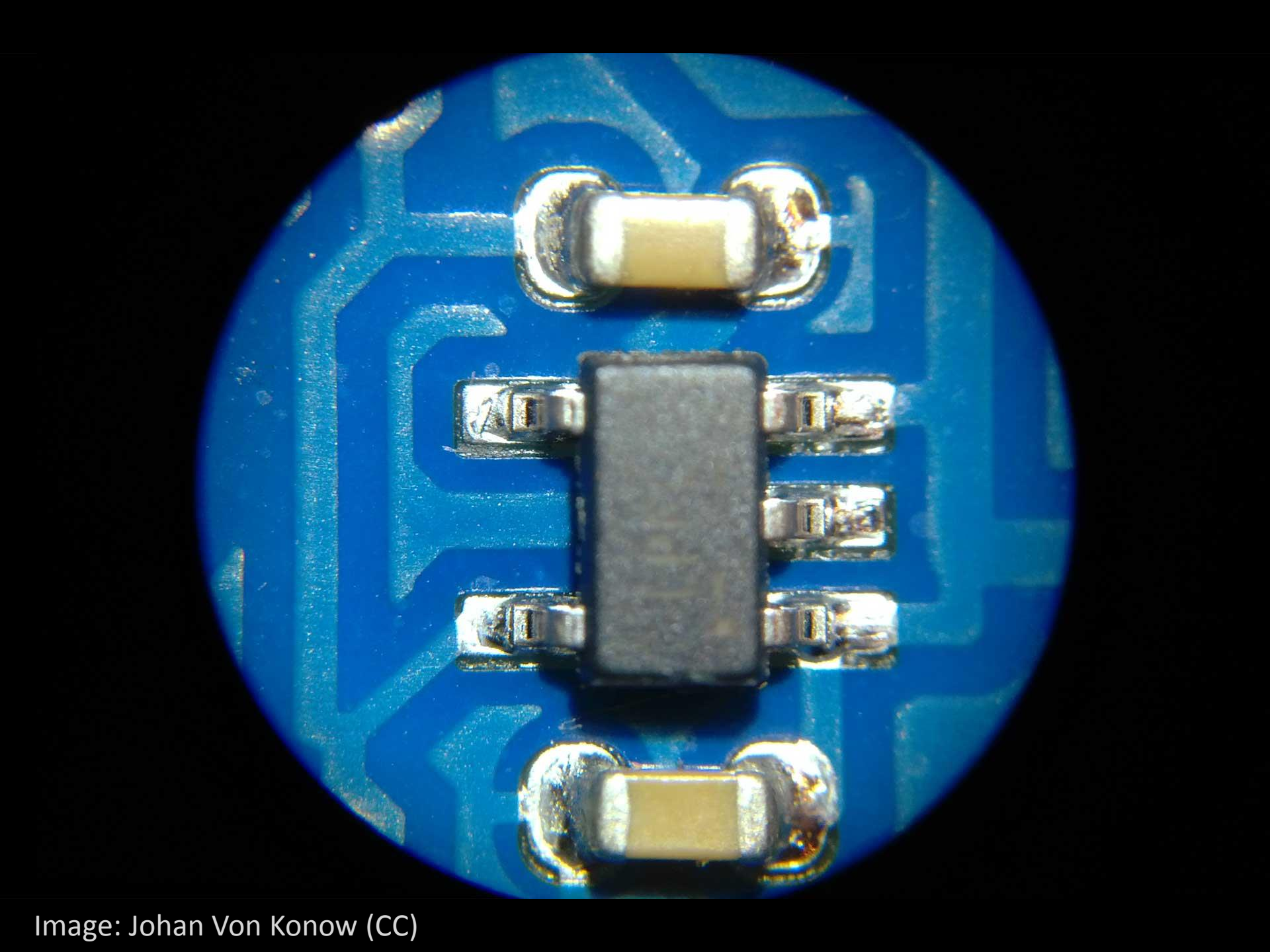


Image: Johan Von Konow (CC)

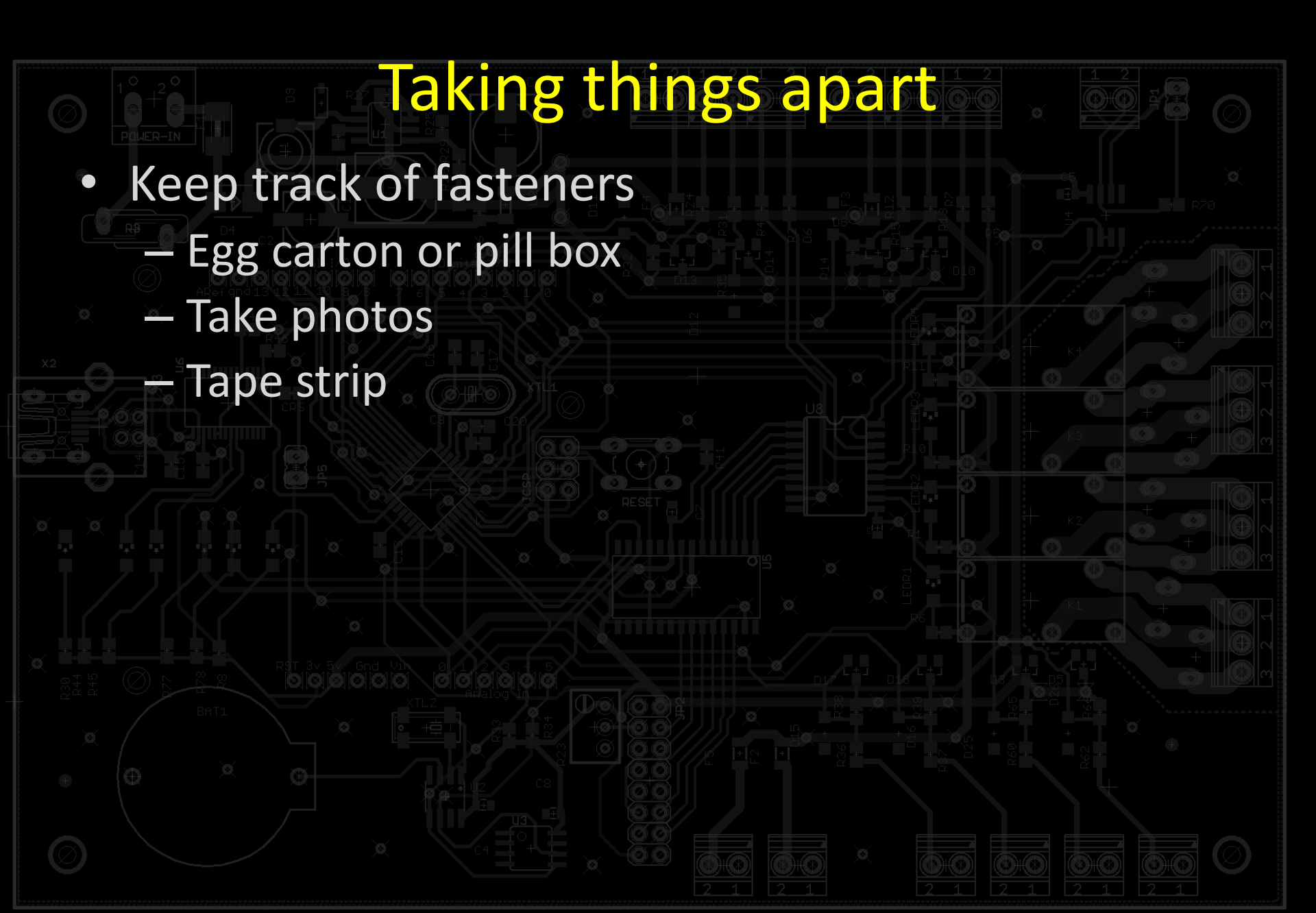
Taking things apart

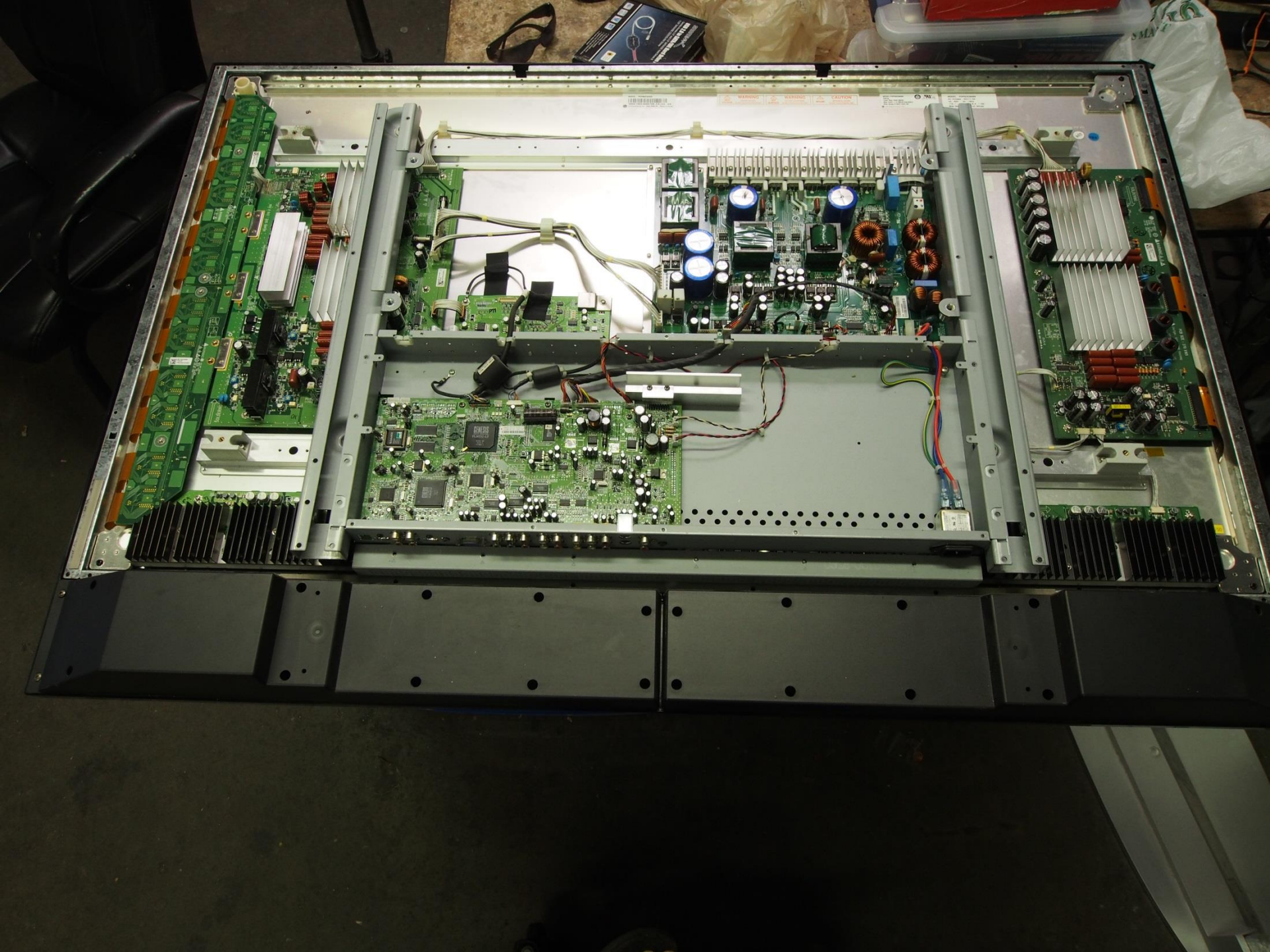
- Remove power
- Locate fasteners and remove
  - Screws
  - Hidden screws (check under stickers, rubber feet)
  - Glue (soften with heat or crack/saw plastic welds loose)
  - Plastic tabs (use guitar pick or case spreader)


AC IN

Taking things apart

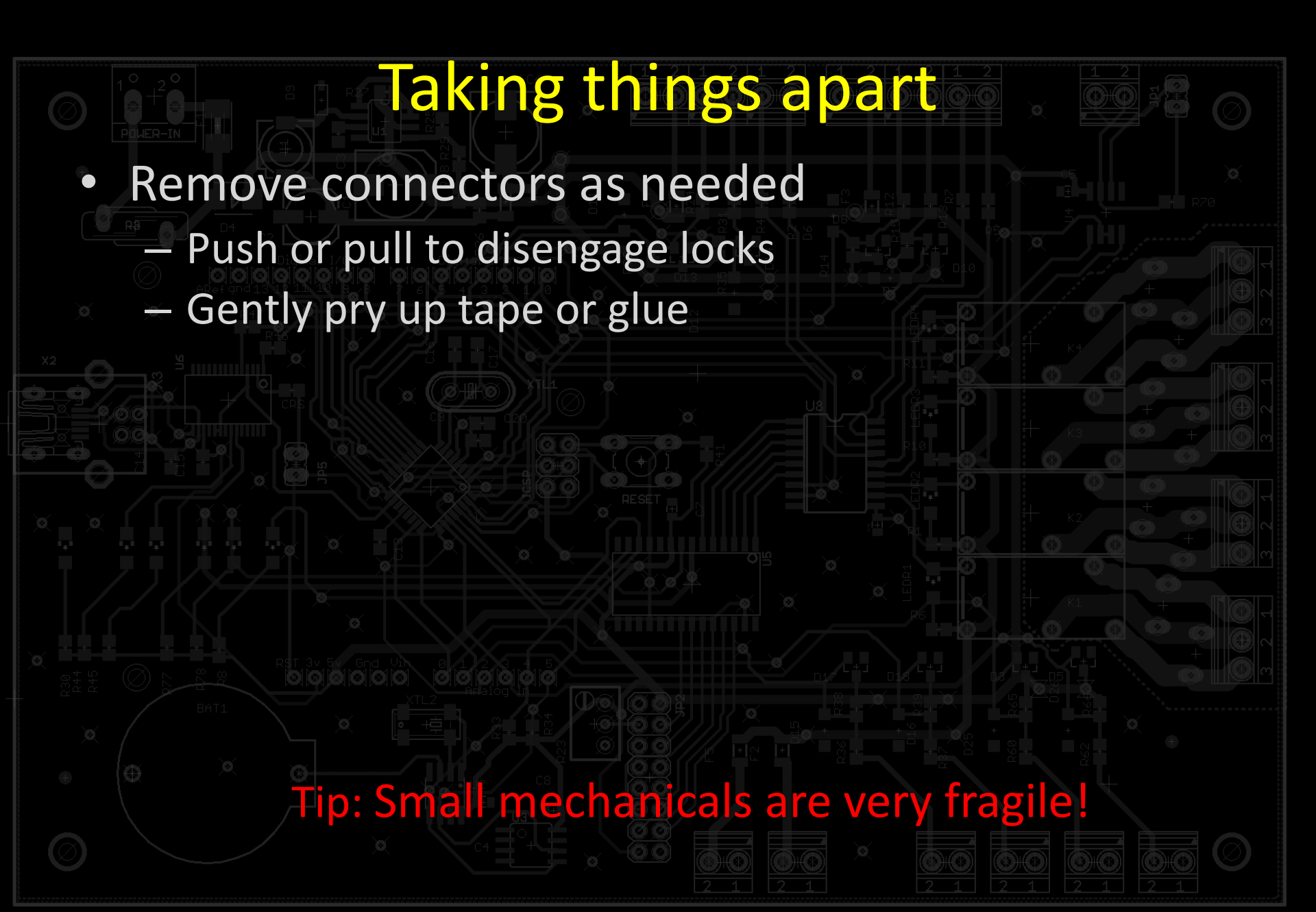
- Keep track of fasteners
  - Egg carton or pill box
  - Take photos
  - Tape strip



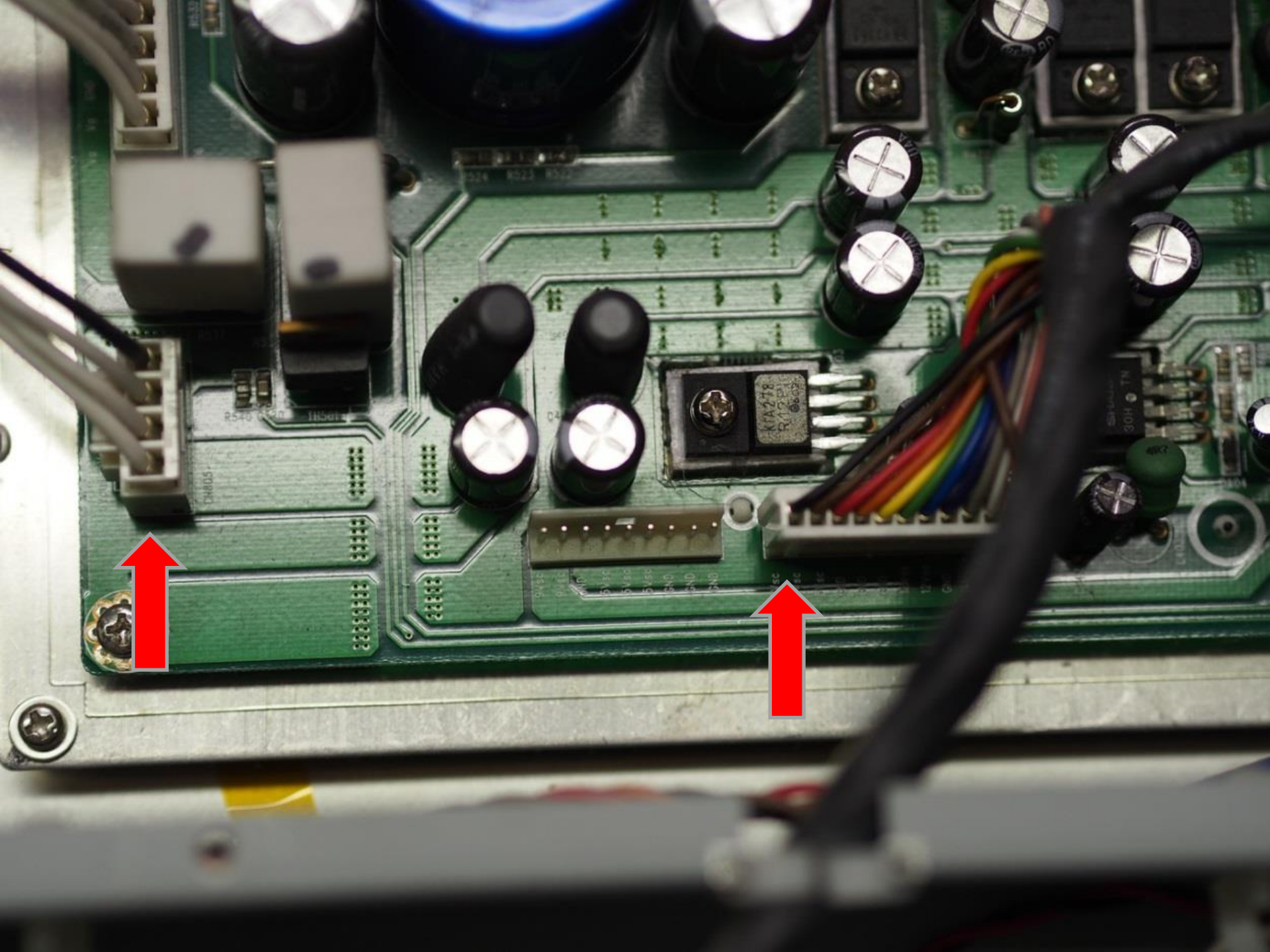


Taking things apart

- Remove connectors as needed
  - Push or pull to disengage locks
  - Gently pry up tape or glue

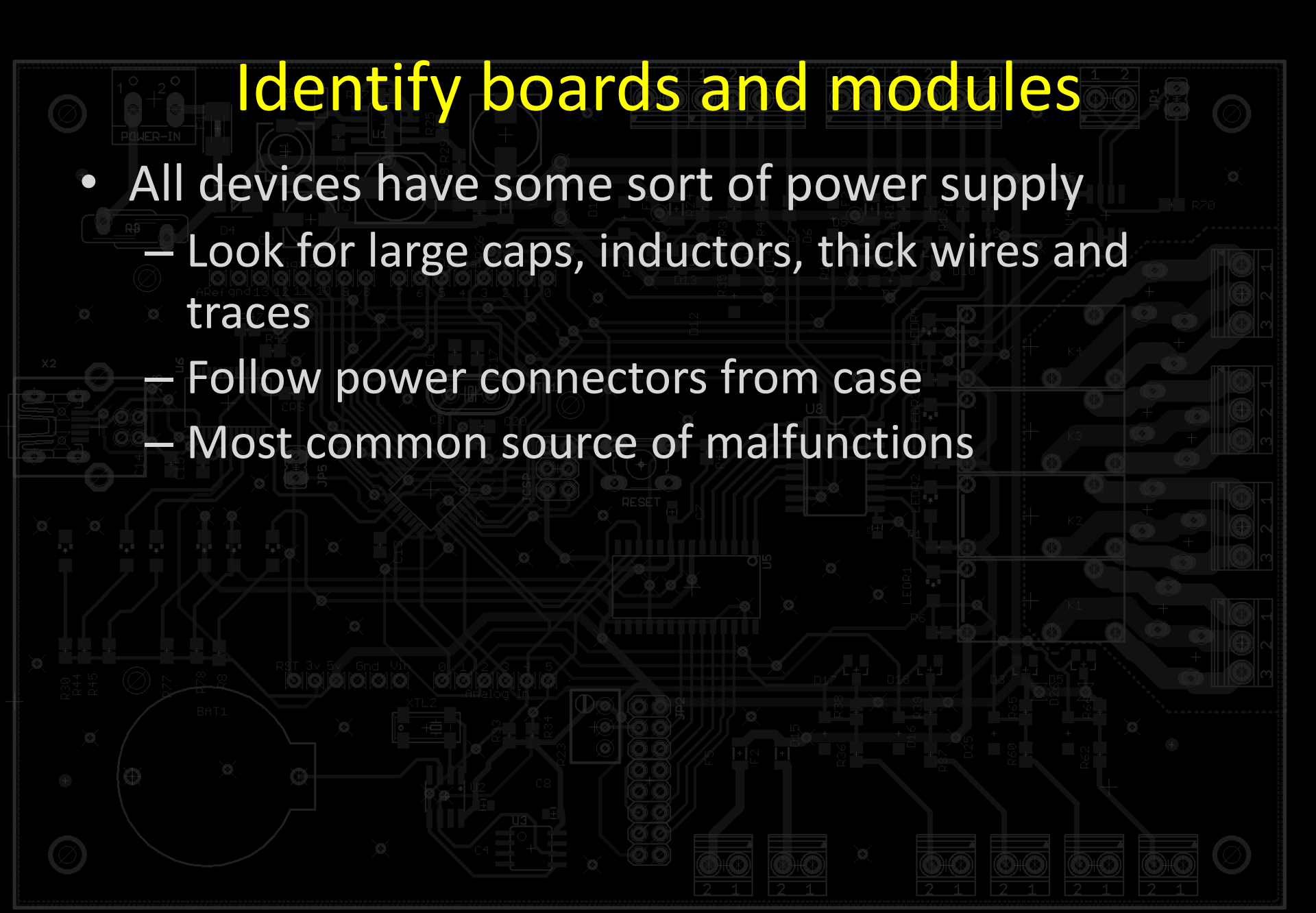


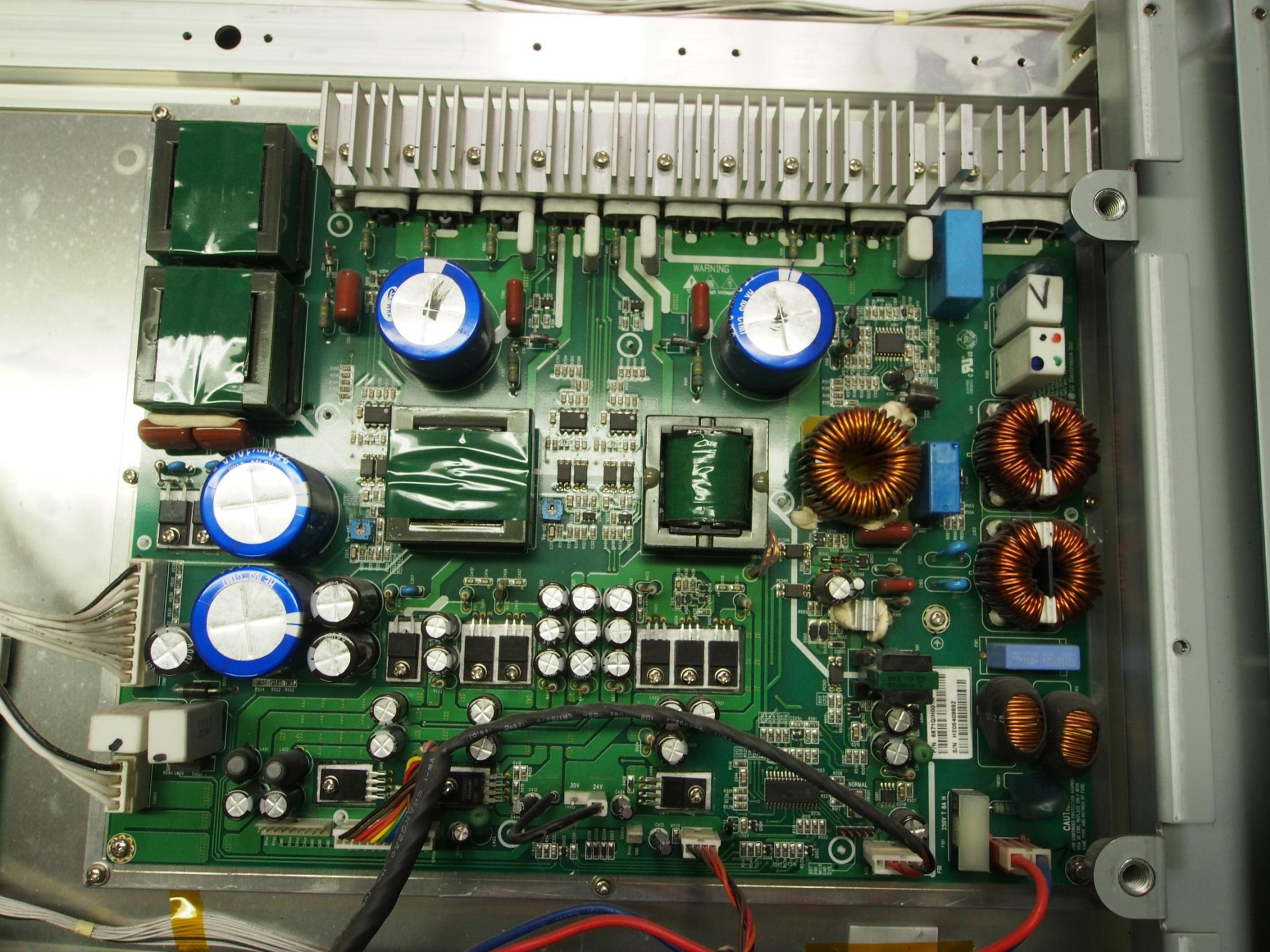
Tip: Small mechanicals are very fragile!


KIA278
R12PI

Identify boards and modules

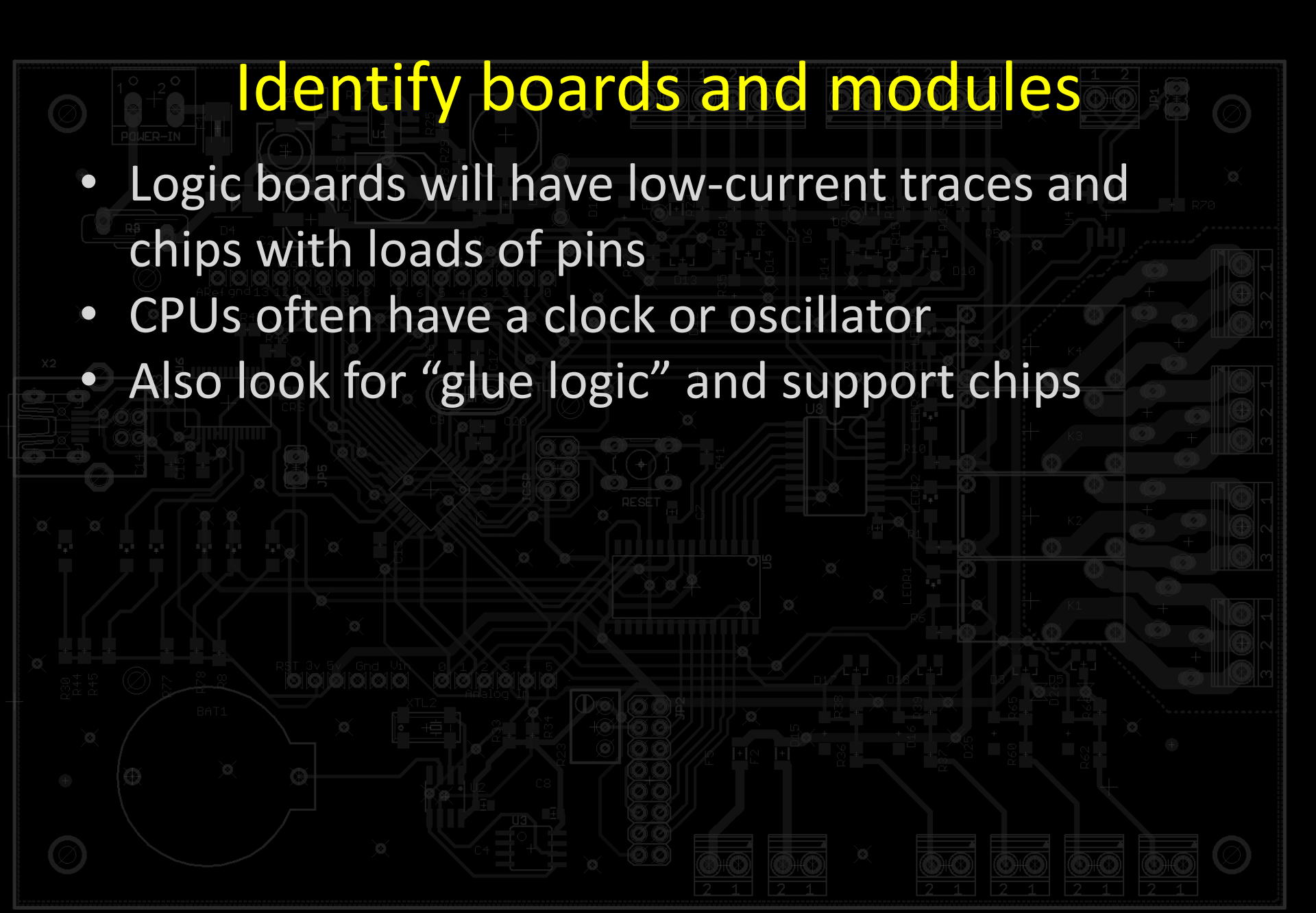
- All devices have some sort of power supply
  - Look for large caps, inductors, thick wires and traces
  - Follow power connectors from case
  - Most common source of malfunctions

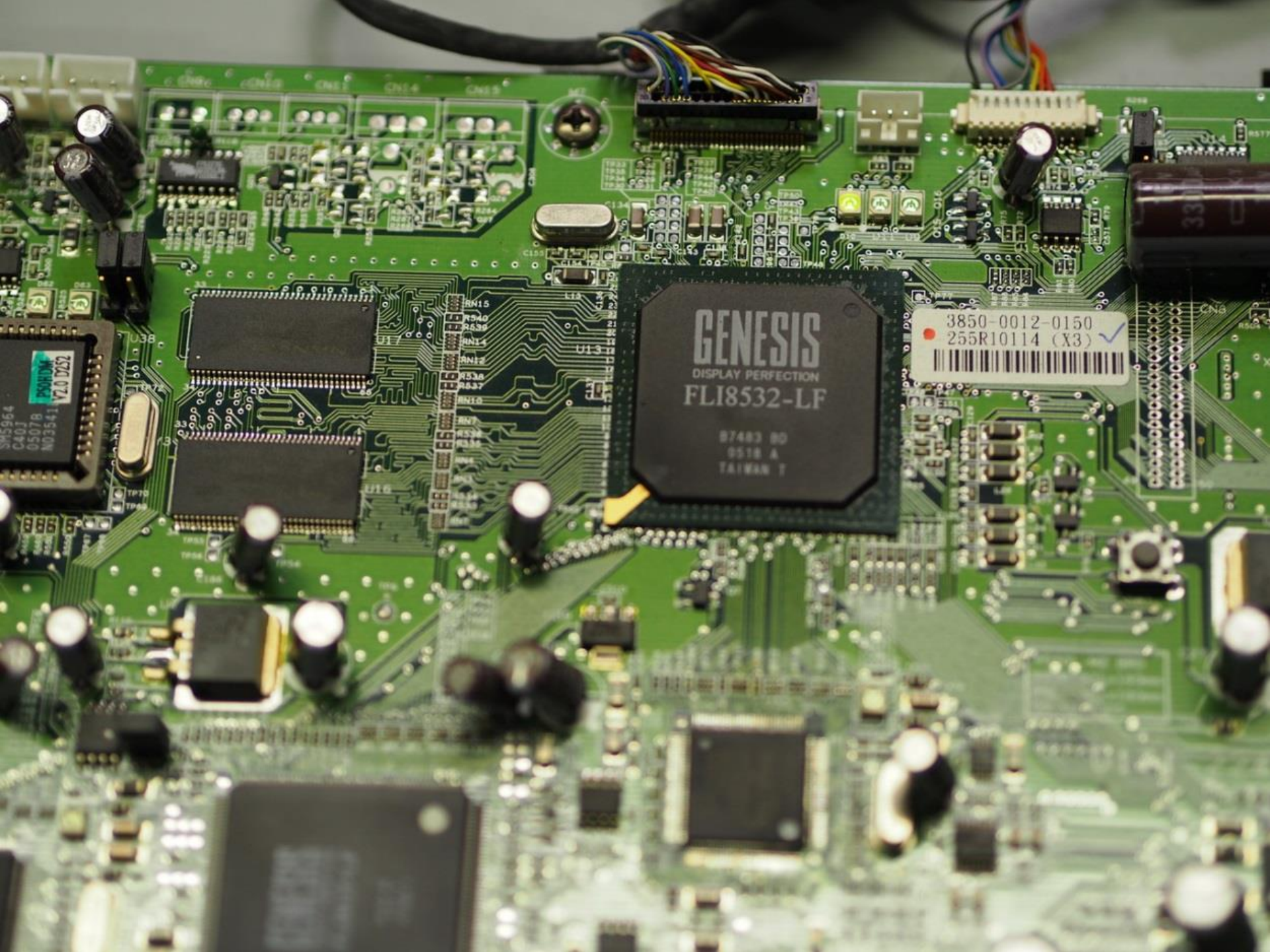



WARNING
NORMAL

Identify boards and modules

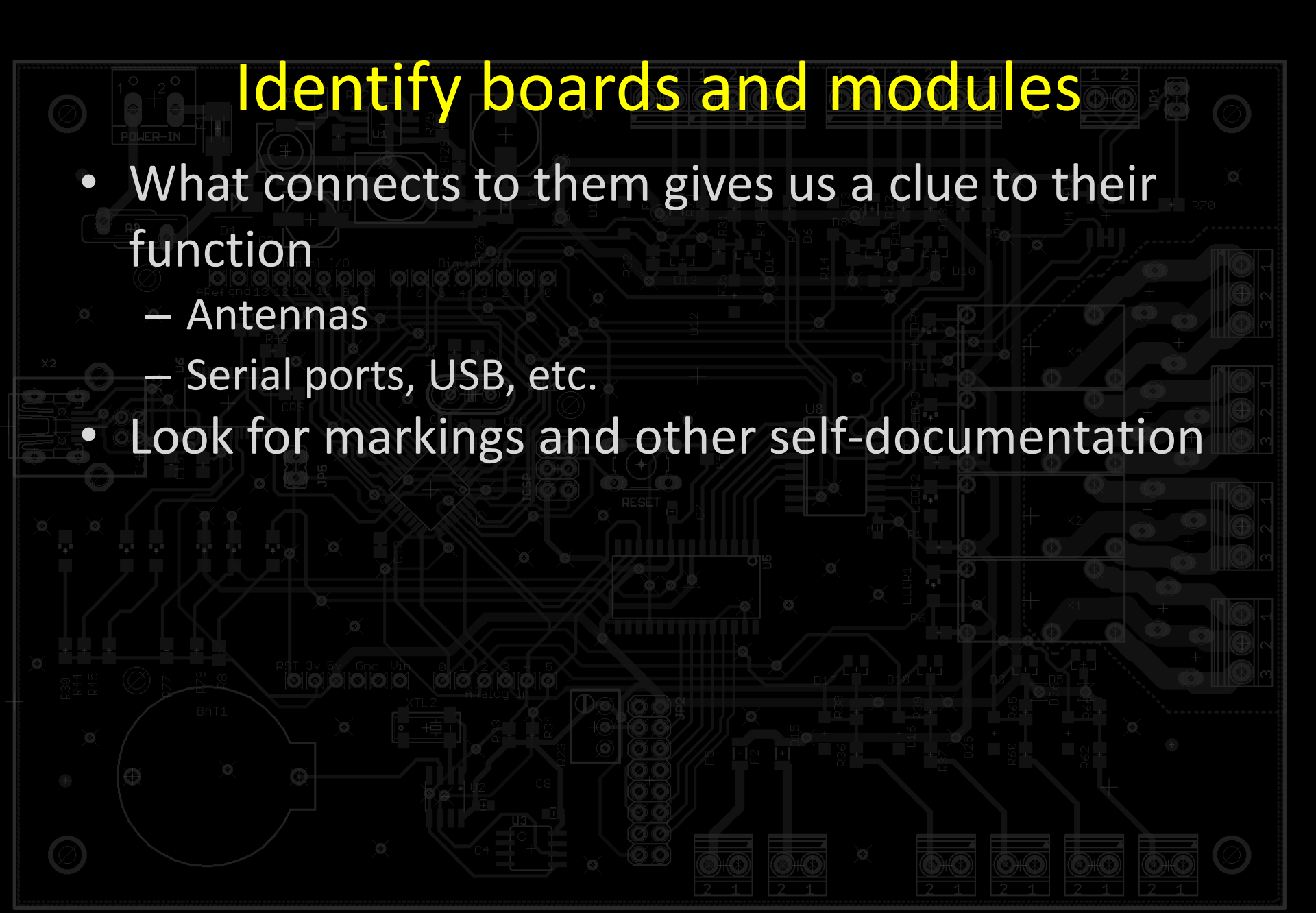
- Logic boards will have low-current traces and chips with loads of pins
- CPUs often have a clock or oscillator
- Also look for “glue logic” and support chips




GENESIS
DISPLAY PERFECTION
FLI8532-LF
3850-0012-0150
255R10114 (X3)

Identify boards and modules

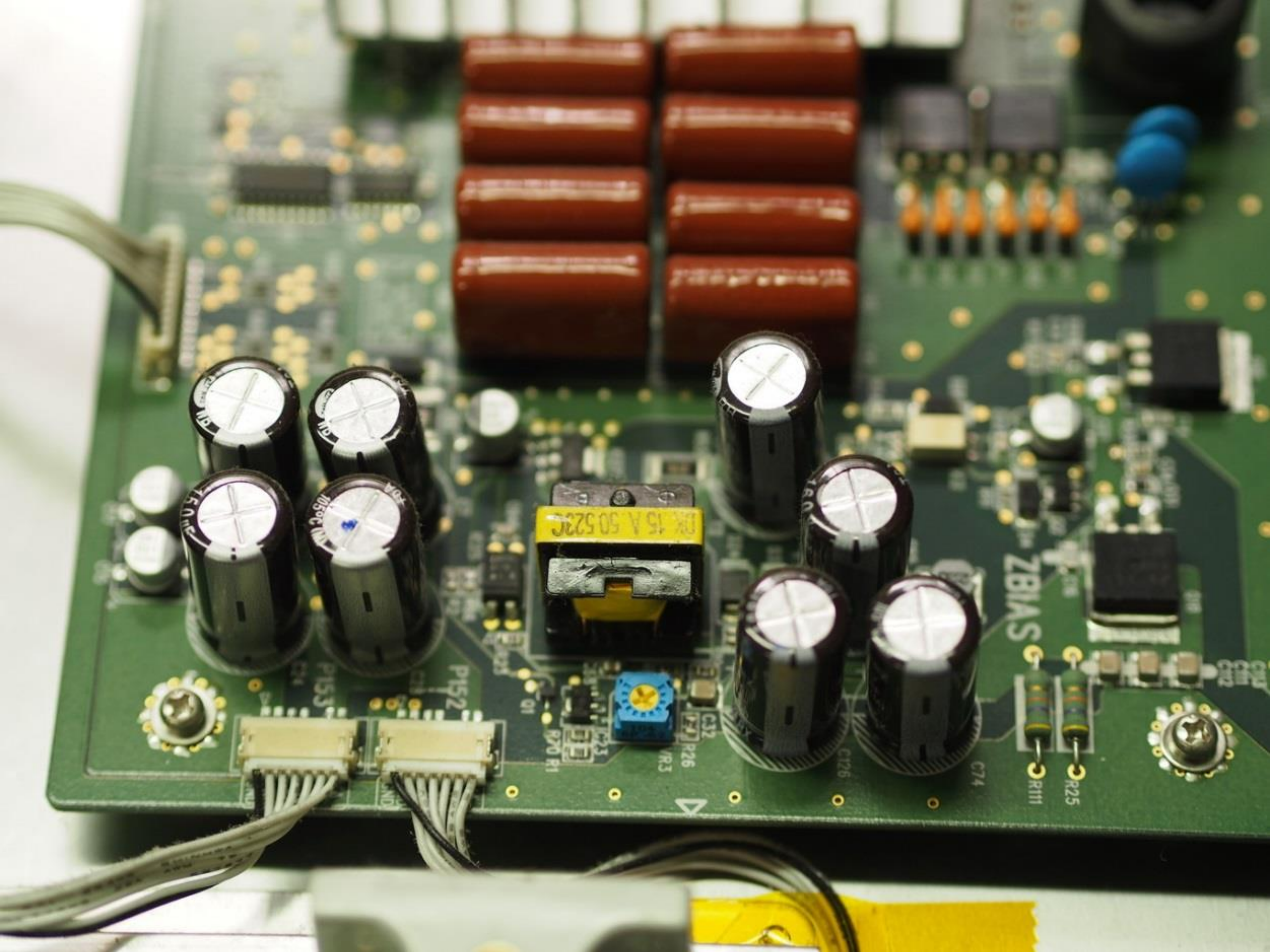
- What connects to them gives us a clue to their function
  - Antennas
  - Serial ports, USB, etc.
- Look for markings and other self-documentation




DC1
DC2
DATA_IN
LE
CLK_IN
MICOM
DC1
DC2
DATA_OUT
CLK_OUT
+5V
WARNING
LGE PDP 050303
MODEL :50X3
BOARD : YDRV_BTM
PART NO : 6870QDC005A
LOC NO : 7XXX
P6
6871QDH089A
YDRVBT

Identify components

- The components on a PCB also give us clues
- Large passive components usually indicate power
  - -PTH capacitors
  - -Power resistors
  - -Inductors
- Small-sized passives are for signals
  - Diodes
  - Chip capacitors
  - SMT resistors

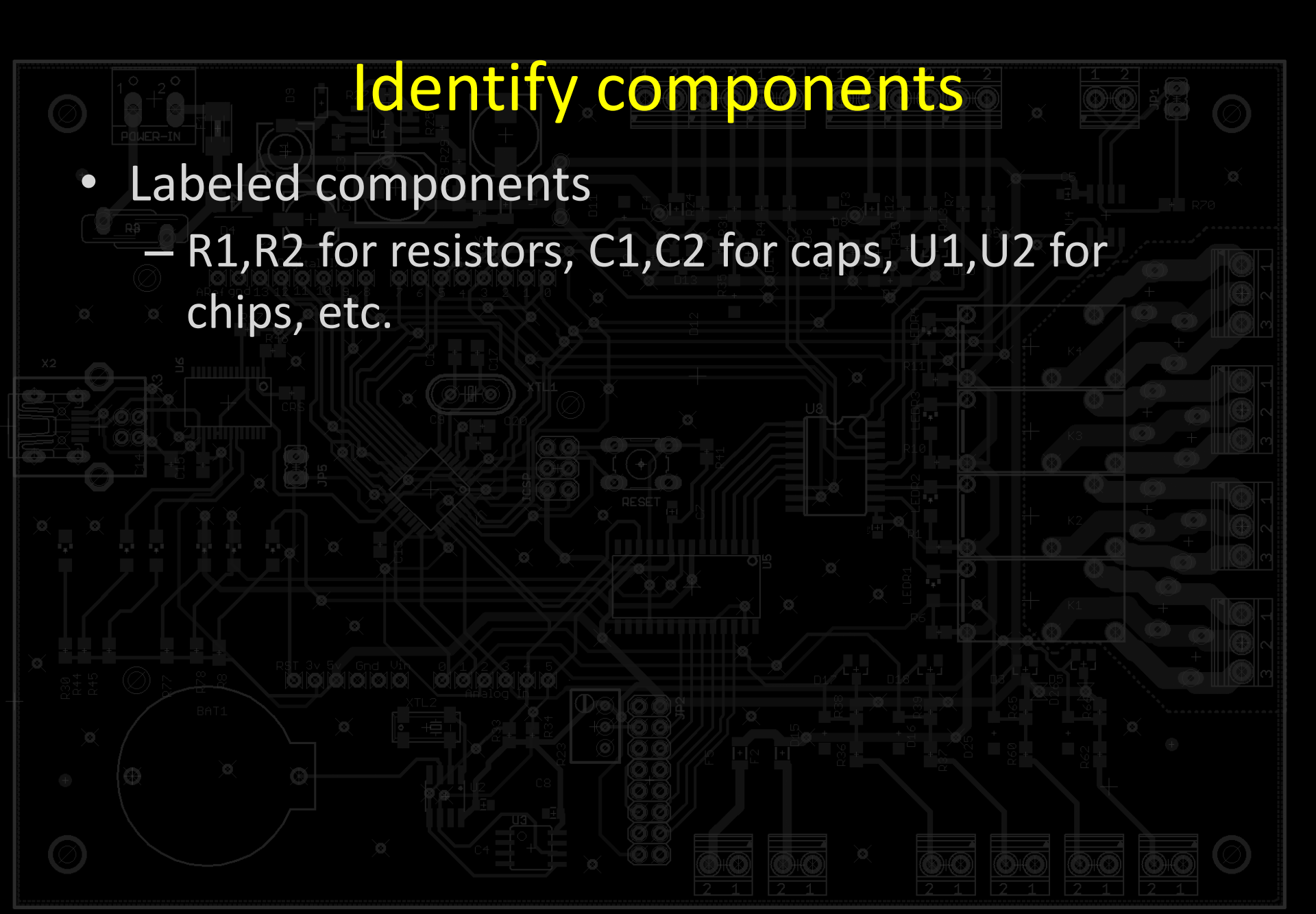

ZBIAS
P152
P153
C74
C126
R111
R25
VR3
R26

Identify components

- RF modules often have metal shielding around them
  - Not an SD card holder!
- Other obvious components
  - Relays
  - Surge protection devices and fuses
  - Input protection circuits

Identify components

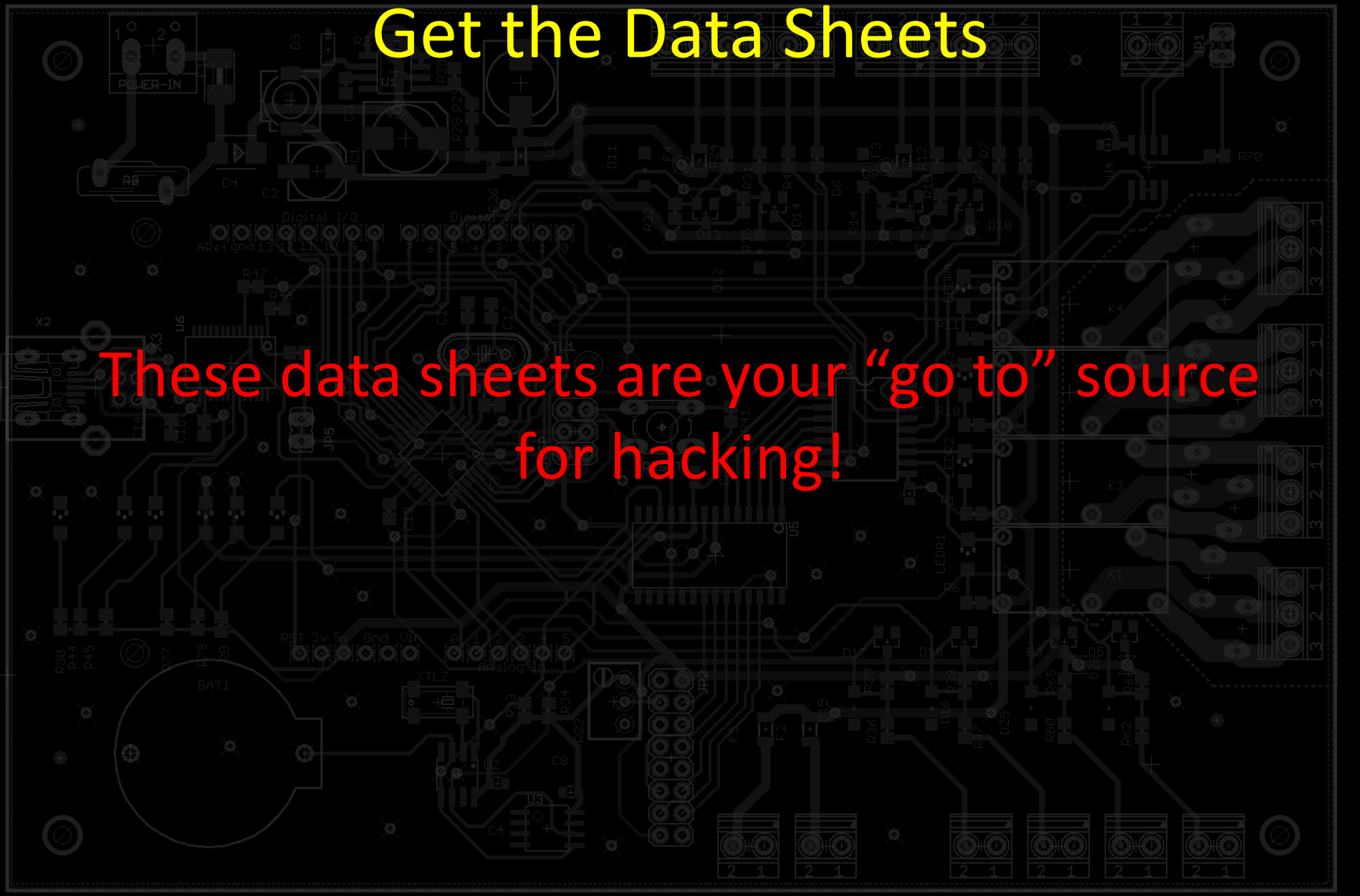
- Labeled components
  - R1,R2 for resistors, C1,C2 for caps, U1,U2 for chips, etc.



Get the Data Sheets

- Confirm identity of components by looking up part numbers
  - Alldatasheet.com
  - Digikey.com
  - Mouser.com
  - Manufacturer website (manufacturer logo or code in part number)

Get the Data Sheets



2 Pin configuration

Figure 2. Pin connections

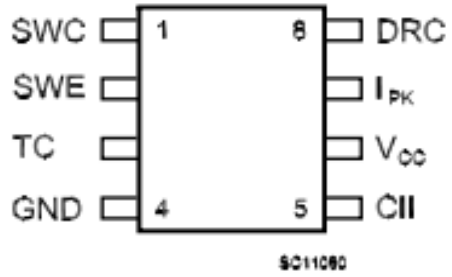


Table 2. Pin description

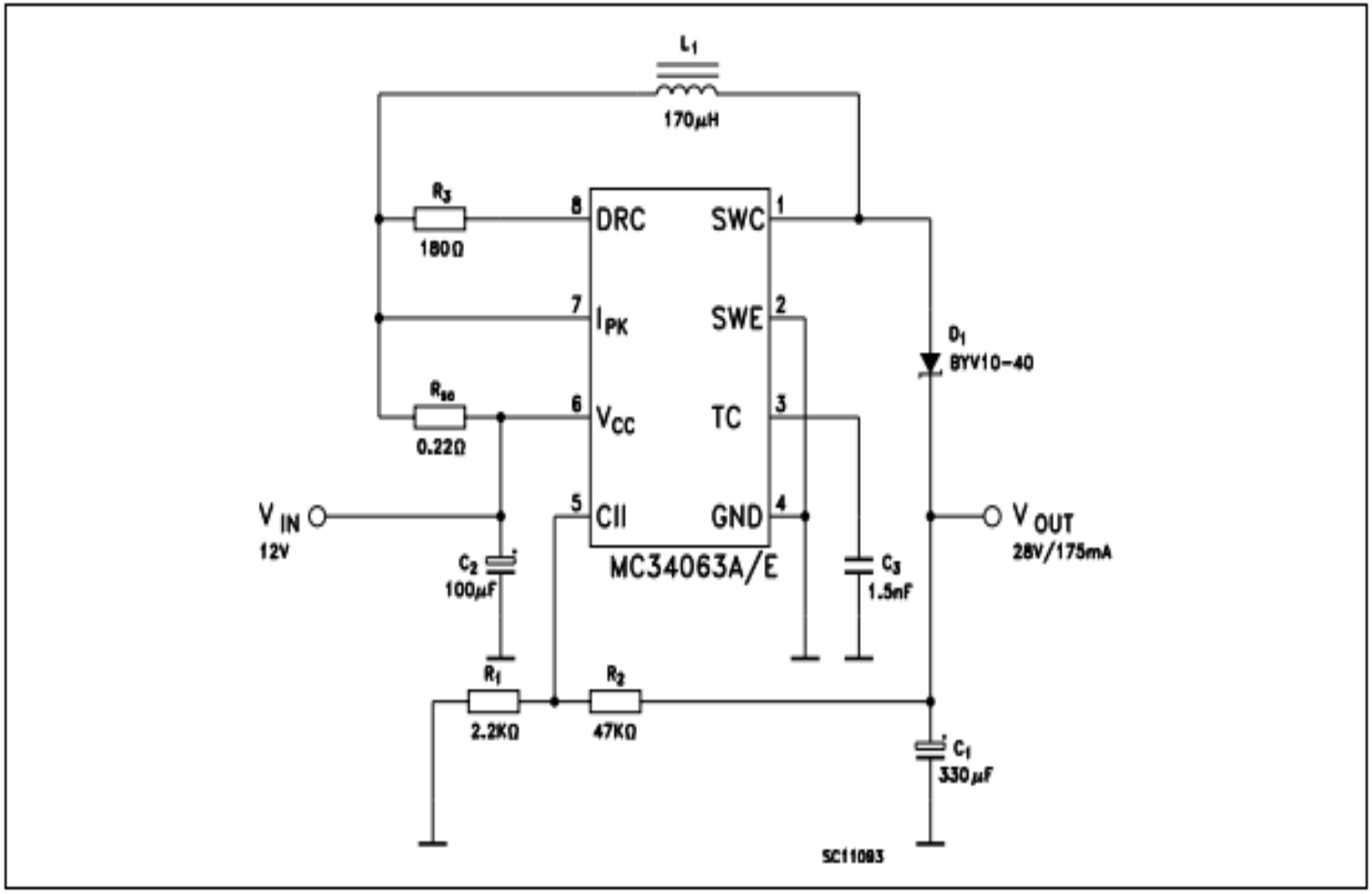
Pin n°	Symbol	Name and function
1	SWC	Switch collector
2	SWE	Switch emitter
3	TC	Timing capacitor
4	GND	Ground
5	CII	Comparator inverting input
6	V_{CC}	Voltage supply
7	I_{PK}	I_{PK} sense
8	DRC	Voltage driver collector

Get the Data Sheets

- A chip or other component often comes with a reference design
  - Your device will usually contain something very similar to the reference design. Look for it!
  - May also have programming, other hacking info

6 Typical application circuit

Figure 13. Step-up converter



Make an educated guess as to function

- Designers are lazy
  - After a while, you'll see the same circuits over and over
    - Power supply circuits
    - Input protection
    - Outputs/relay drivers/lighting control
    - Op-amps and other front-end signals

Figure out your hacking strategy

- What am I trying to do?
  - Fix it?
  - Add a feature?
  - Cannibalize it for parts?

Figure out your hacking strategy

- Questions to ask
  - Do the parts come up when I do a search?
  - Any OTP devices?
  - High-speed devices?
  - Difficult access (BGA, multilayer PCBs)

Figure out your hacking strategy

- Some strategies
  - Dump the program ROM and change it
    - Requires locating the proper chip and attaching a device
    - Security fuses may prevent extraction
    - May require extensive knowledge of assembly language and embedded debug tools

Example: “Mod chips” for OBD-I cars

Figure out your hacking strategy

- Write a new program and upload it
  - May be best option if a tool chain is available.
  - Also helps if device is simple and uses well-documented peripherals

Example: Open firmware for Baofeng UV3r radio

Figure out your hacking strategy

- Build an add-on module
  - Add a daughter board to take over or supplement the device's own logic
  - Replace a module with your own

Example: Fake GPS Module, UV3r beacon

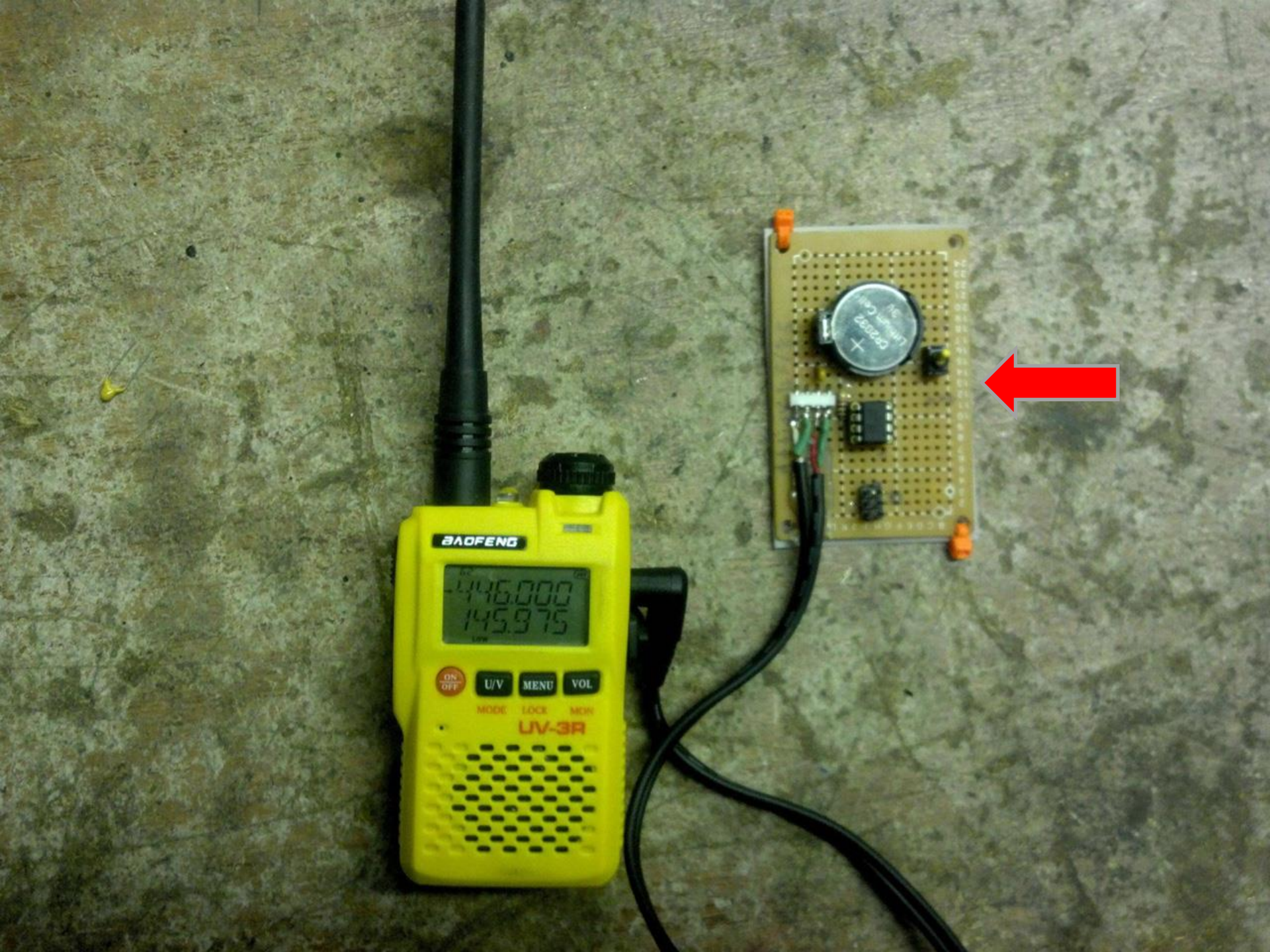

BAOFENG
446.000
145.975
ON OFF
U/V
MENU
VOL
MODE
LOCK
MON
UV-3R

Figure out your hacking strategy

- More strategies
  - Break out unused pins
  - Solder on missing parts

Example: Xbox USB add-on

Figure out your hacking strategy

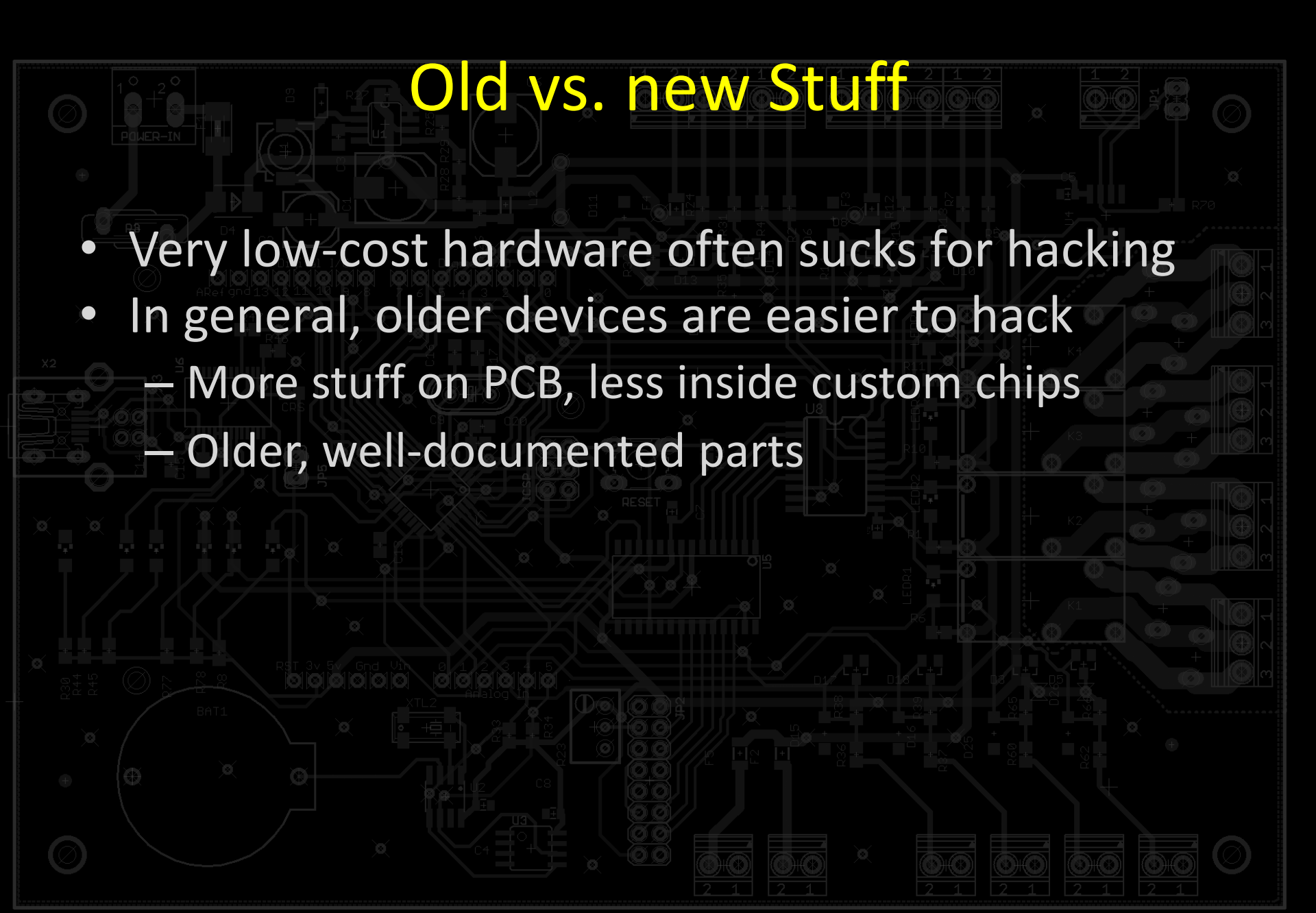
- More strategies

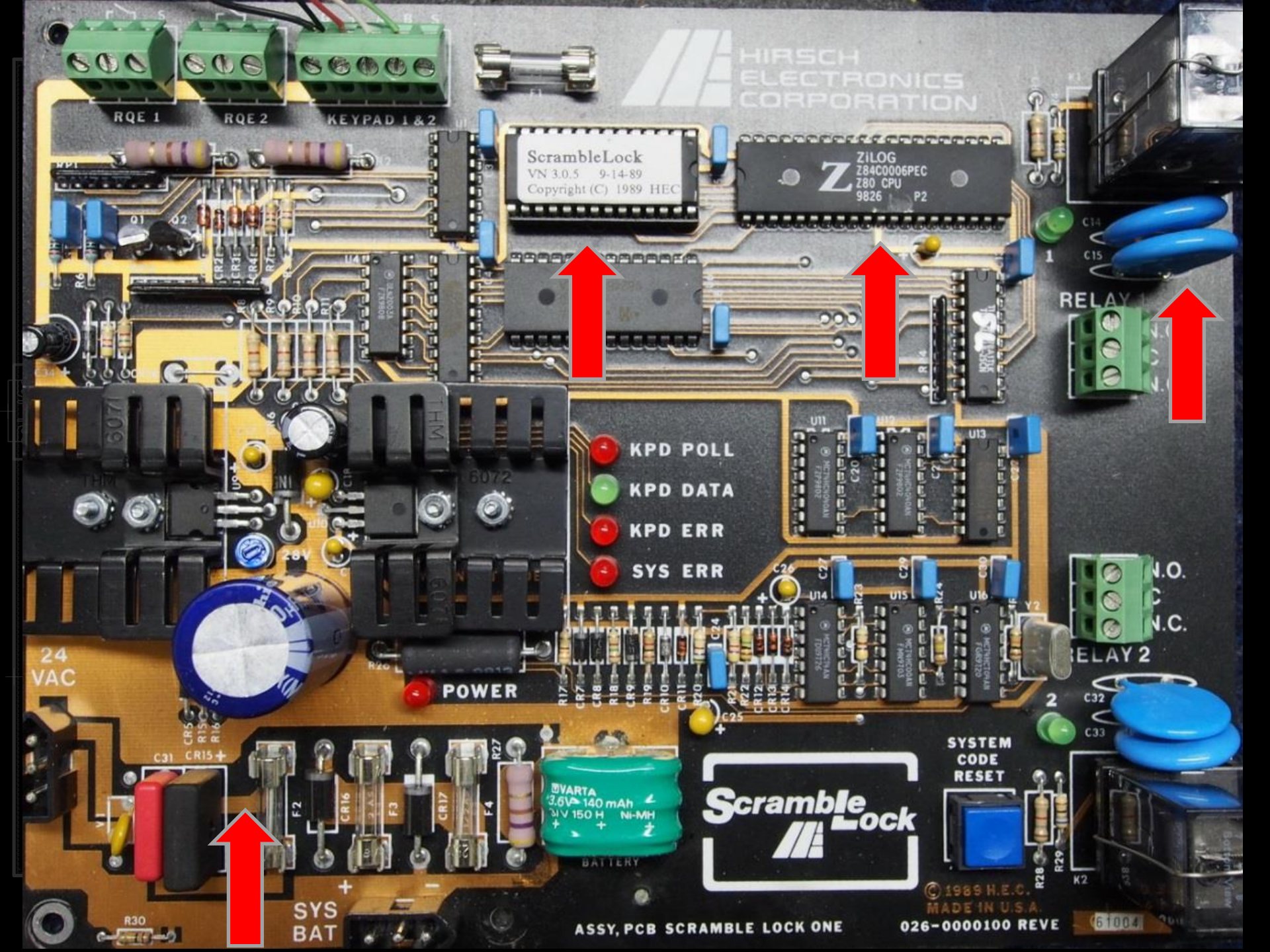
  -Figure out it's protocol and plug into it
  - Find the pin out (starting with GND)
  - Use scope, logic analyzer, data sheets
  - SPI
  - Serial
  - Clock/Data

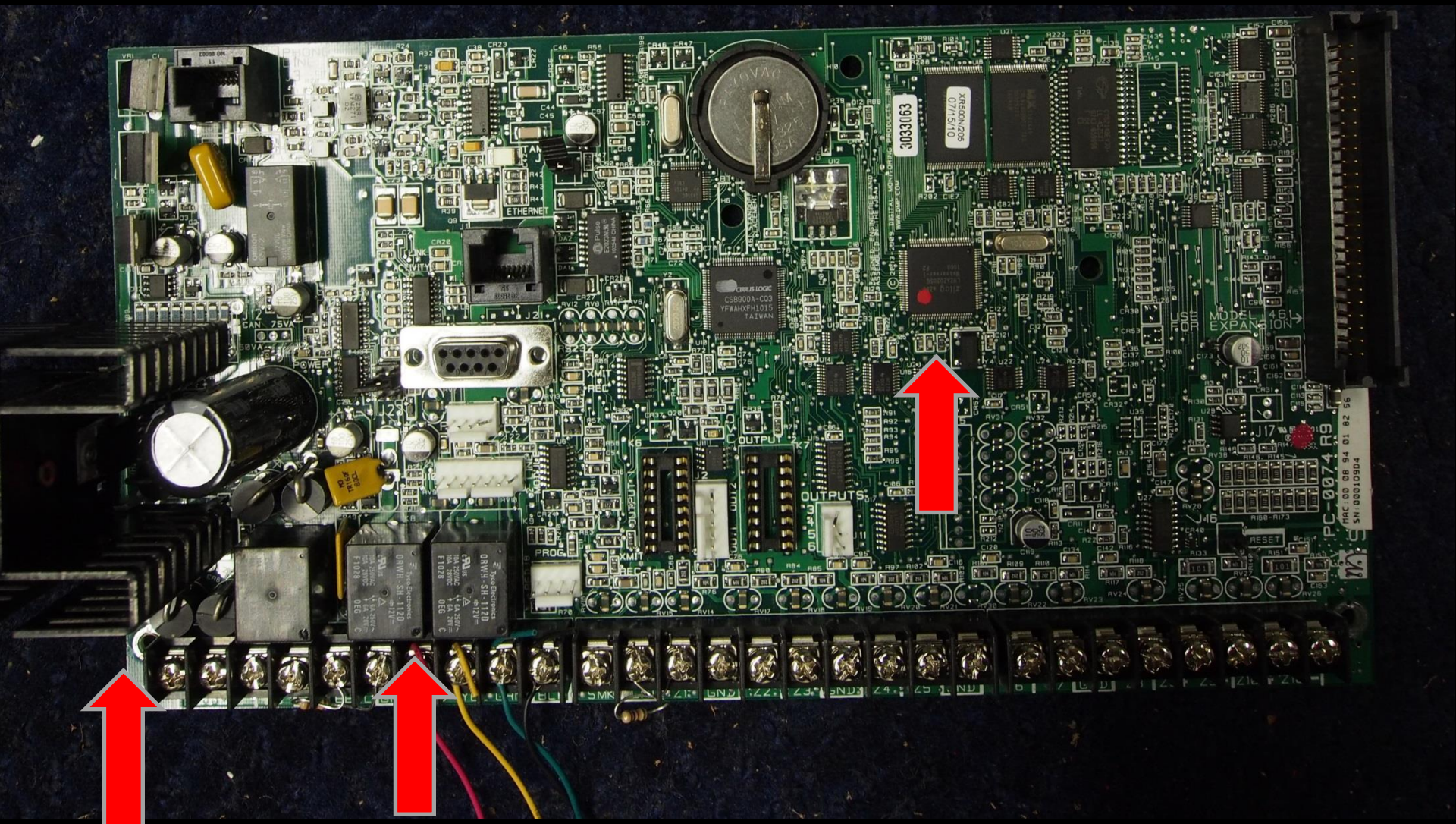
Example: Alarm system protocols

Old vs. new Stuff

- Very low-cost hardware often sucks for hacking
- In general, older devices are easier to hack
  - More stuff on PCB, less inside custom chips
  - Older, well-documented parts




HIRSCH
ELECTRONICS
CORPORATION
RQE 1
RQE 2
KEYPAD 1&2
ScrambleLock
VN 3.0.5 9-14-89
Copyright (C) 1989 HEC
ZiLOG
Z84C0006PEC
Z80 CPU
9826 P2
RELAY 1
KPD POLL
KPD DATA
KPD ERR
SYS ERR
RELAY 2
N.O.
N.C.
24
VAC
POWER
SYSTEM
CODE
RESET
ScrambleLock
SYS
BAT
BATTERY
VARTA
3.6V 140 mAh
150 H Ni-MH
© 1989 H.E.C.
MADE IN U.S.A.
ASSY, PCB SCRAMBLE LOCK ONE
026-0000100 REVE

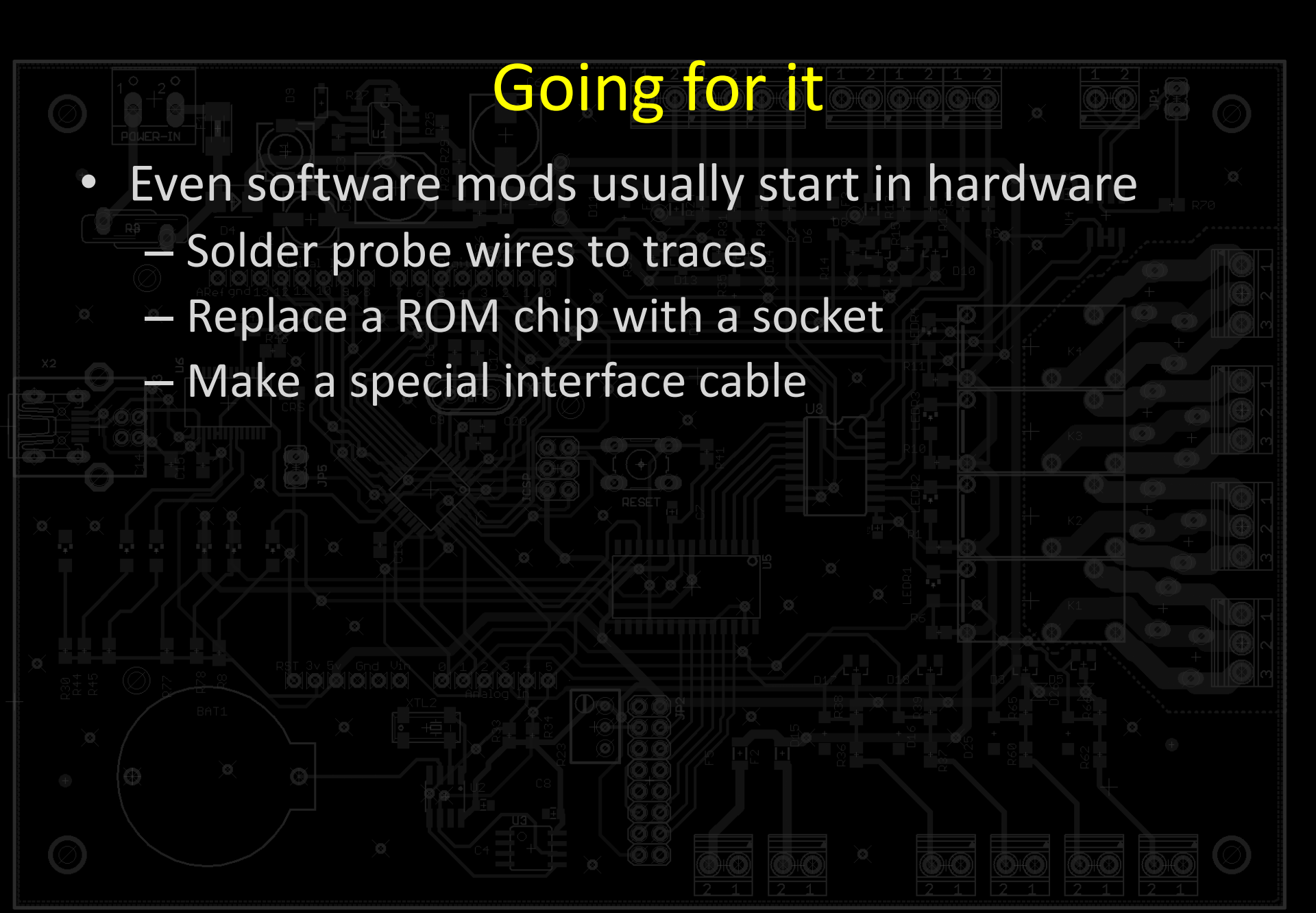

ETHERNET
OUTPUTS
RESET
PC-0074-R8
USE FOR MODEL 46 EXPANSION
CAN 75VA
50VA
XMIT
REC
PROG

Going for it

- Simple analog devices respond to parts swaps
  - Switching PSUs
    - Can be reprogrammed with resistors
  - Beeping/flashing toys
  - Musical instruments
    - Look for R-C oscillators, try swapping values

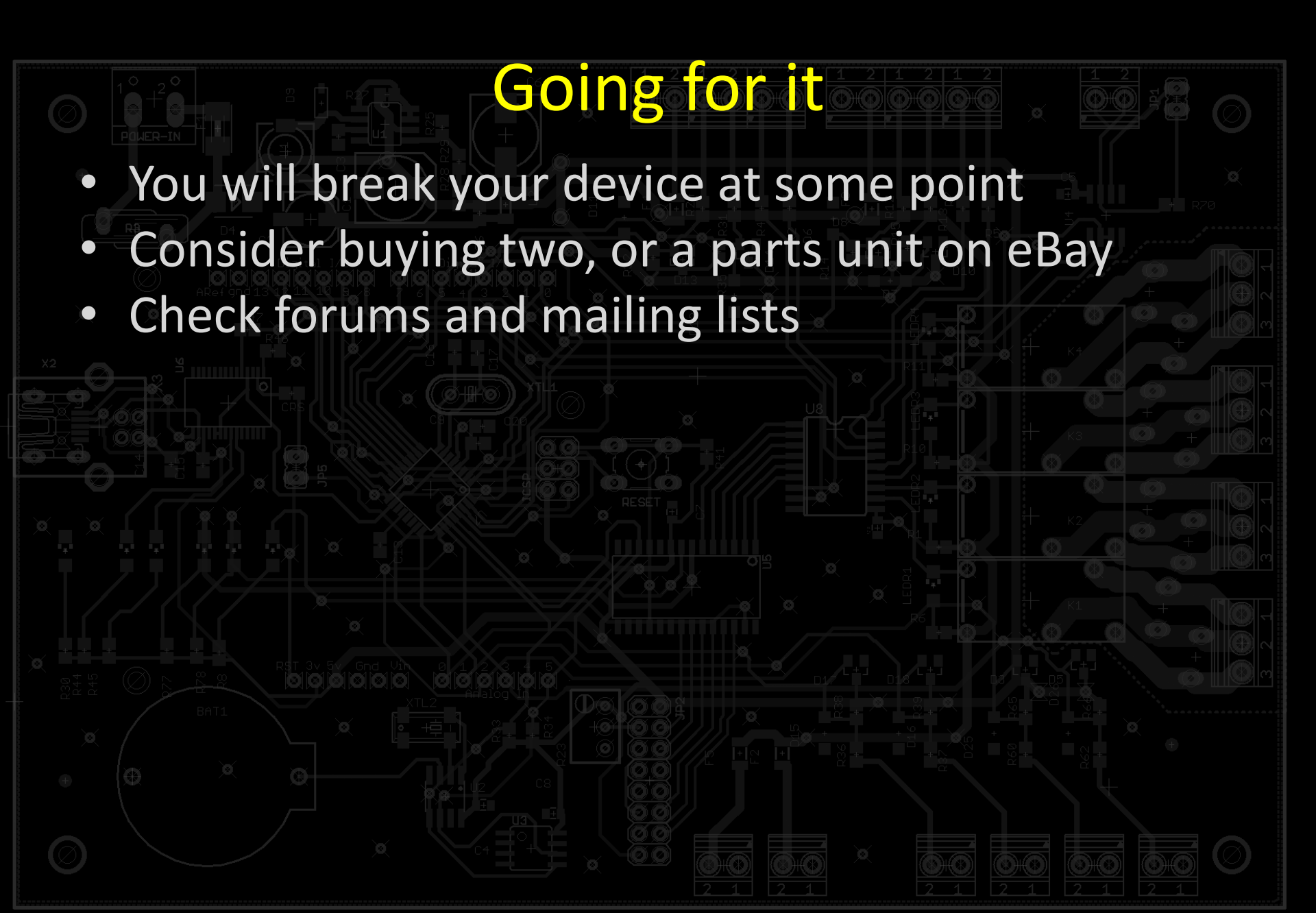
Going for it

- Even software mods usually start in hardware
  - Solder probe wires to traces
  - Replace a ROM chip with a socket
  - Make a special interface cable



Going for it

- You will break your device at some point
- Consider buying two, or a parts unit on eBay
- Check forums and mailing lists



Legal issues

- In the U.S., DMCA is your main worry
- Section 1201(f) allows for exemption for developers to circumvent protection is order to achieve "the elements necessary to achieve interoperability of an independently created computer program with other programs.“

Legal issues

- Things to consider:
  - Be careful what you document and share
  - Can be construed as “circumvention” under DMCA
  - Some info sharing can be construed as “trafficking.”
  - In general, the more paranoid and tied to expensive hardware a company is, the more likely they are to attack you .

Legal issues

- Bottom line:

You can be right and still get screwed!

Further Reading

- Safety
  - Sam's LASER FAQ
    - http://www.repairfaq.org/sam/safety.htm
- General Electronics
  - Forrest Mimms III – Getting Started in Electronics
    - http://www.forrestmims.org/publications.html
  - Analog Seekrets – Leslie Green
    - http://www.logbook.freeserve.co.uk/seekrets/
- Component ID
  - Wikibooks Electronic Component ID guide
    - http://en.wikibooks.org/wiki/Electronics/Component_Identification

Further Reading

- Video Blogs and Forums
  - EEVBLOG – Teardowns, tutorials, etc.
    - http://www.eevblog.com
- Reverse Engineering Techniques
  - Bunnie Huang - Hacking the Xbox (Now available free!)
  - http://nostarch.com/xboxfree
- Legal
  - EFF Reverse Engineering FAQ
    - https://www.eff.org/issues/coders/reverse-engineering-faq
  - Chilling Effects Reverse Engineering Guide
    - http://chillingeffects.org/reverse/faq.cgi

Thank you!

- Questions?
- My contact
  - http://www.accxproducts.com/wiki
  - E-mail: jnorman@accxproducts.com