

Making (and Hacking) the DEFCON 17 Badge

by Joe Grand aka Kingpin

Me.



electrical engineer.

hardware hacker.

daddy.

Hackers: The Next Generation



Last Year

This Year



KINGPIN

- Introduction
- Hardware
- Firmware
- Manufacturing

A Poem.

DEFCON 17 Haiku
Joe Grand aka Kingpin
Electronic badge

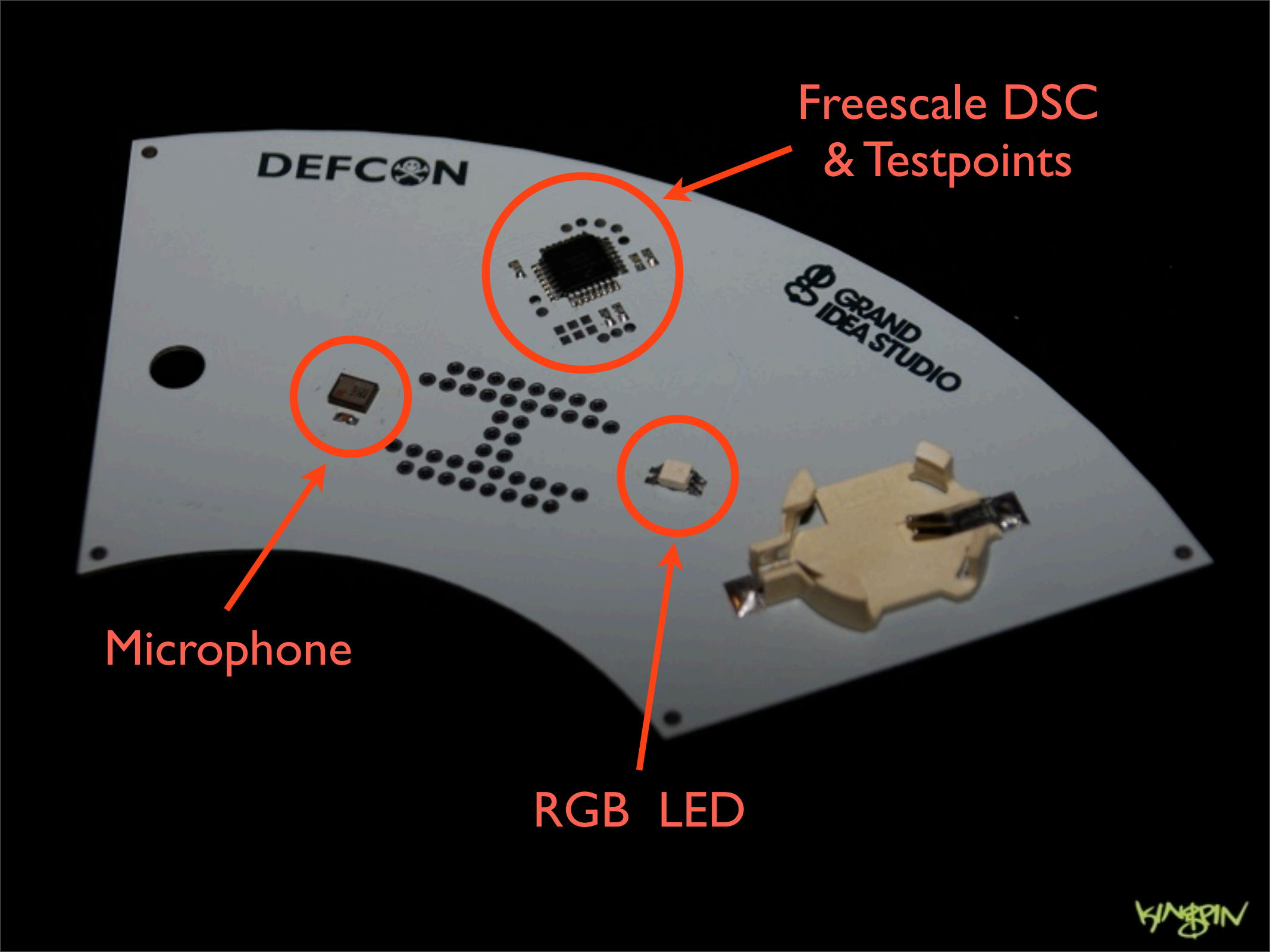
Audio input
Affects LED output
Sound and light combined

Upload new firmware
With serial bootloader
Voltage reassigned

Puzzle of seven
Badge-to-badge interfacing
Using I2C

Hack badge for prizes
Clever modifications
Can you impress me?

KINGPIN


Freescale DSC
& Testpoints
DEFCON
GRAND IDEA STUDIO
Microphone
RGB LED

Badge Operation

- ★ Bootloader
- ★ Party Mode
- ★ Quiet Mode
- ★ Sleep
- ★ ???



Timeline

- ★ Fall 2008: Recover from DEFCON 16
- ★ December 2008: Initial design & parts selection
- ★ January 2009: Prototype hardware design
- ★ February: PCB design completed, production order
- ★ March: Production component orders
- ★ April: Firmware frozen
- ★ May: All components shipped to e-Teknet China
- ★ June: Wait for Customs to release the only box containing parts we couldn't easily get duplicates of
- ★ July: Badge assembly/test

Customs: China v. UPS

Location	Date	Local Time	Description
ZHUHAI CN	22/07/2009	10:35	DELIVERED
GUANGZHOU CN	22/07/2009	3:41	DEPARTURE SCAN
GUANGZHOU CN	21/07/2009	21:47	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / RELEASED BY CLEARING AGENCY. NOW IN-TRANSIT FOR DELIVERY
	21/07/2009	21:47	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / RELEASED BY CLEARING AGENCY. NOW IN-TRANSIT FOR DELIVERY
GUANGZHOU CN	17/07/2009	14:23	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER
GUANGZHOU CN	16/07/2009	16:47	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER
GUANGZHOU CN	09/07/2009	15:38	AD NAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	06/07/2009	11:38	ITIO MPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	30/06/2009	11:18	ADD NAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	29/06/2009	13:26	ADDITIONA DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	23/06/2009	16:12	ADD T DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	19/06/2009	9:52	ADDITIONAL RT D ENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	18/06/2009	9:57	ADDITIONAL ORT CUM ATION IS REQUIRED FOR CLEARANCE
	18/06/2009	9:53	ADDITIONAL IMP DOC NTATION IS REQUIRED FOR CLEARANCE / PACKAGE ABANDONED HE SENDER AND THE RECEIVER
	18/06/2009	9:53	ADDITIONAL CUSTOMS RANCE PROCESSING IS REQUIRED FOR FORMAL ENTRY SUBMISSION / PAC ABANDONED BY THE SENDER AND THE RECEIVER
	18/06/2009	9:53	ADDITIONAL CLEARING AGENCY INFORMATION OR DOCUMENTATION IS REQUIRED FOR CLEARANCE / PACKAGE ABANDONED BY THE SENDER AND THE RECEIVER
	18/06/2009	9:52	ADDITIONAL CLEARING AGENCY INFORMATION OR DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER
GUANGZHOU CN	16/06/2009	17:57	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	11/06/2009	13:52	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	10/06/2009	9:51	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	09/06/2009	11:00	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	08/06/2009	11:44	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE
GUANGZHOU CN	01/06/2009	11:53	ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / DOCUMENTS OR INFO REQUESTED FROM THE CUSTOMER WERE RECEIVED AND ARE BEING PROCESSED FOR CLEARANCE

FAIL

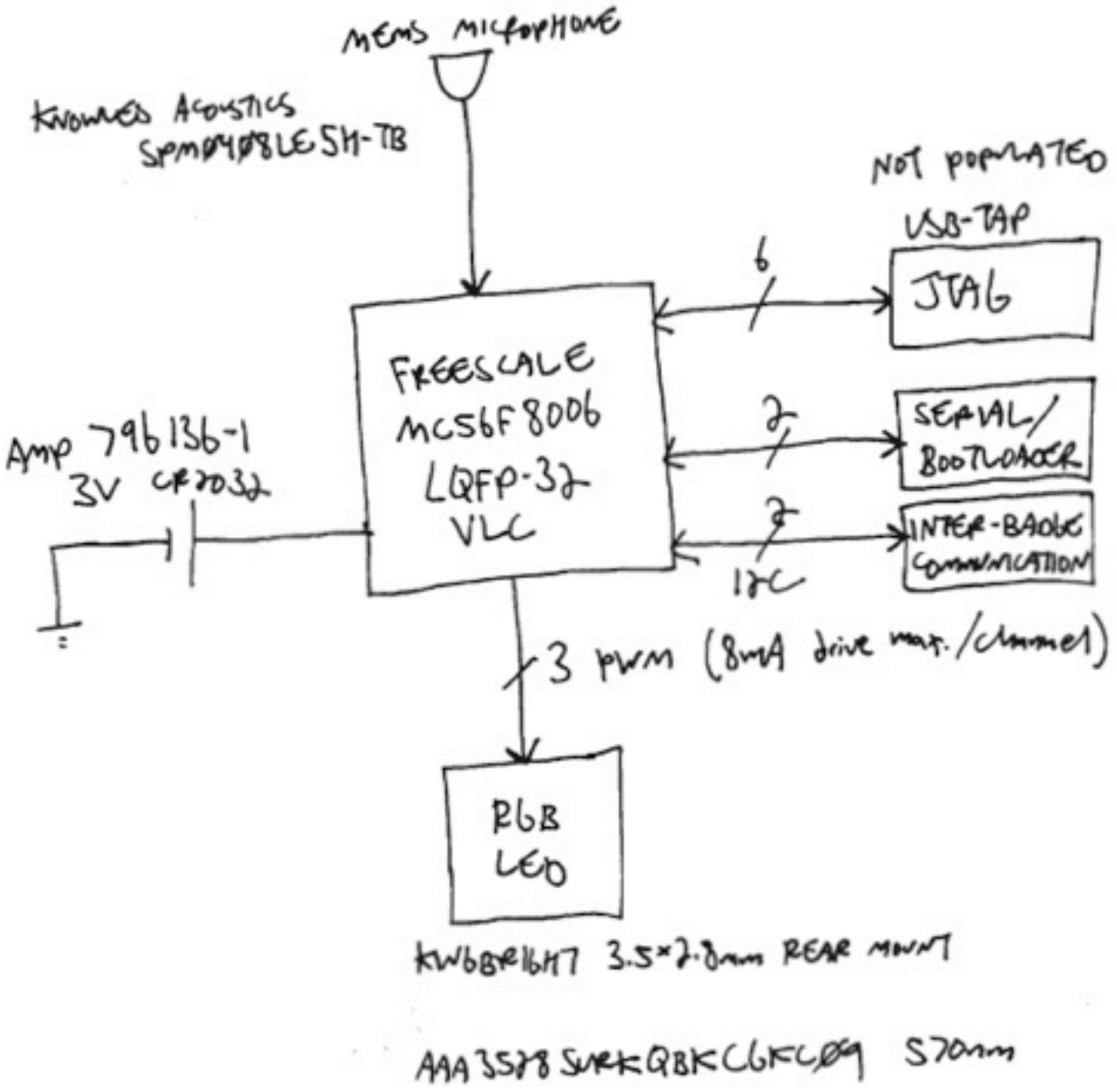
China wins!

Status:	Delivered Proof of Delivery
Delivered On:	22/07/2009 10:35
Signed By:	GUO HEXIANG
Delivered To:	CN
Shipped/Billed On:	21/05/2009
Type:	Package
Service:	EXPEDITED
Weight:	27.00 Lb

FedEx gets a small :(, too

Jul 28, 2009 10:30 PM	Shipment exception	SHENZHEN CN	Delay beyond our control

DC17 BADGE FINAL BLOCK DIAGRAM 1/14/09



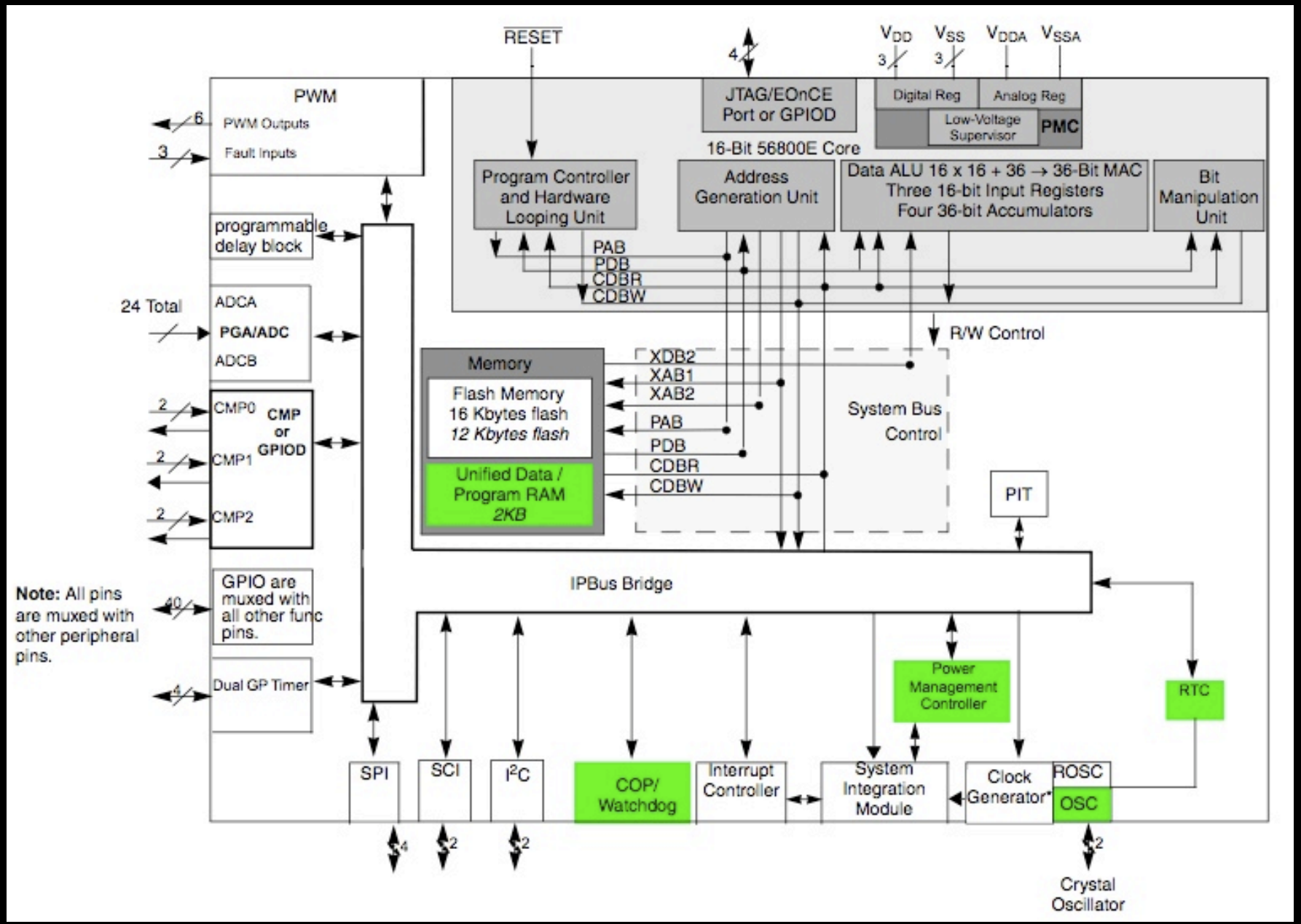
Freescale MC56F8006



- Digital Signal Controller
  - Part of the MC56F8xxx family
  - Newly released
  - Freescale gave us alpha samples to begin badge development back in November 2008
  - Main product page: `http://tinyurl.com/lyorks`
  - Direct link to data sheet: `www.freescale.com/files/dsp/doc/data_sheet/MC56F8006.pdf`
  - John Winters, co-designer of this part, is here at DEFCON!

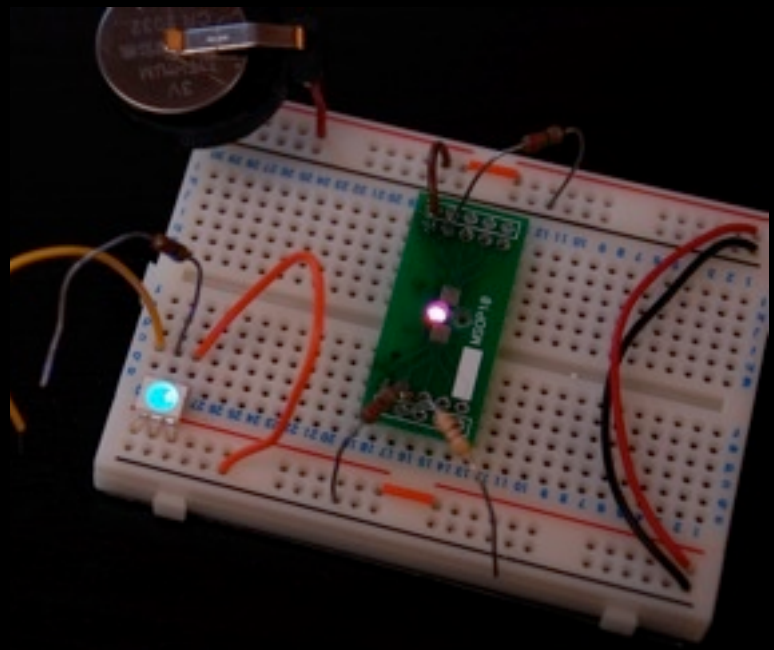
KINGPIN

Freescale MC56F8006



It's Not Easy Picking an LED





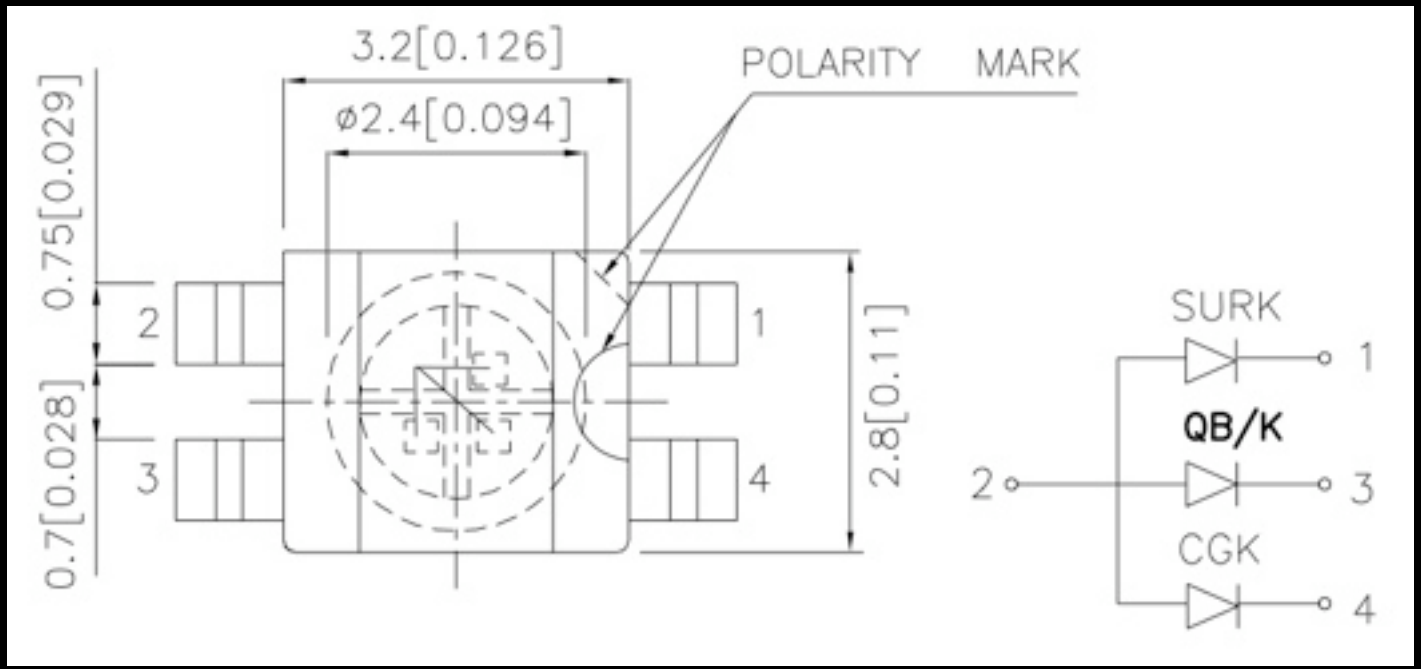




KINGPIN

Kingbright RGB LED

- AAA3528SURKQBDCGKC09
  - Rear-mounting
  - Three individual diodes in single package
  - 200/80/90mcd @ 20mA (R/G/B)



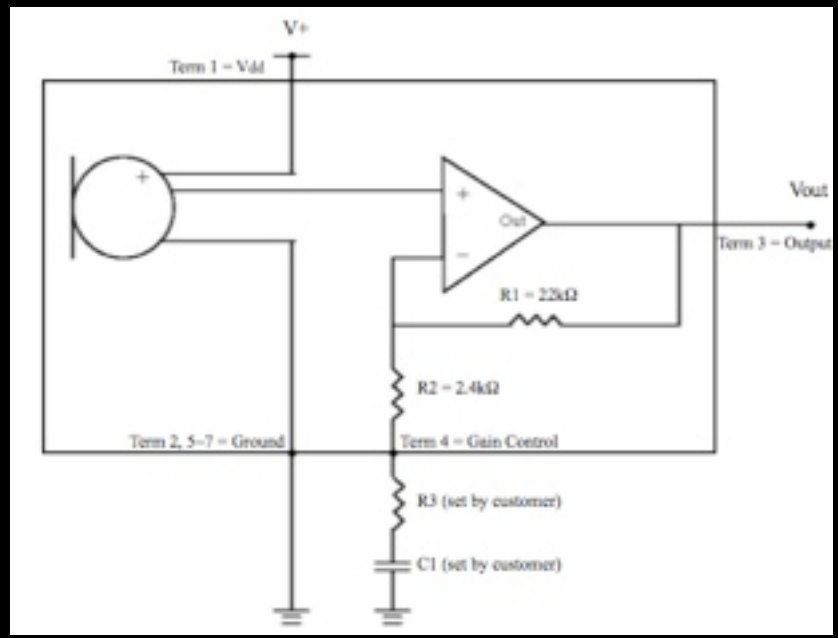
Knowles Acoustics Microphone

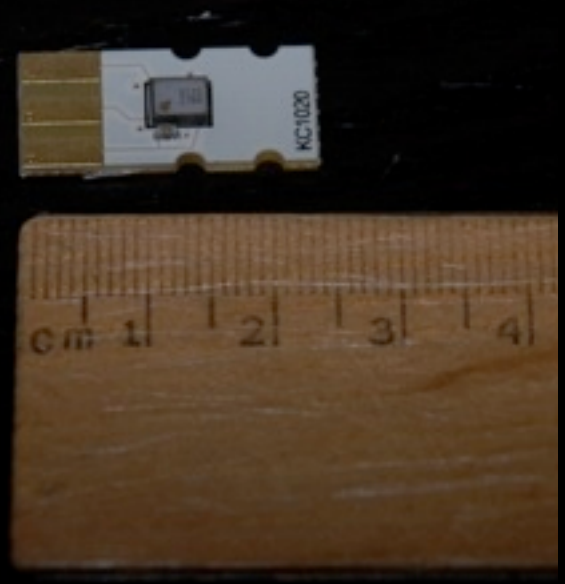
- Dr. Hugh Knowles developed first balanced armature receiver for hearing aids
- Developed the first silicon/MEMS microphone in 1988
- First moon landing: Neil Armstrong was wearing a Plantronics headset with Knowles microphone
- Nearly 1 billion sold
  - Used in laptops, cellphones, headsets
- www.knowles.com

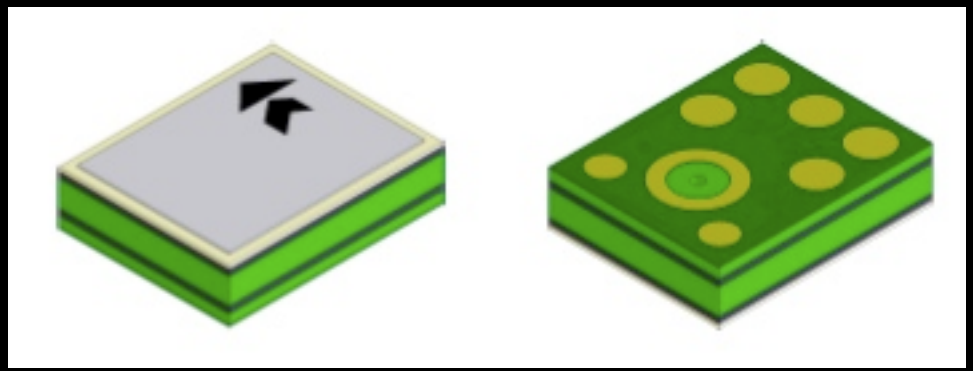


Knowles Acoustics Microphone 2

- ★ SPM0408LE5H-TB
  - ◉ Rear-mounting
  - ◉ Amplified (20dB gain)
  - ◉ RF protected



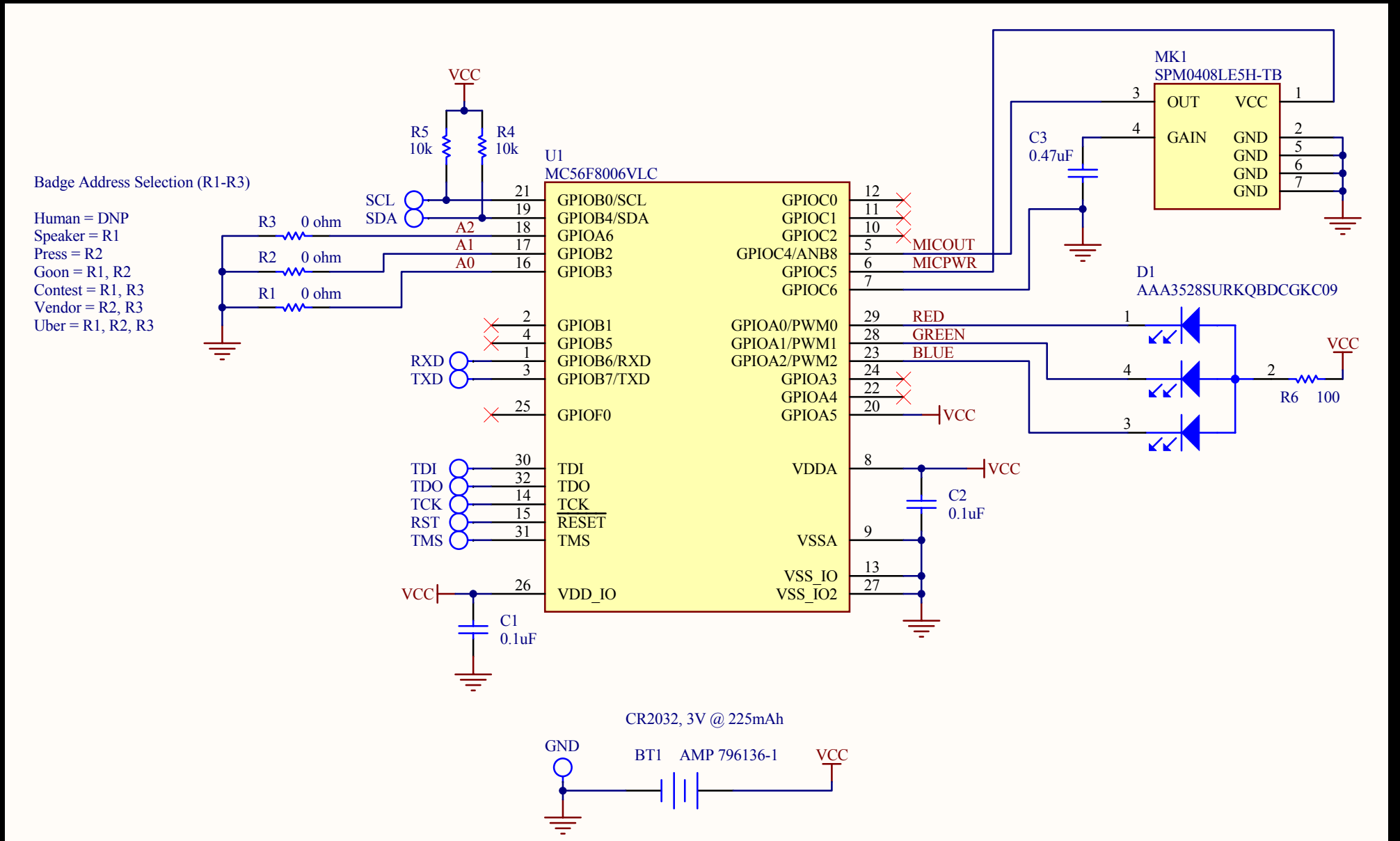




Development Hardware



Freescale MC56F8006-DEMO board + custom circuitry


Badge Address Selection (R1-R3)
Human = DNP
Speaker = R1
Press = R2
Goon = R1, R2
Contest = R1, R3
Vendor = R2, R3
Uber = R1, R2, R3
VCC
R5 10k
R4 10k
U1
MC56F8006VLC
SCL
SDA
R3 0 ohm
R2 0 ohm
R1 0 ohm
A2
A1
A0
GPIOB0/SCL
GPIOB4/SDA
GPIOA6
GPIOB2
GPIOB3
GPIOB1
GPIOB5
GPIOB6/RXD
GPIOB7/TXD
GPIOF0
RXD
TXD
TDI
TDO
TCK
RST
TMS
VDD_IO
C1 0.1uF
GPIOC0
GPIOC1
GPIOC2
GPIOC4/ANB8
GPIOC5
GPIOC6
GPIOA0/PWM0
GPIOA1/PWM1
GPIOA2/PWM2
GPIOA3
GPIOA4
GPIOA5
VDDA
VSSA
VSS_IO
VSS_IO2
MICOUT
MICPWR
RED
GREEN
BLUE
C2 0.1uF
MK1
SPM0408LE5H-TB
OUT
GAIN
VCC
GND
C3 0.47uF
D1
AAA3528SURKQBDCGKC09
R6 100
CR2032, 3V @ 225mAh
GND
BT1 AMP 796136-1

Schematic

Bill-of-Materials

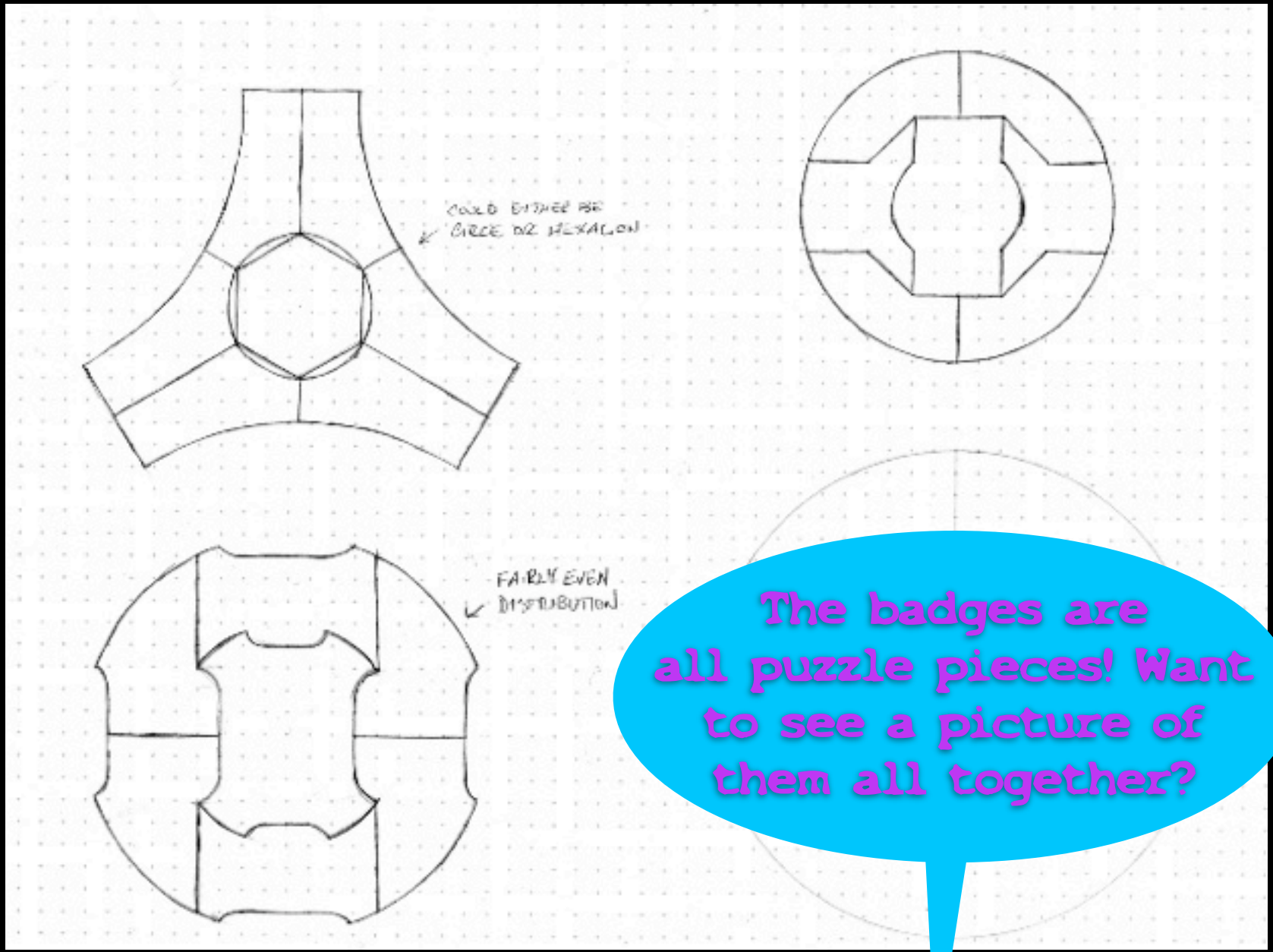
DEFCON 17 Circuit Board Badge
Bill-of-Materials

Note: Refer to schematic for R1, R2, R3 population requirements

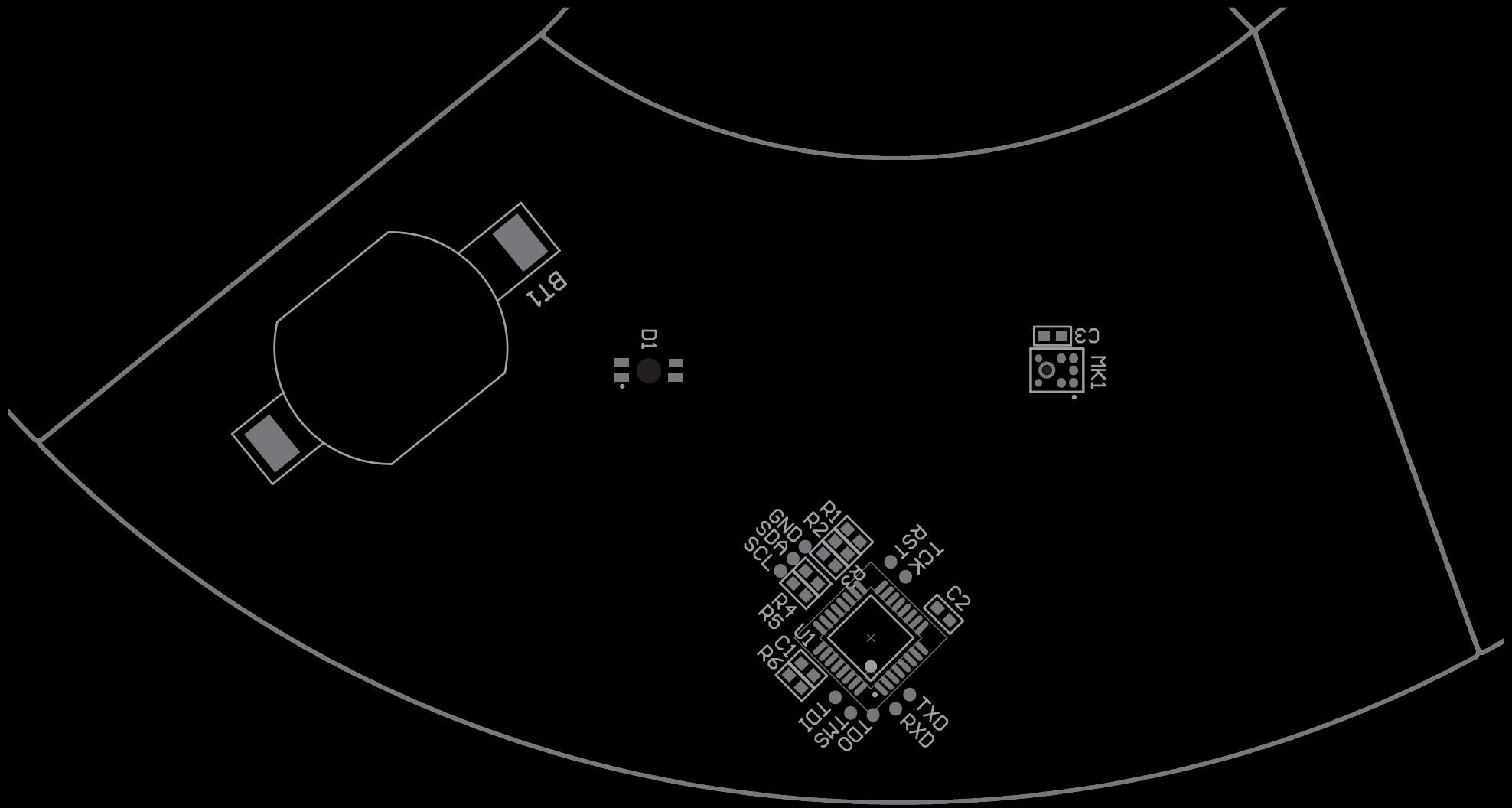
Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	1	BT1	AMP	796136-1	Digi-Key	A99327-ND	Single-cell battery holder for CR2032, SMD
1a	1	N/A	Panasonic	CR2032	Digi-Key	P189-ND	CR2032 Lithium 3V Coin Cell Battery (225mAh)
2	2	C1,C2	Kemet	C0603C104K4RACTU	Digi-Key	399-1096-2-ND	0.1uF ceramic capacitor, 16V, X7R, 0603
3	1	C3	Kemet	C0603C474K4RACTU	Digi-Key	399-4922-2-ND	0.47uF ceramic capacitor, 16V, X7R, 0603
4	1	D1	Kingbright	AAA3528SURKQBDCGKC09	N/A	N/A	LED, RGB, 200/80/90mcd @ 20mA, 3.5mm x 2.8mm, SMD
5	1	MK1	Knowles Acoustics	SPM0408LE5H-TB	N/A	N/A	Microphone, 20dB internal pre-amp, SMD
6	3	R1,R2,R3	Panasonic	ERJ-3GEY0R00V	Digi-Key	P0.0GTR-ND	0 ohm, 5%, 1/10W, 0603
7	2	R4,R5	Panasonic	ERJ-3GEYJ103V	Digi-Key	P10KGTR-ND	10k, 5%, 1/10W, 0603
8	1	R6	Panasonic	ERJ-3GEYJ101V	Digi-Key	P100GTR-ND	100, 5%, 1/10W, 0603
9	1	U1	Freescale	MC56F8006VLC	Avnet	N/A	Microcontroller/Digital Signal Controller, LQFP32
9a	1	N/A	N/A	N/A	Avnet	N/A	Microcontroller programming service
10	1	PCB	e-Teknet	DC17 1.0	N/A	N/A	PCB (includes assembly and testing)



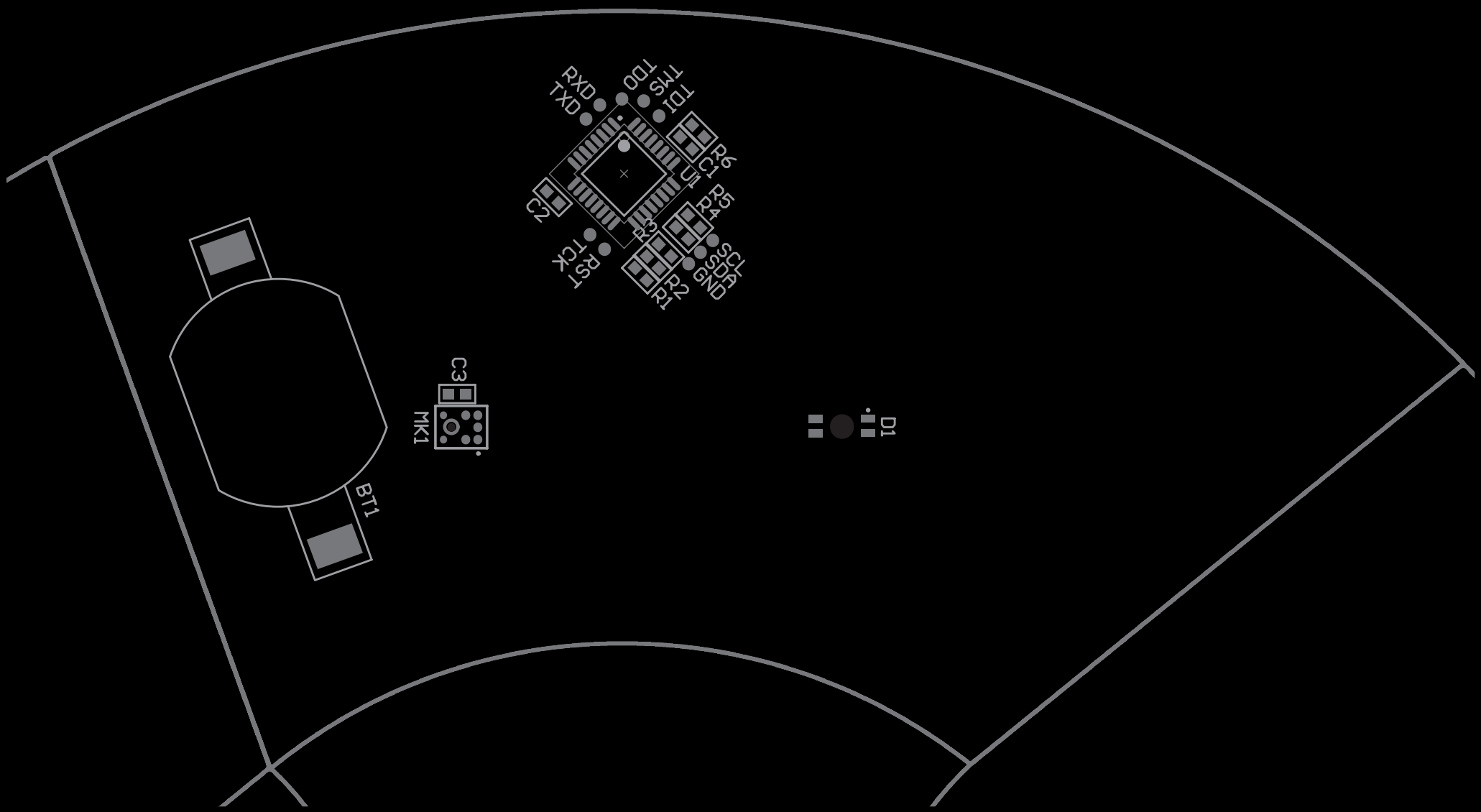
Badge Shape Concepts



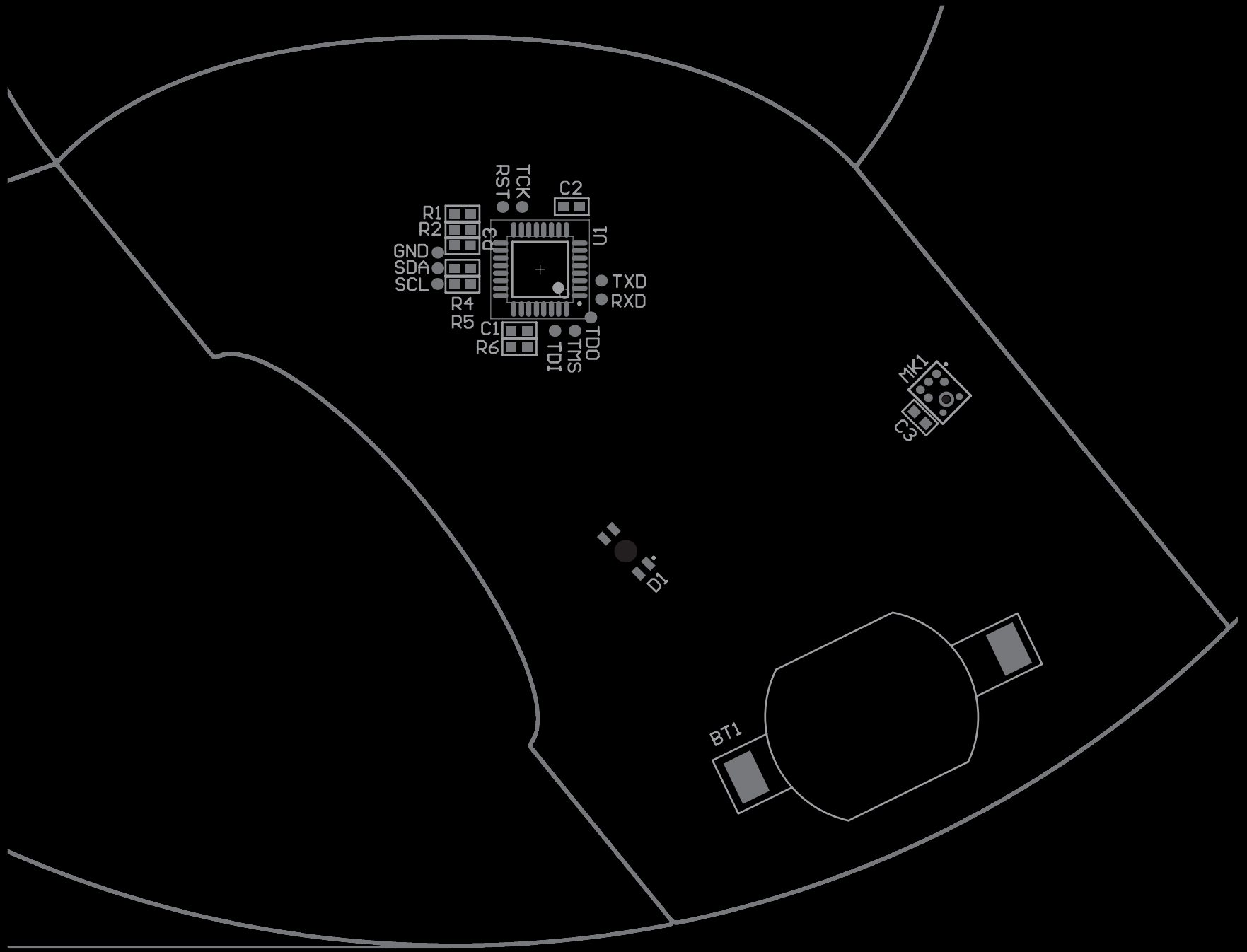
The badges are all puzzle pieces! Want to see a picture of them all together?



Assembly Drawing: Human

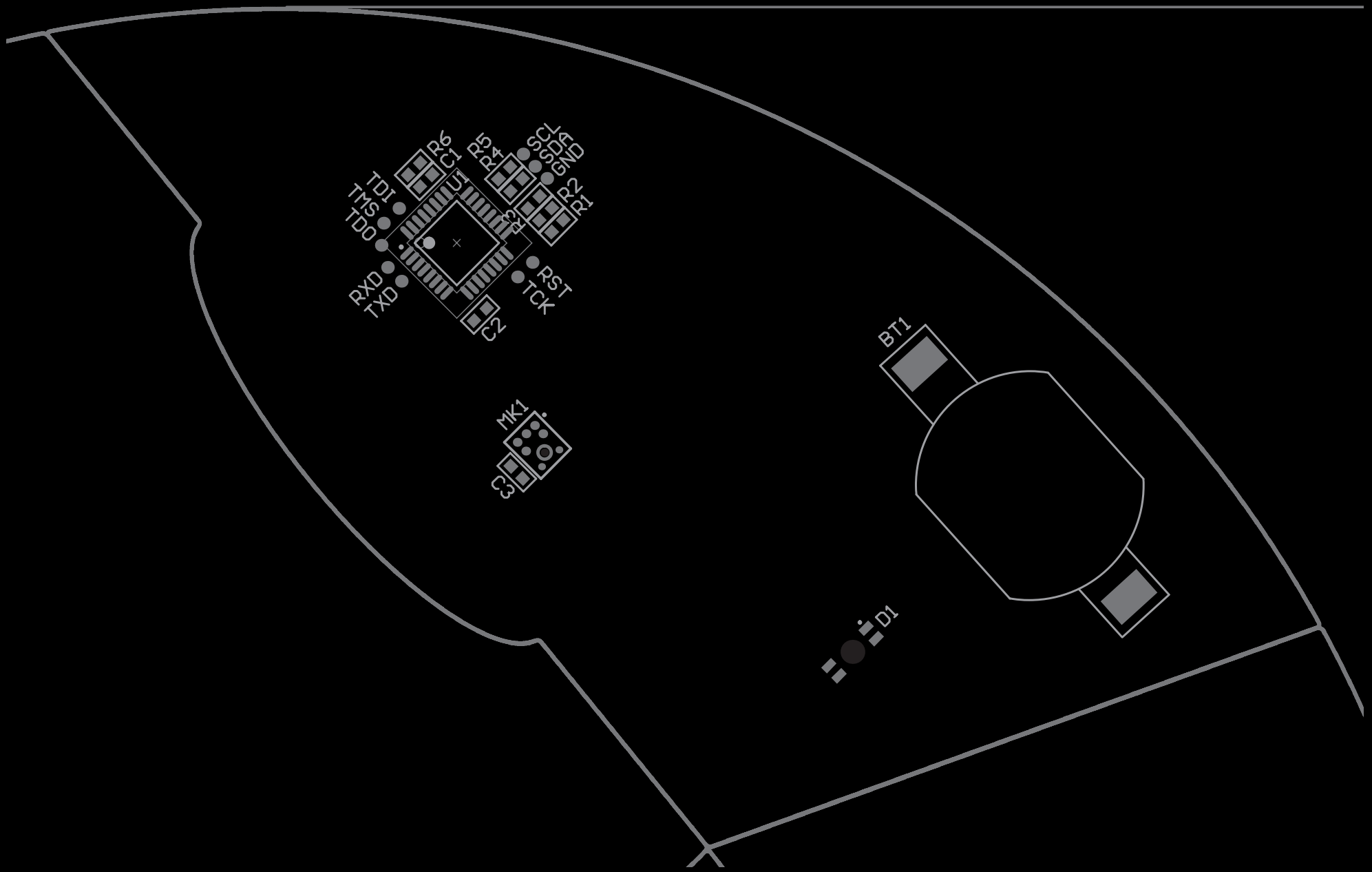


Assembly Drawing: Speaker

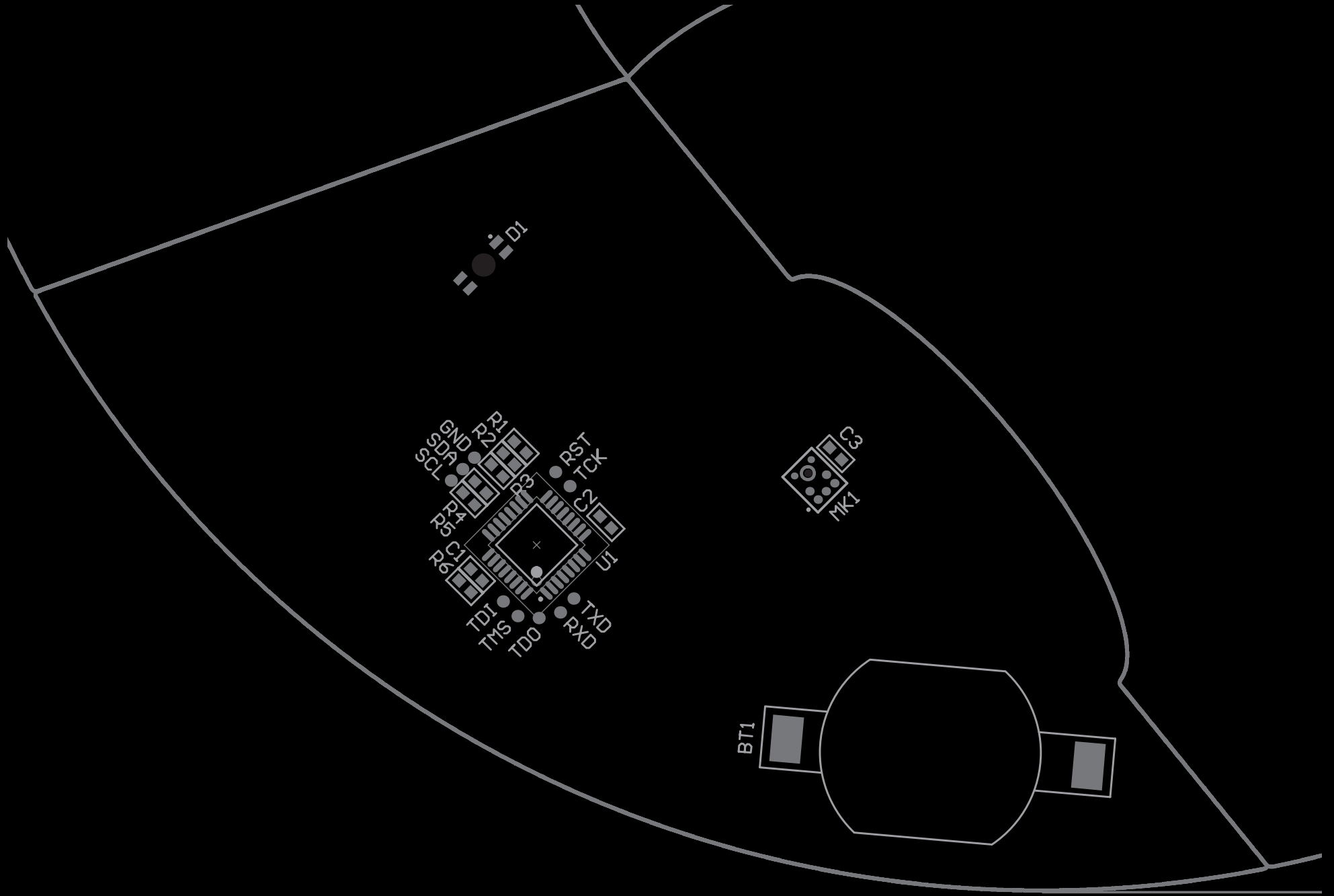


Assembly Drawing: Goon

KINGPIN

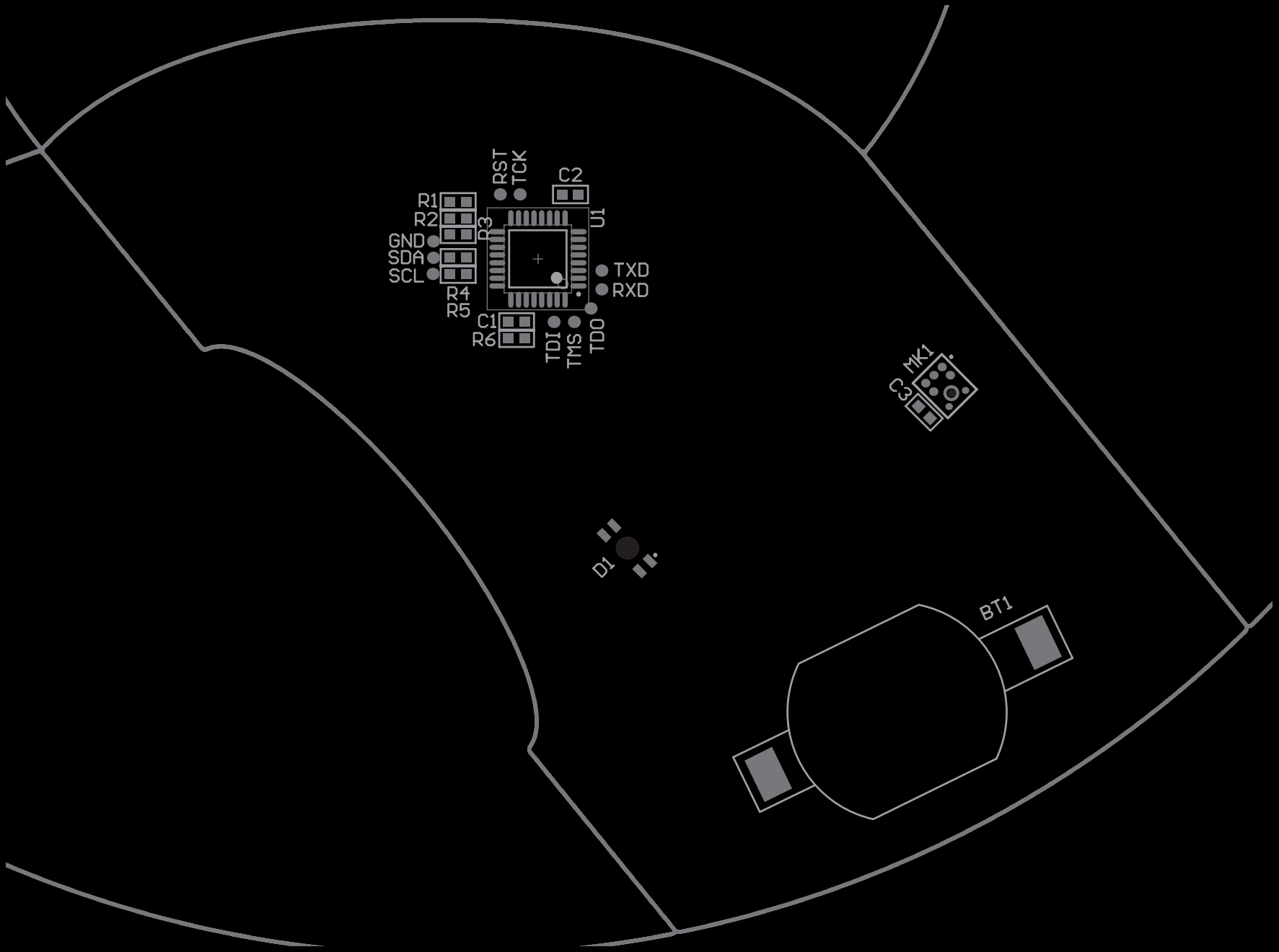


Assembly Drawing: Vendor

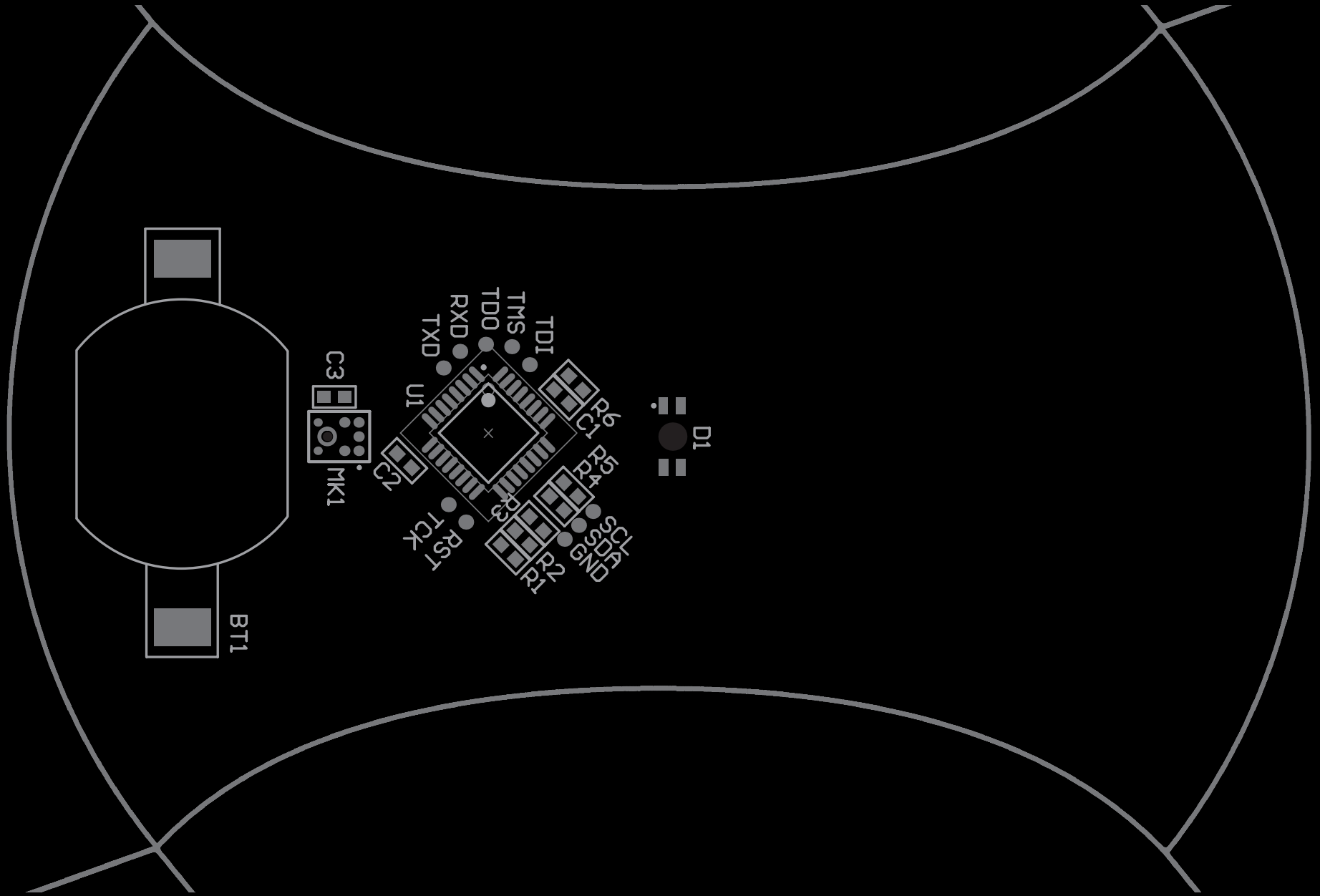


Assembly Drawing: Contest

KINGPIN

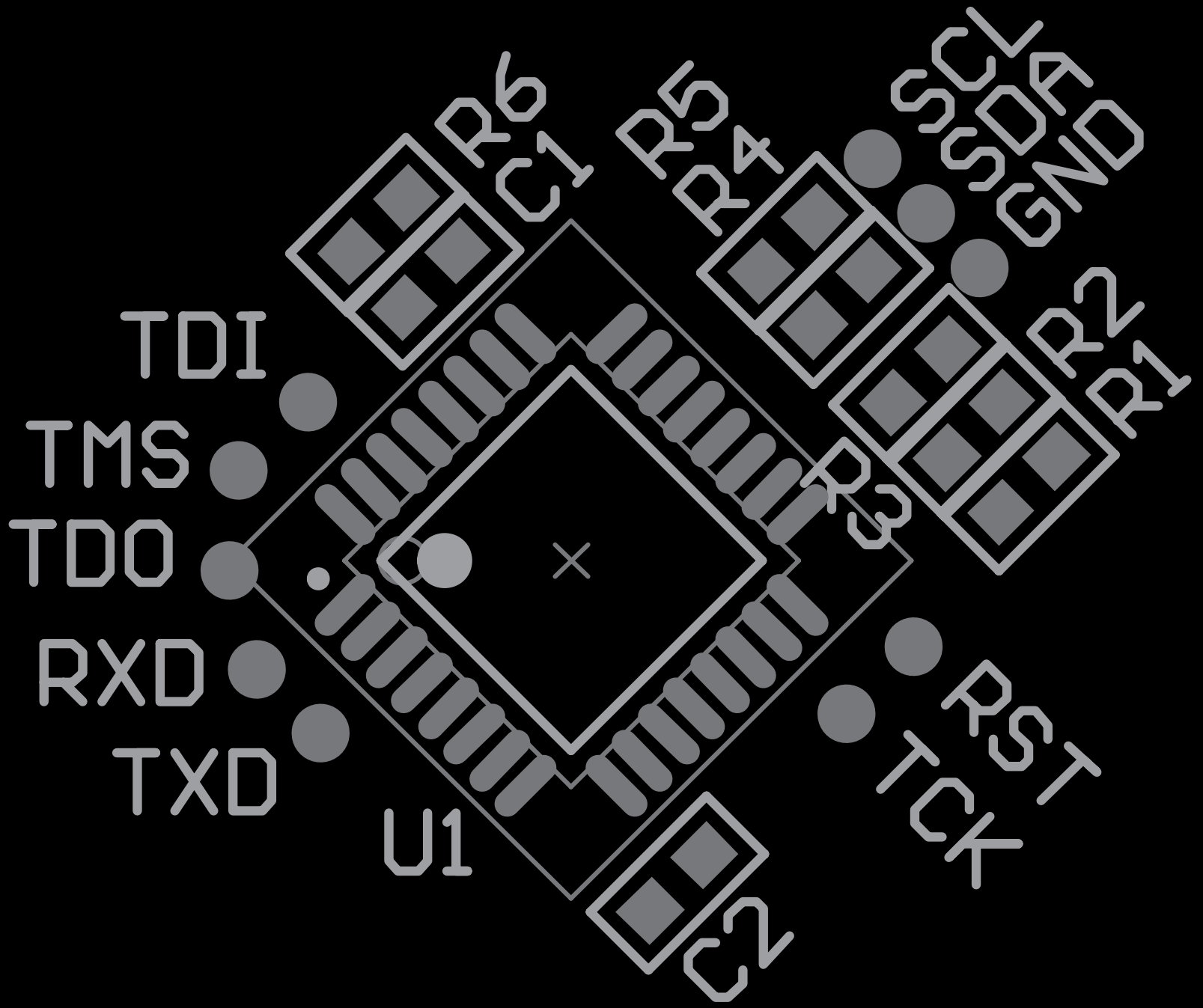


Assembly Drawing: Press



Assembly Drawing: Uber

KINGPIN



Assembly Drawing: Close-Up

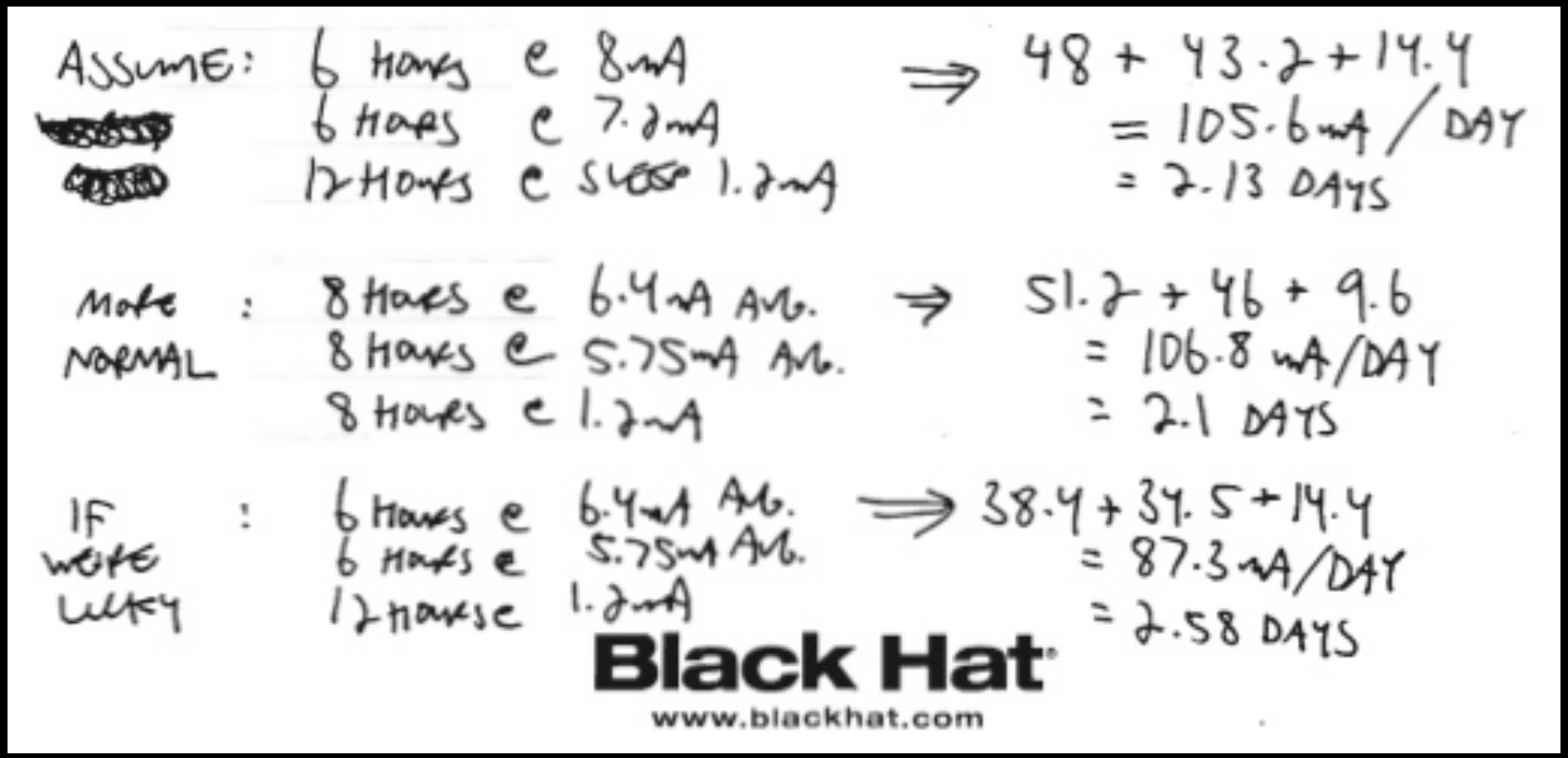
DC17 BADGE FINAL POWER MEASUREMENTS

VCC = 3V

MODE	CURRENT
IDLE/RGB BLEND	4.8mA - 8mA
DANCE/COLOR ORGAN	4.3mA - 7.2mA
SLEEP	1.2mA

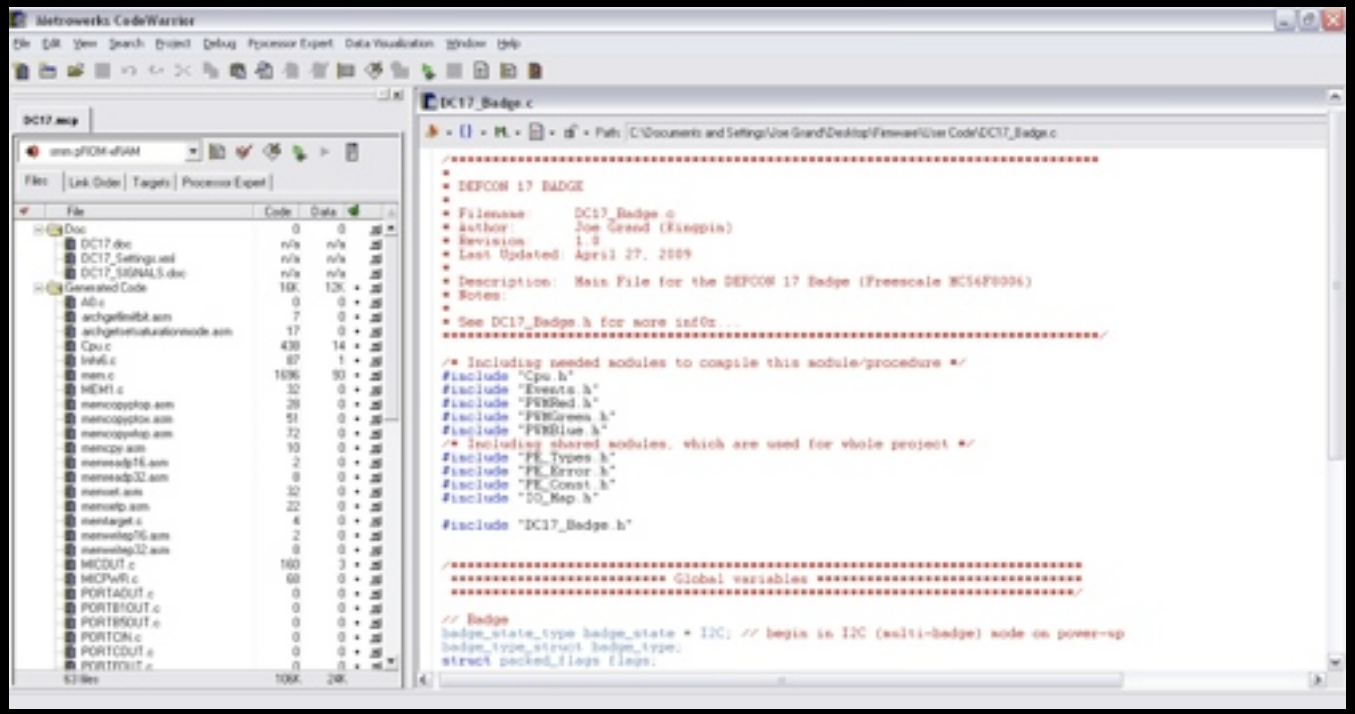
WE USE CR2032 = 225mAh → 2V

Battery Life Estimates



Development Environment

Freescale CodeWarrior for 56800/E Digital Signal Controllers

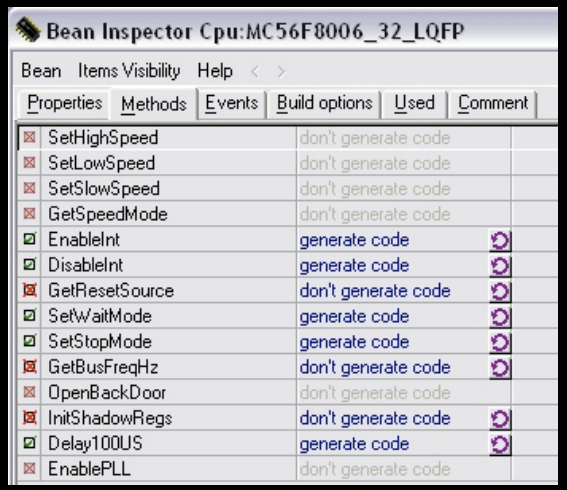


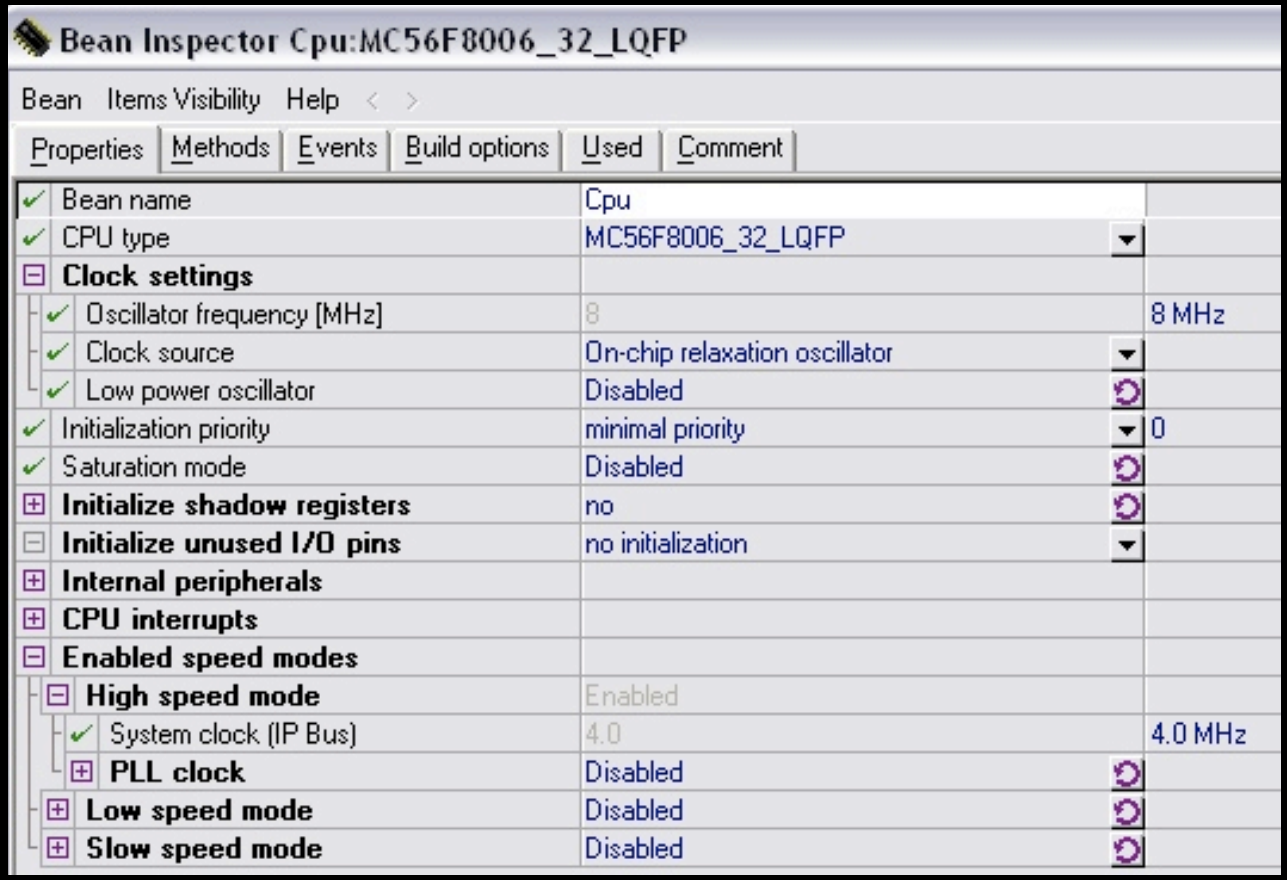
- ★ Free for up to 16KB Flash
- ★ All tools on DEFCON CD (for real, this time)
- ★ `http://tinyurl.com/kuwloq`

KINGPIN

Development Environment 2

Processor Expert





- ★ GUI for peripheral configuration
- ★ Generates required drivers/function code for desired modules

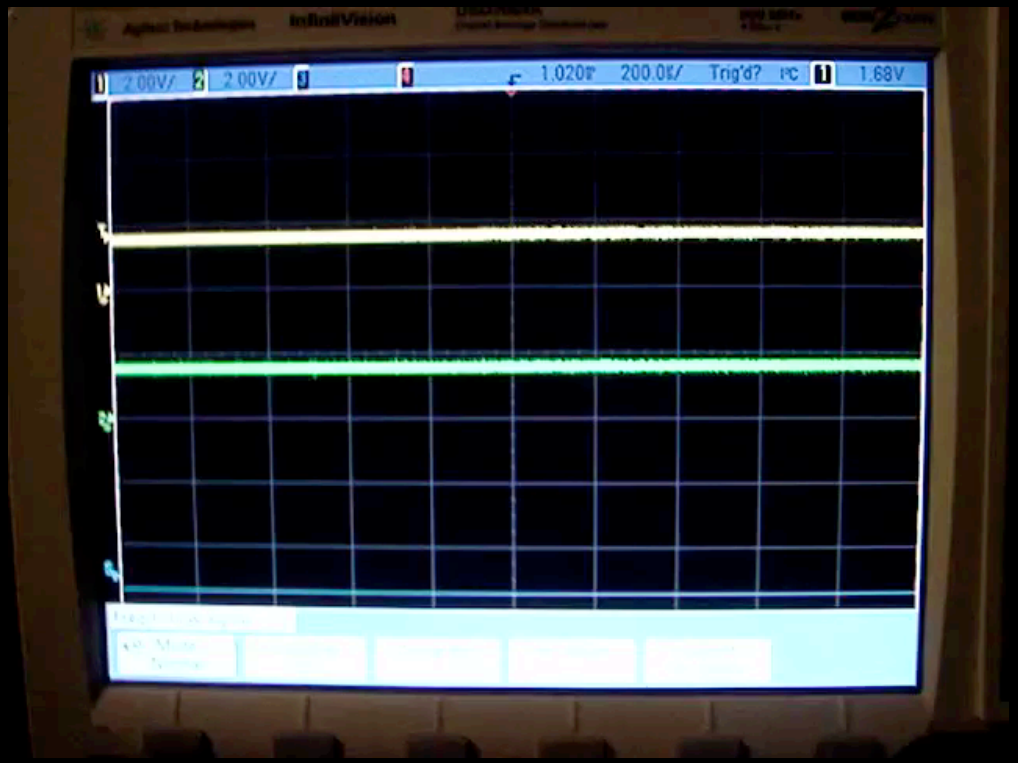
Fast Fourier Transform (FFT)

- ★ Audio/signal processing function
- ★ Separates input signal from mic into N discrete bins (frequency elements)
- ★ Calculates power of each bin
- ★ RGB LED color and brightness vary based on sound/frequency



Badge-to-Badge Communication

- I2C
  - SCL (Serial Clock)
  - SDA (Serial Data)
  - GND
- Human = Master
- Non-Human = Slaves

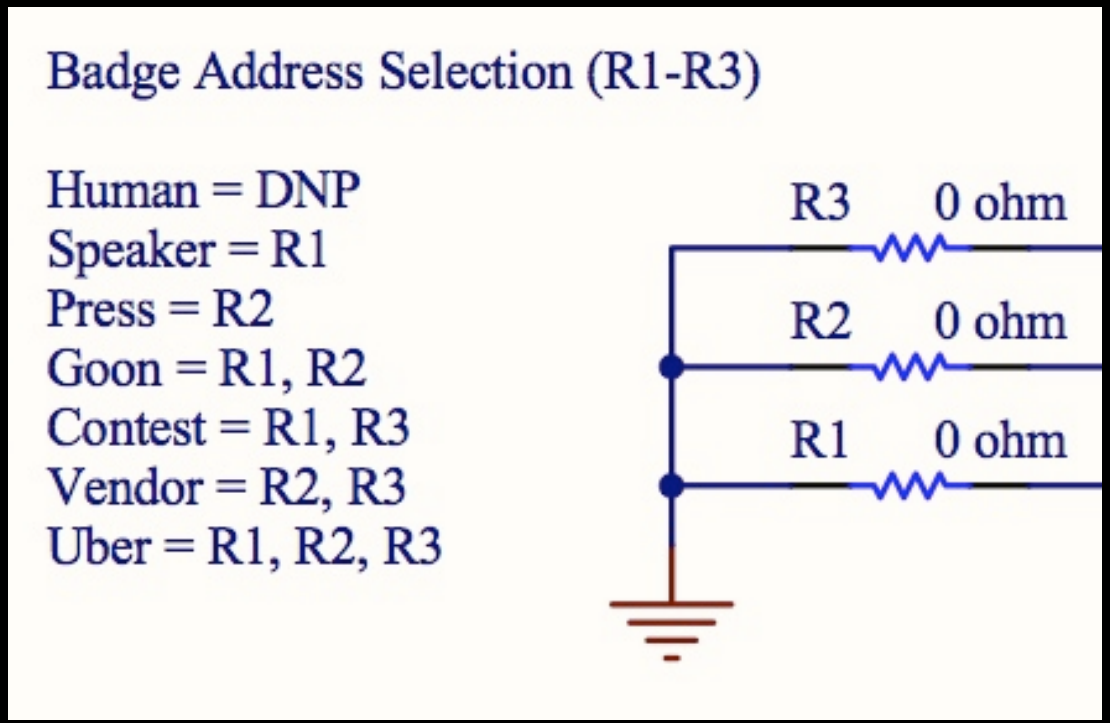


- As long as they are all on the bus, it doesn't matter what order they are connected
- Master only checks for slaves on power-up
  - Make sure slave badges are on, then power master

KINGPIN

Badge-to-Badge Communication 2

- ★ Individually addressable
  - ◉ Three resistors for setting device address
- ★ Data format (7 bytes)
  - ◉ Address (1) : Red (2) : Green (2) : Blue (2)

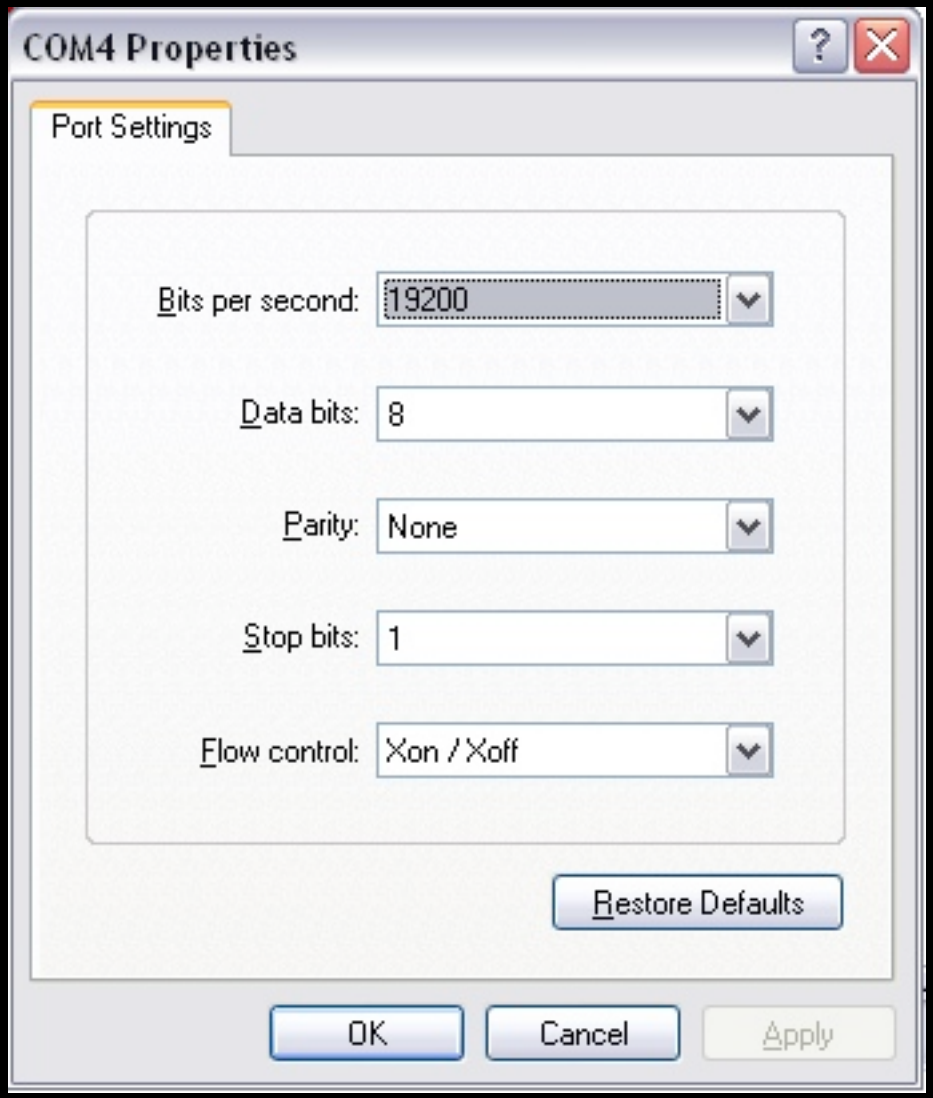


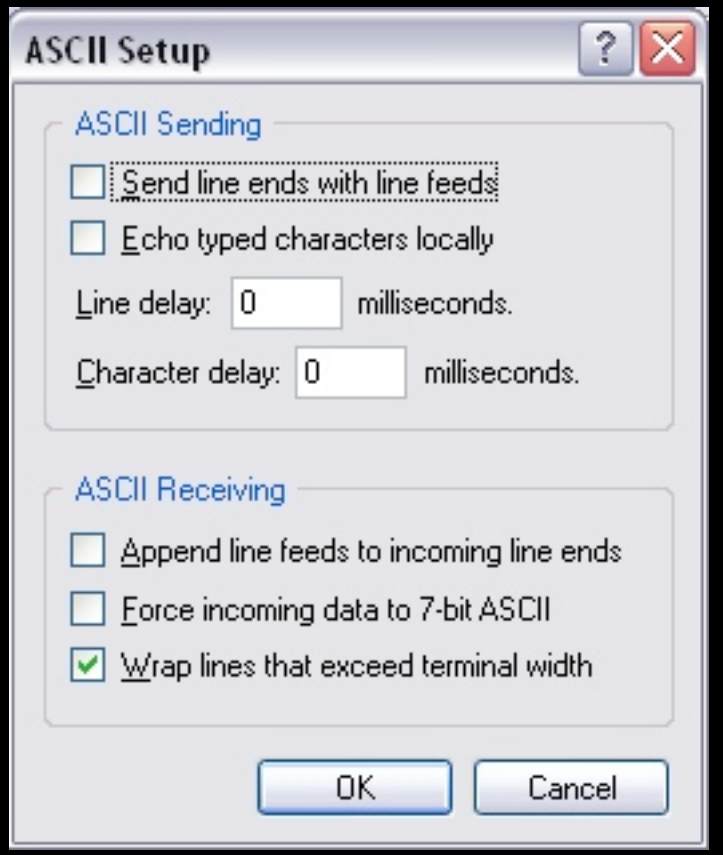
Static Serial Bootloader

- ★ Serial port + HyperTerminal = Load your own firmware onto the badge
  - ◉ TX, RX, GND
  - ◉ Level-shifter required (HHV kit!)
- ★ Enabled for 10 seconds on power-up
- ★ When modifying the User Code, read the comments in cpu.c
  - ◉ Need to ensure reset vector points to bootloader and not user code
    - Otherwise, you'll never be able to get to the bootloader

KINGPIN

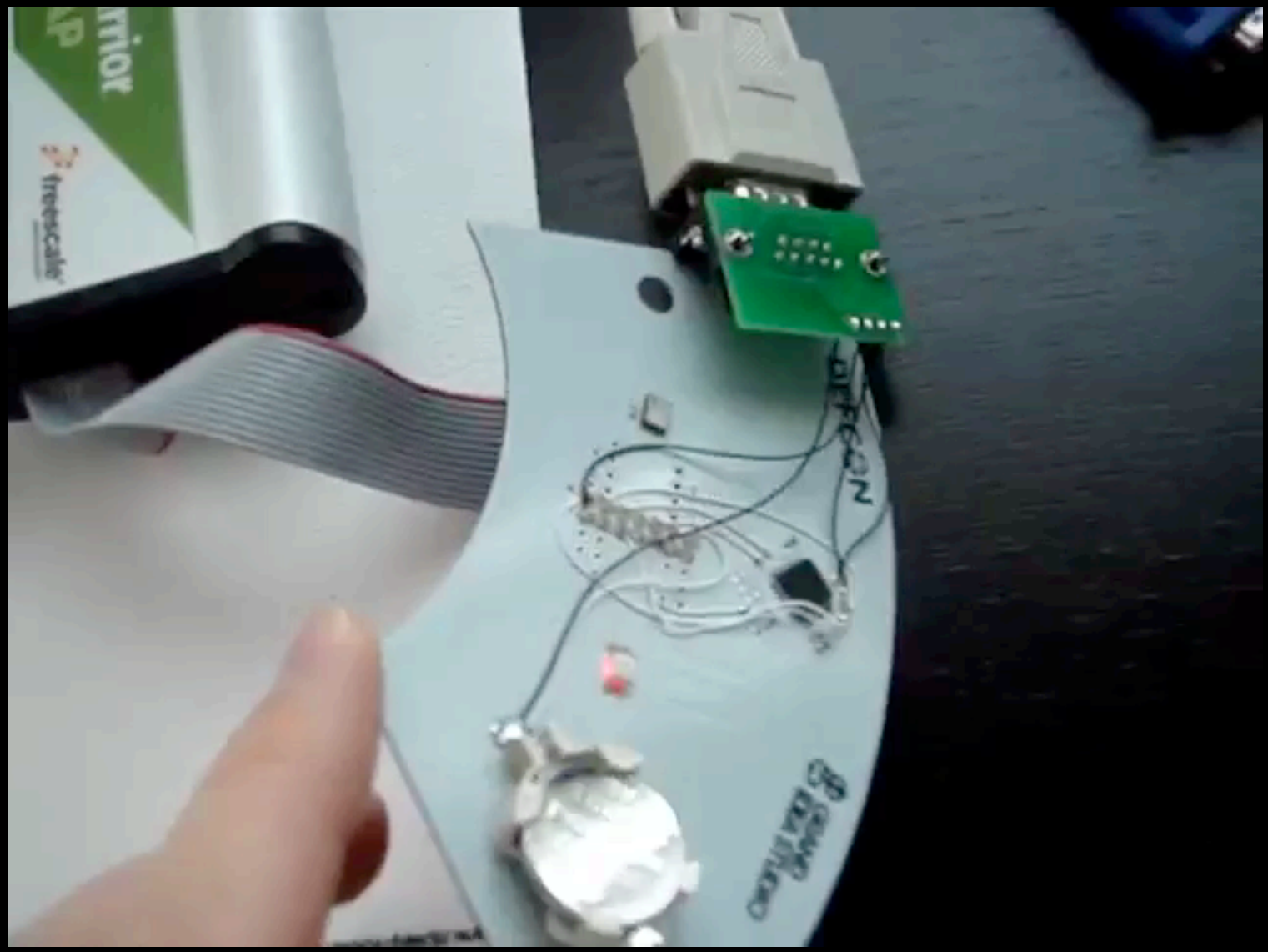
Static Serial Bootloader 2





Static Serial Bootloader 3

★ Simply upload hex file and the badge will do the rest...



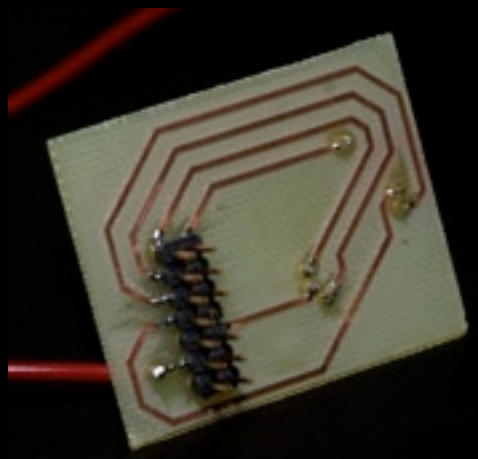
Break Glass In Case Of Bricking

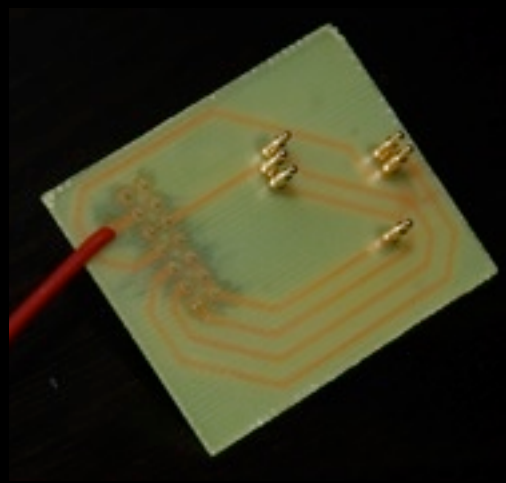
- ★ MC56F8006 typically programmed through JTAG interface
  - ◉ Uses CodeWarrior USB TAP hardware, `www.freescale.com/webapp/sps/site/prod_summary.jsp?code=USBTAP`
- ★ But, there is no direct JTAG connector on the badge



Break Glass In Case Of Bricking

- I built a small header board that connects to the JTAG test points on the badge using pogo pins
- Unit will be available in the Hardware Hacking Village for emergencies
- You could solder a 2x7 male header onto prototyping area of the badge and connect wires to test points



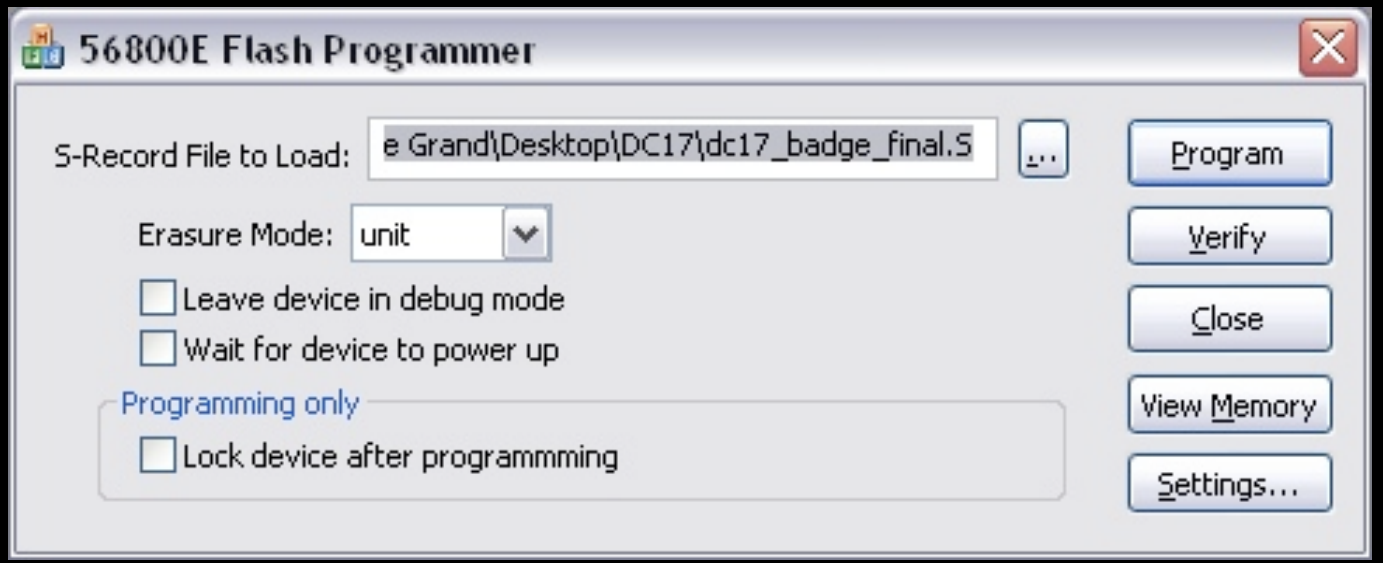




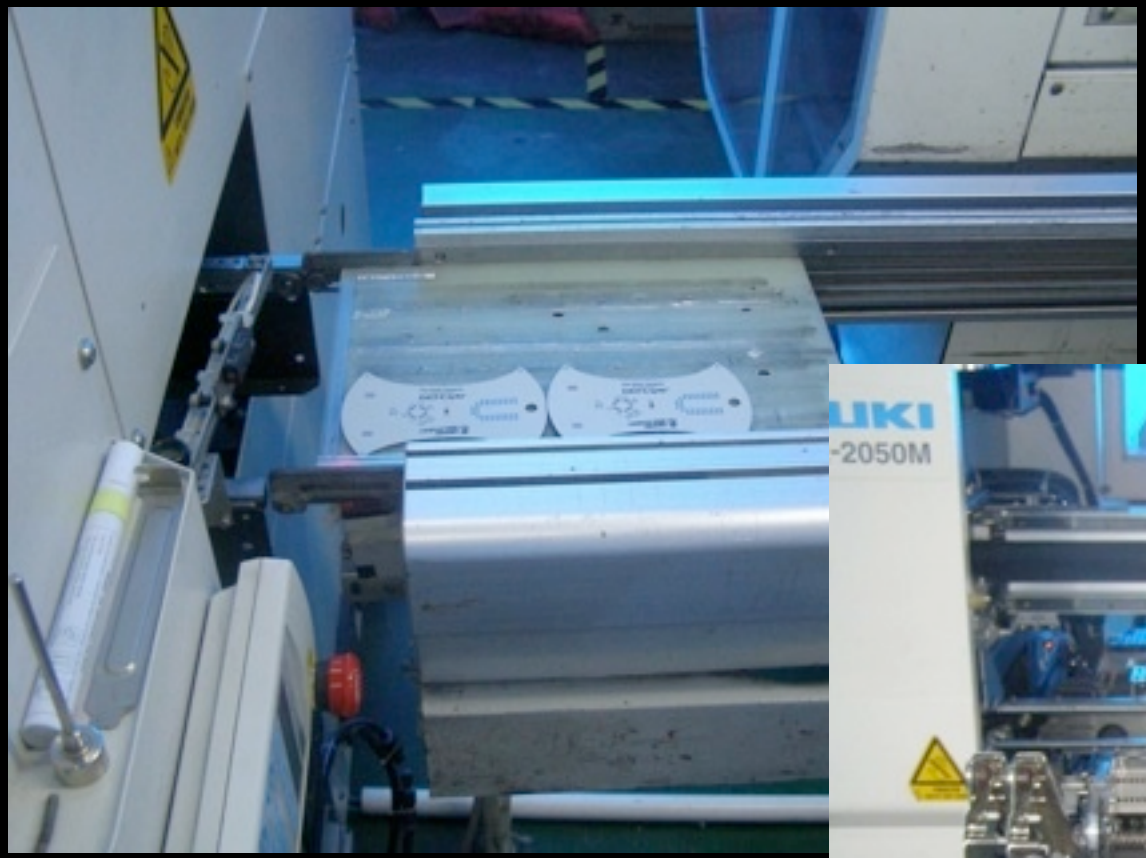
KINGPIN

Break Glass In Case Of Bricking

- ★ Use in conjunction with CodeWarrior or 56800E Flash Programmer tool to reload original firmware (including new bootloader)

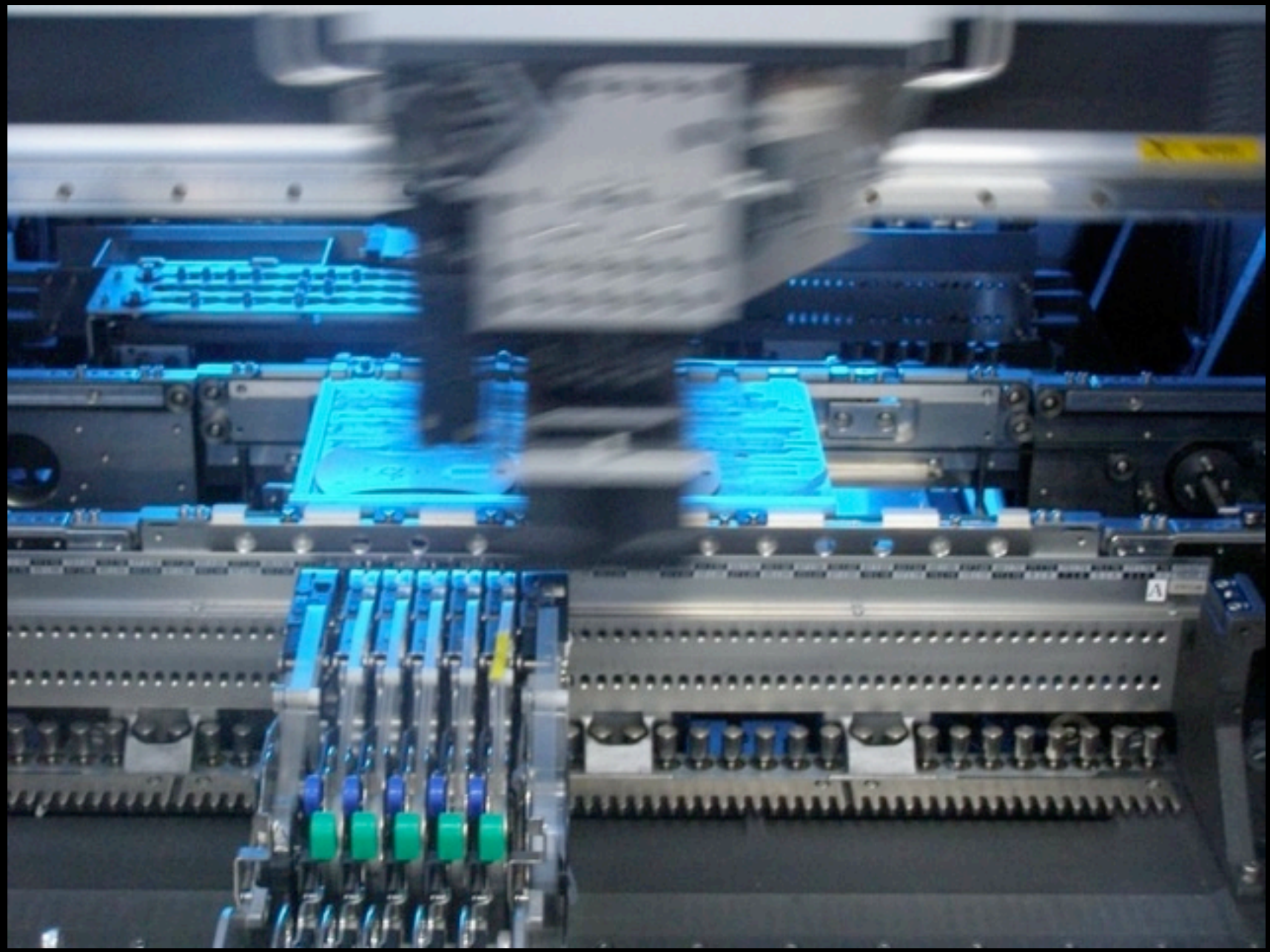


Production Assembly @ e-Teknet





Production Assembly @ e-Teknet



Production Assembly @ e-Teknet



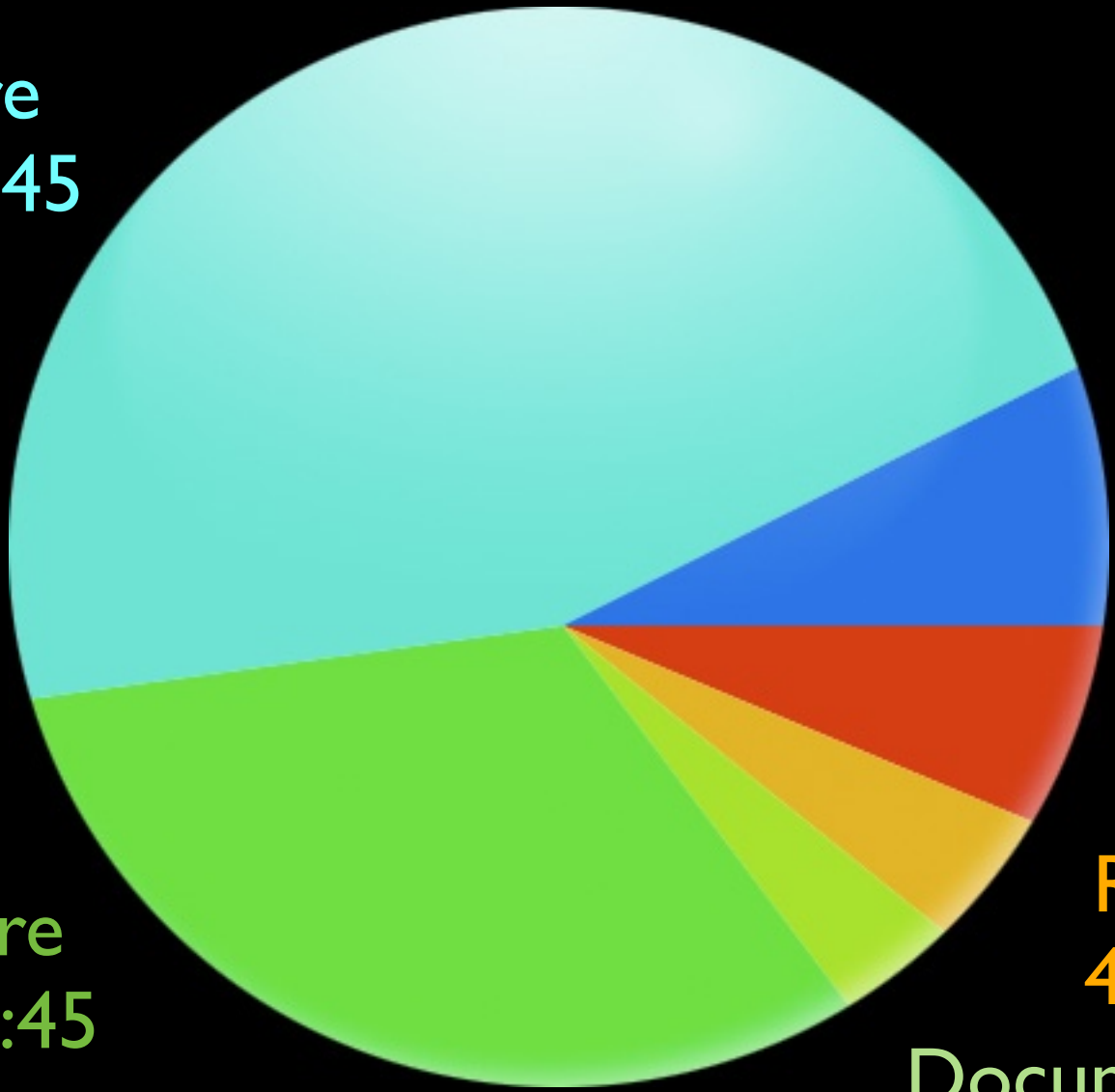
Total Badge Types



Speaker = 200
Goon = 200
Press = 200
Vendor = 100
Contest = 100
Uber = 50
Human = 5844

Total = 6694

A Labor of Love...



Firmware
44.5% 82:45

Admin
7.8% 14:35

Meetings
6.5% 12:05

Research
4.6% 8:30

Documentation
3.9% 7:20

Hardware
32.7% 60:45

TOTAL: 186 hours

KINGPIN

Badge Hacking Contest

Now w/ Black Badge status!

Badge Hacking Contest HQ @ Hardware Hacking Village

Submissions due to Kingpin @ HHV by 2pm Sunday

Previous results at www.grandideastudio.com/portfolio/defcon-14-badge, /defcon-15-badge, & /defcon-16-badge

Complete source code, schematics, etc. on DEFCON CD

KINGPIN

This project did not happen in a vacuum.

Freescale (esp. John Winters, Dennis Hicks, Erin Greene, Chris Coleman, William Jiang)

e-Teknet - PCB manufacturing & assembly (esp. Mike, Sam, Thomas, Kitty)

The Dark Tangent, Black Beetle, Neil



Keely & Ben


DEFCON
THE END!
KP@KINGPINEMPIRE.COM
WWW.GRANDIDEASTUDIO.COM