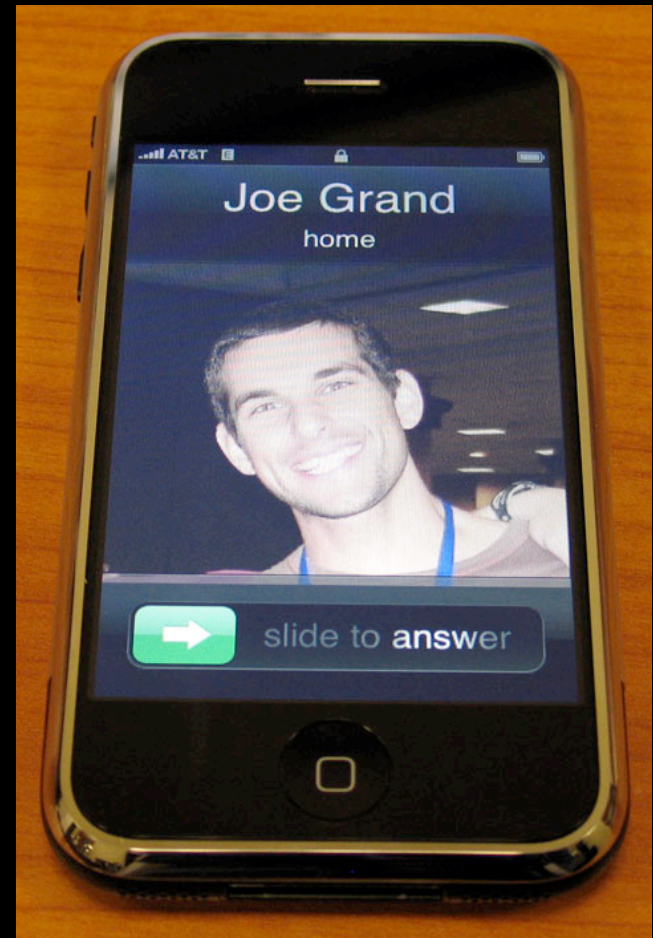


by



*Dateline NBC
Undercover Camera*



Contact a **GOON!**

Have you seen me?

An Ode to the DEFCON 15 Badge...



josh fernandez, poet extraordinaire

170 hours...

2 nights of my honeymoon...

3 PCB revisions...

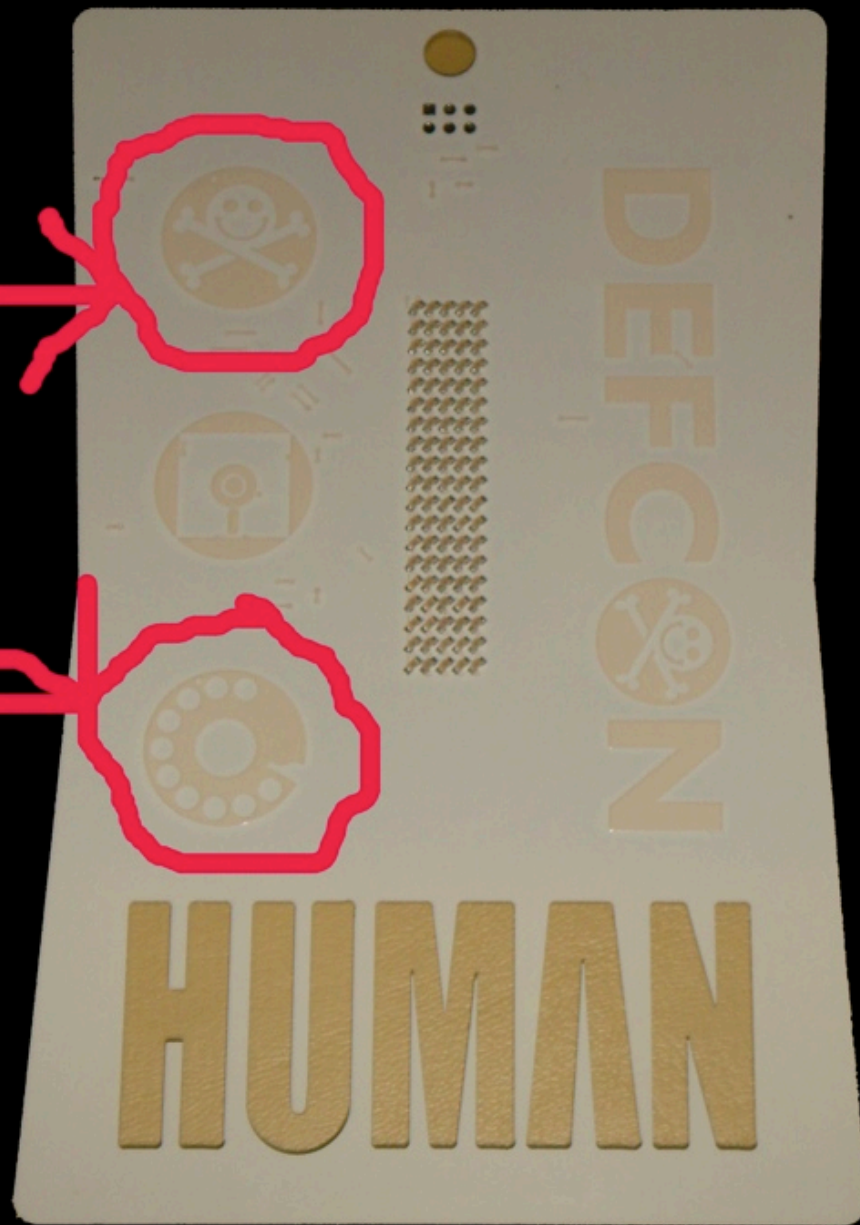
863,600 total components...

6,800 hackers...

kingpin

SW1

SW2



kingpin

BDM Prog. & Debug Connector (2x3 header)

74HC595 Shift Registers (3x)

QT100 Cap. Sensor

MC9508QG8 Micro MMA7260QT Accelerometer

MC13191FC Wireless TX/RX (w/ On-Board Antennas)

QT100 Cap. Sensor

LDO Reg. 2.5V

LDO 2.5V Reg.

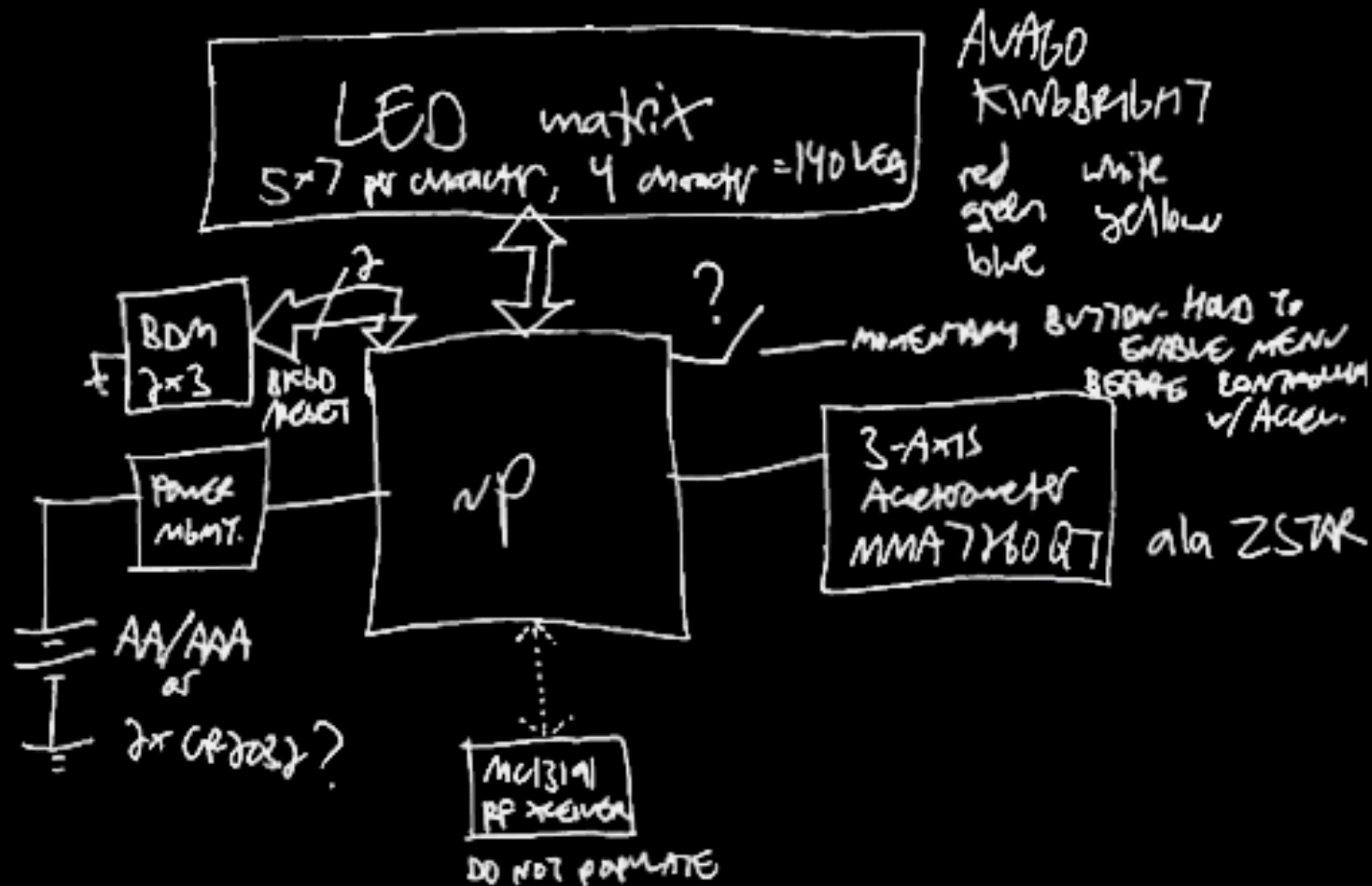
Batteries (2x CR2032) 6V



kingpin

Preliminary block diagram...

DEFCON IS ABOVE CONCEPT REMEMBERED 2/9/07



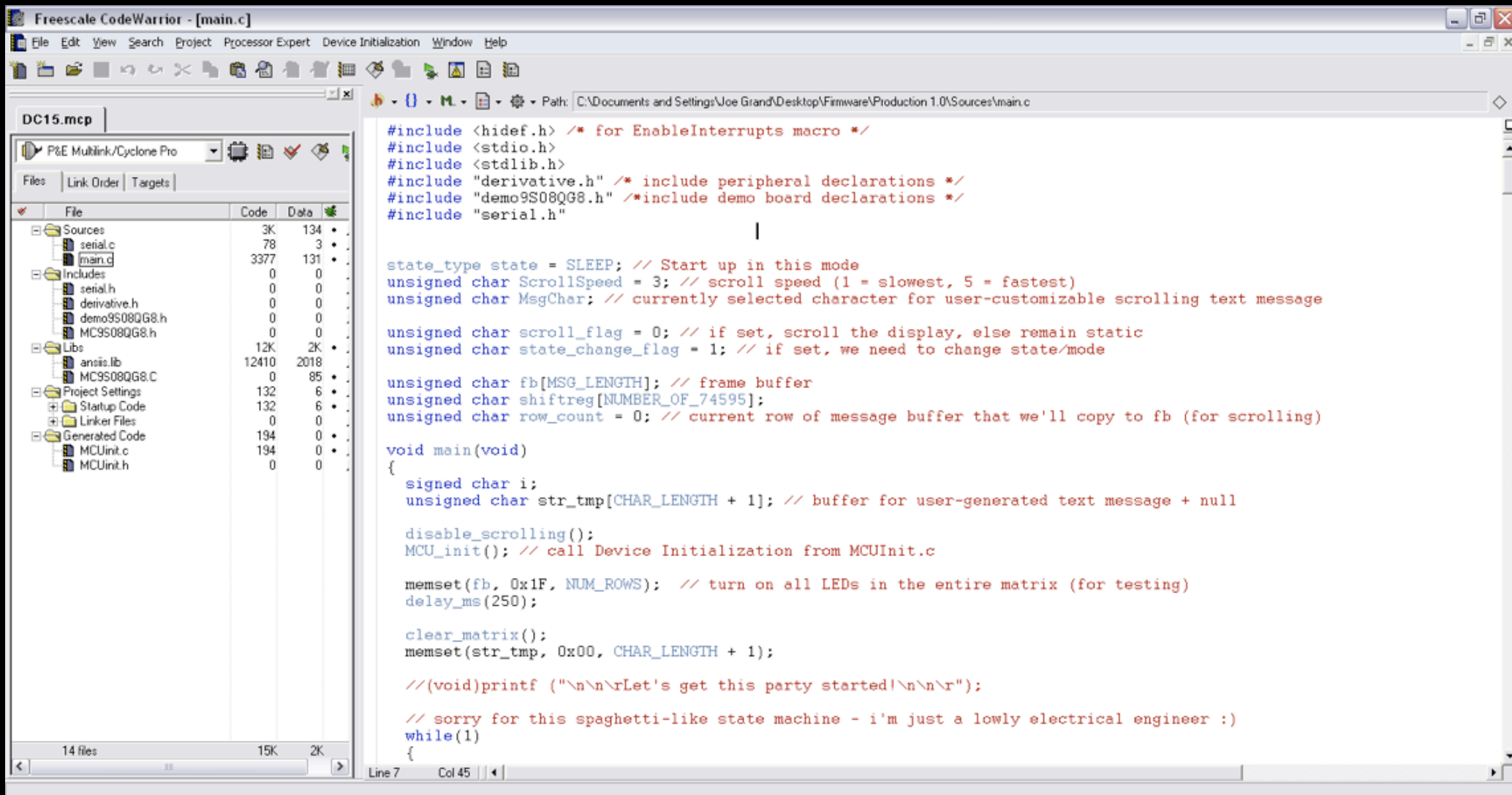
Development environment requirements...

- Must have C compiler → Freescale CodeWarrior for Q8 - FREE up to 1GB ↓
- Open-Source BDM → Angel to supply link to Schematic/Code

USB SPYDER Q8 USB dev. stick tool for Q8, QD, Q6 ⇒ \$29 Disi-key

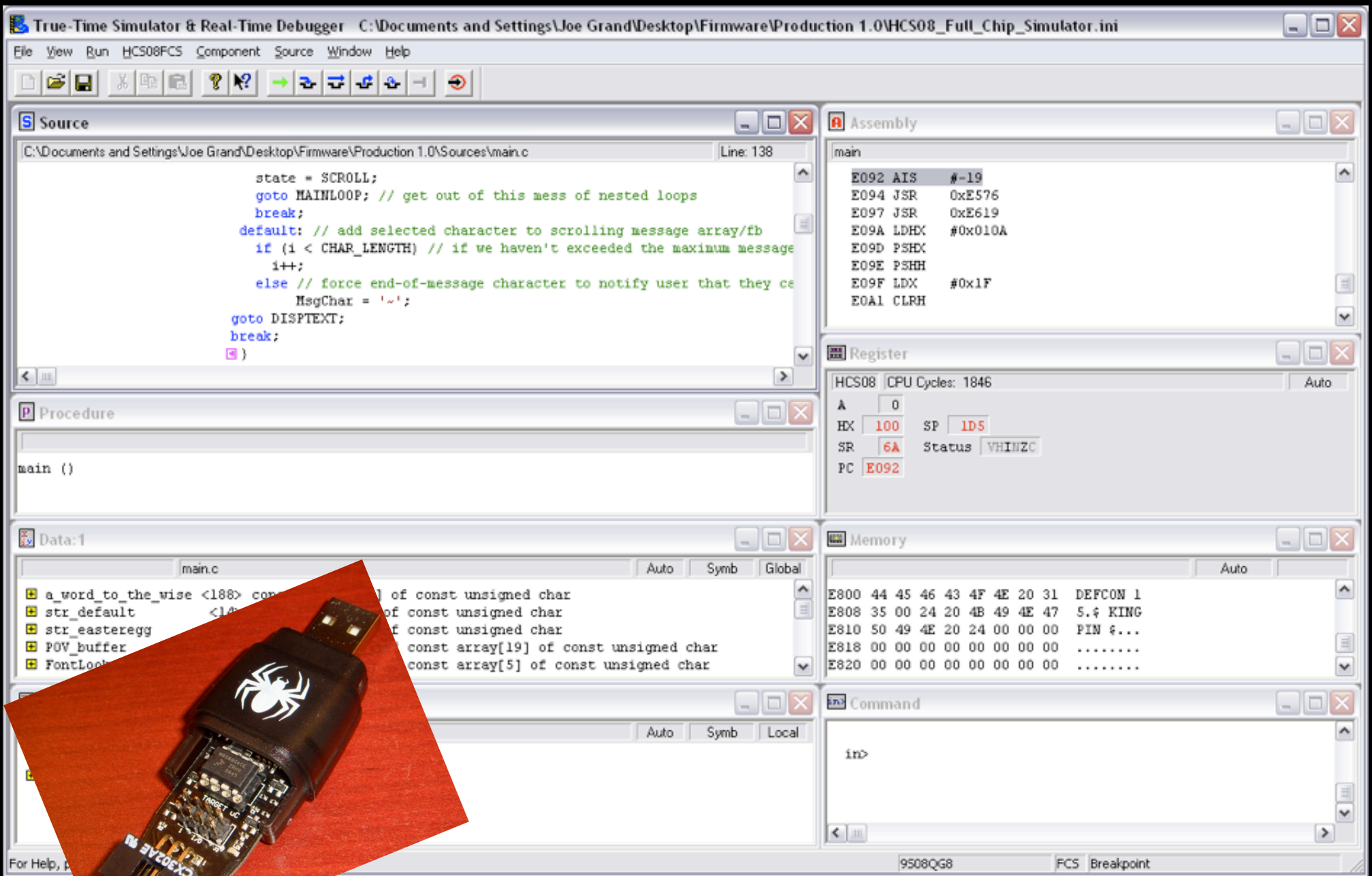
DEMO Q8 QD Q6 Hardware dev. board w/ BDM interface built-in ⇒ \$59

BDM: 6-pin header, 2x3 → leave as accessible test points on board PCB



Freescale CodeWarrior Dev. Studio for HC(S)08
www.freescale.com/codewarrior
(Free for < 16KB)

kingpin



USBSPYDER08 module or
P&E HCS08 MultiLink BDM (USB-ML-12)

kingpin

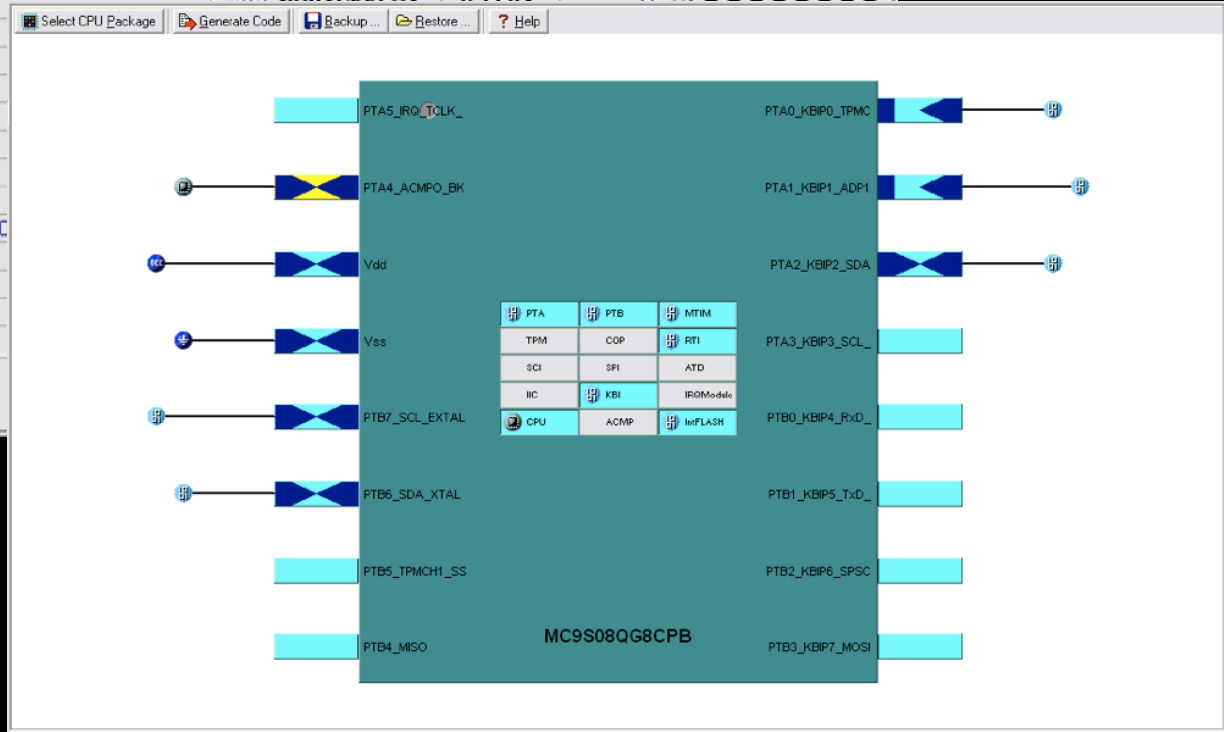
Inspector MC9S08QG8CPB

Bean Parameters

- Clock settings**
 - Source CPU clock: Internal Clock (31.25 kHz)
 - Internal clock**
 - Internal oscillator frequency [kHz]: 31.25
 - Initialize trim value: yes
 - Trim value address: FFAF
 - Fine trim value address: FFAE
 - External clock**: Disabled
 - Bus freq. divider: 1 (8.0 MHz)
 - Internal bus clock: 8.0 MHz
 - Fixed freq. clock clk src.: Divided reference clock
 - Fixed frequency clock: 0.015625 (0.015625 MHz)
 - FLL mode**: Engaged
 - FLL ref. clock source: Internal Clock
 - FLL ref. clock freq. [kHz]: 31.25
 - FLL ref. clock divider: 1
 - Divided FLL ref. clock freq. [kHz]: 31.25
 - FLL output clock freq. [MHz]: 16.0 (16.0 MHz)
 - Low-power modes settings**
 - STOP instruction enabled: yes
 - Power down control: STOP3 - Standby mode
 - Internal clock in stop mode: Disabled
 - External clock in stop mode: Disabled
 - Initialization interrupt priority: interrupts enabled (1)
- Internal peripherals**
 - ADC**: Internal bandgap buffer: Disabled
 - BDM pin support**: Enabled
 - BDM pin: PTA4_ACMPO_BKGD_MS (PTA4_AC)
 - FLASH**
 - Security state: Disabled
 - Protection: Disabled
 - Vector redirection: no

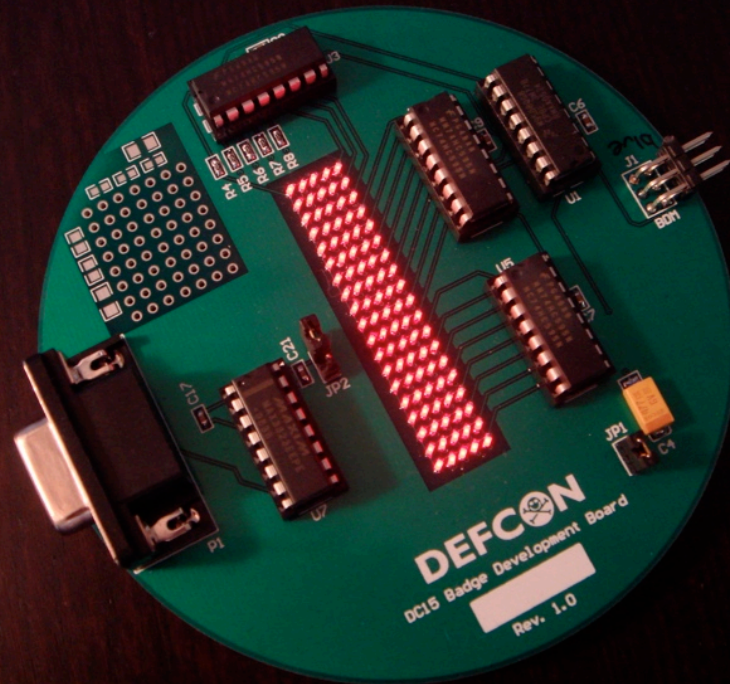
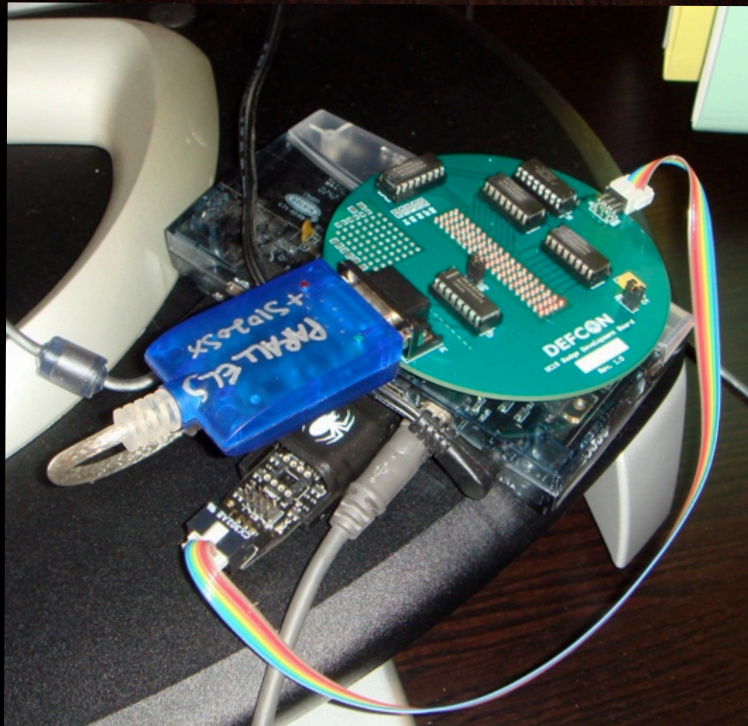
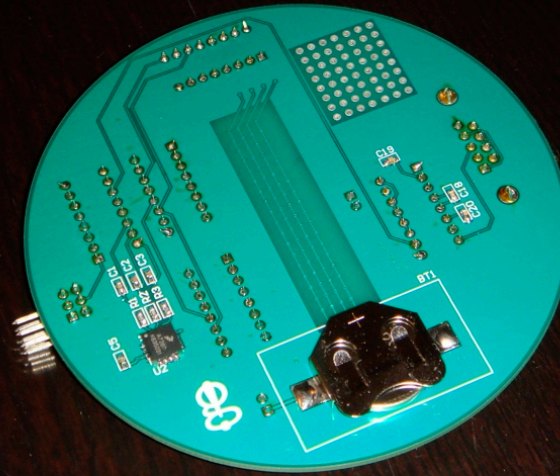
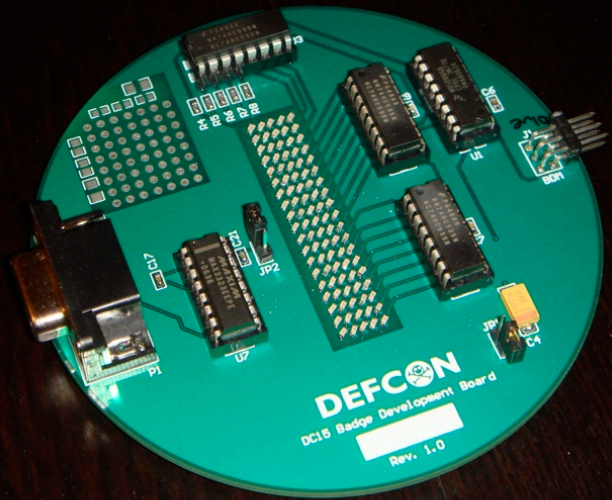
Register Details

Name	Address	Init. value	Register Map
ICSC1	0x0038	04	●●●●●●●●
ICSC2	0x0039	00	●●●●●●●●
ICSTRM	0x003A	80	●●●●●●●●
ICSSC	0x003B	00	●●●●●●●●
SRS	0x1800	?????070	●●●●●●●●
SOPT1	0x1802	72	●●●●●●●●
SDIDH	0x1806	00	●●●●●●●●
SDIDL	0x1807	09	●●●●●●●●
SPMSC1	0x1809	18	●●●●●●●●
SPMSC2	0x180A	00	●●●●●●●●
SPMSC3	0x180C	00	●●●●●●●●
PTASE	0x1841	3F	●●●●●●●●
PTADS	0x1842	00	●●●●●●●●
PTBSE	0x1845	FF	●●●●●●●●
PTBDS	0x1846	00	●●●●●●●●
NVBACKKEY0	0xFFB0	FF	●●●●●●●●
NVBACKKEY1	0xFFB1	FF	●●●●●●●●
NVBACKKEY2	0xFFB2	FF	●●●●●●●●
NVBACKKEY3	0xFFB3	FF	●●●●●●●●



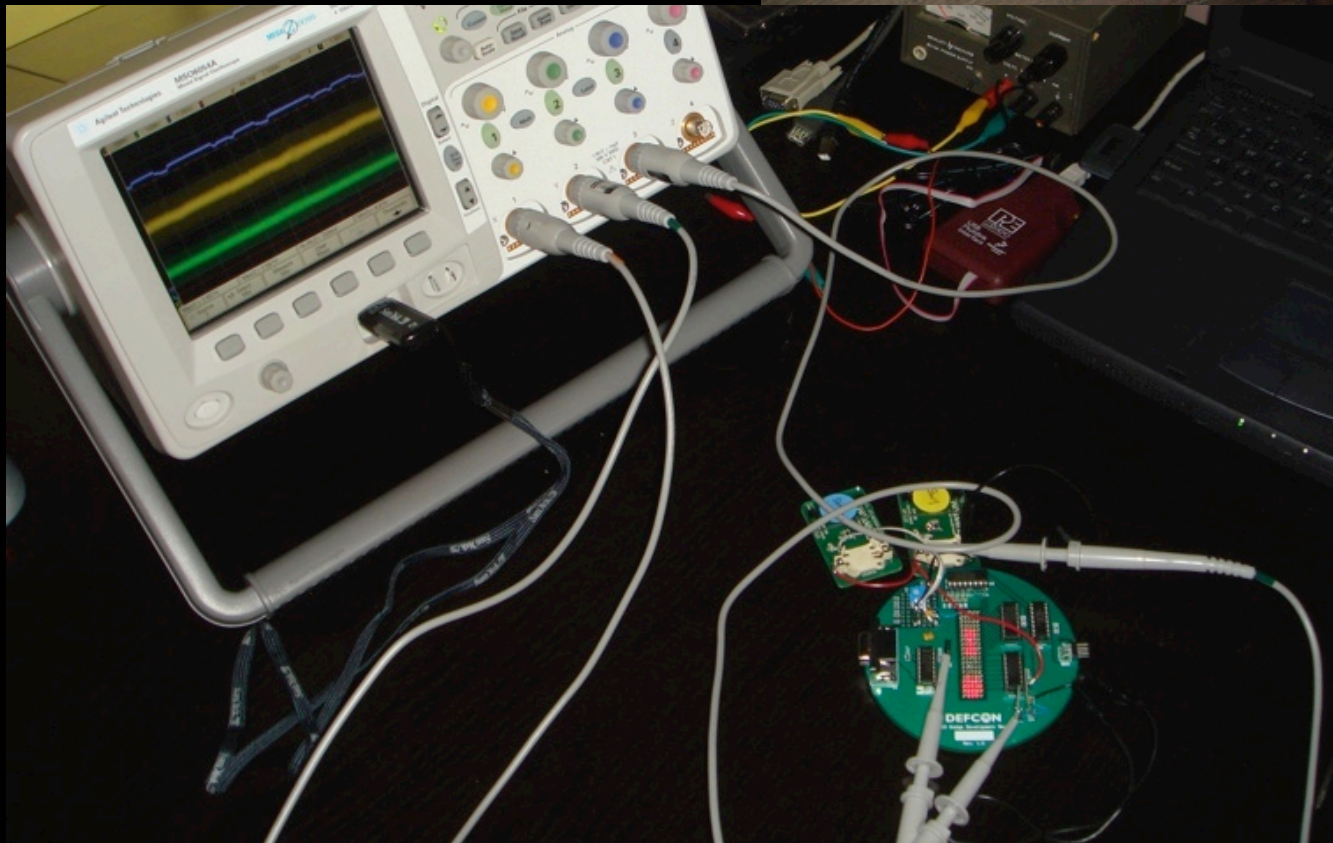
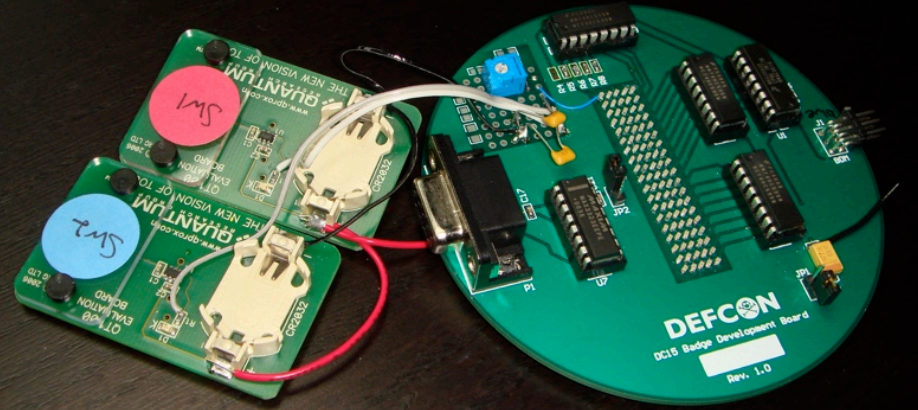
kingpin

Development H/W up and running!




kingpin

Adding capacitive touch...



kingpin

Napkins?

POV: - Disable Scrolling
 - every x ms, load  with new values
 increment POV-cut
 every MTM
 (ensure period is set
 to default no
 interrupt
 scroll speed is set to)

100,000 miles for your thoughts.
 Your feedback is important to us. Visit usa.survey.com within three days of your flight. You could win 100,000 Mileage Plus® miles.

UNITED
 It's time to fly.
See complete rules at usa.survey.com
 ©2007 United Air Lines, Inc. All Rights Reserved.

- if SWI hit, change made
 Cool hack: have POV
 display text string instead
 of fixed image

- Disable Scrolling = Scroll bit
 enable/disable movement
 instead of of pointer
 → static or scroll use
 disabling interrupt

UNITED
 display current settings

if SWI pressed, increment & load new FO
 if SWI pressed, decrement & load new FO

set MTM w/ 1 of 8 values
 ← if both, same value & exit

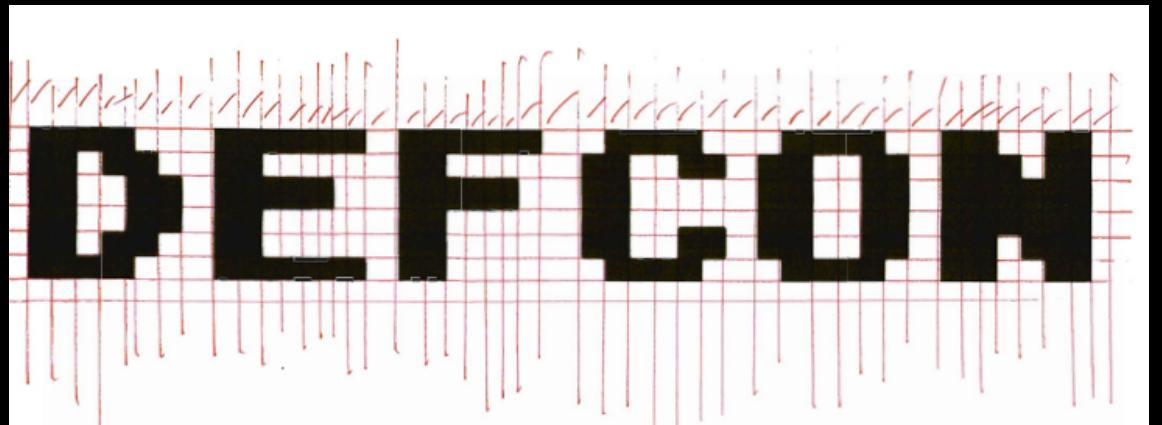
set message: if SWI pressed, increment/decrement
 if both, ~~scroll speed~~ do end.
 need end manually load change into FO
 & ← character w/ loc str? manually increment FO points?

Thank you for flying United.

Pseudok0dez...

kingpin

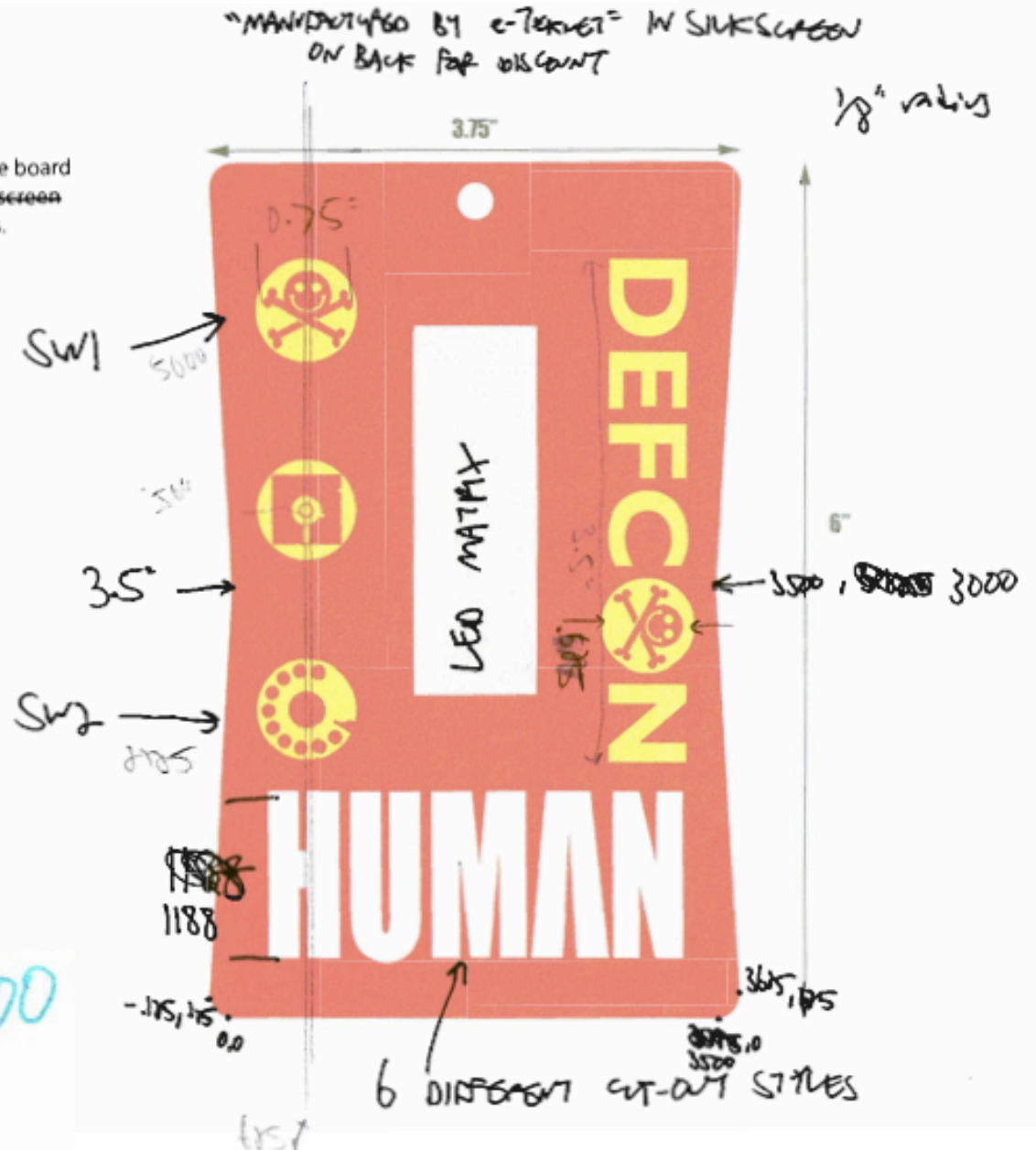
IN DEFCON DEF



kingpin



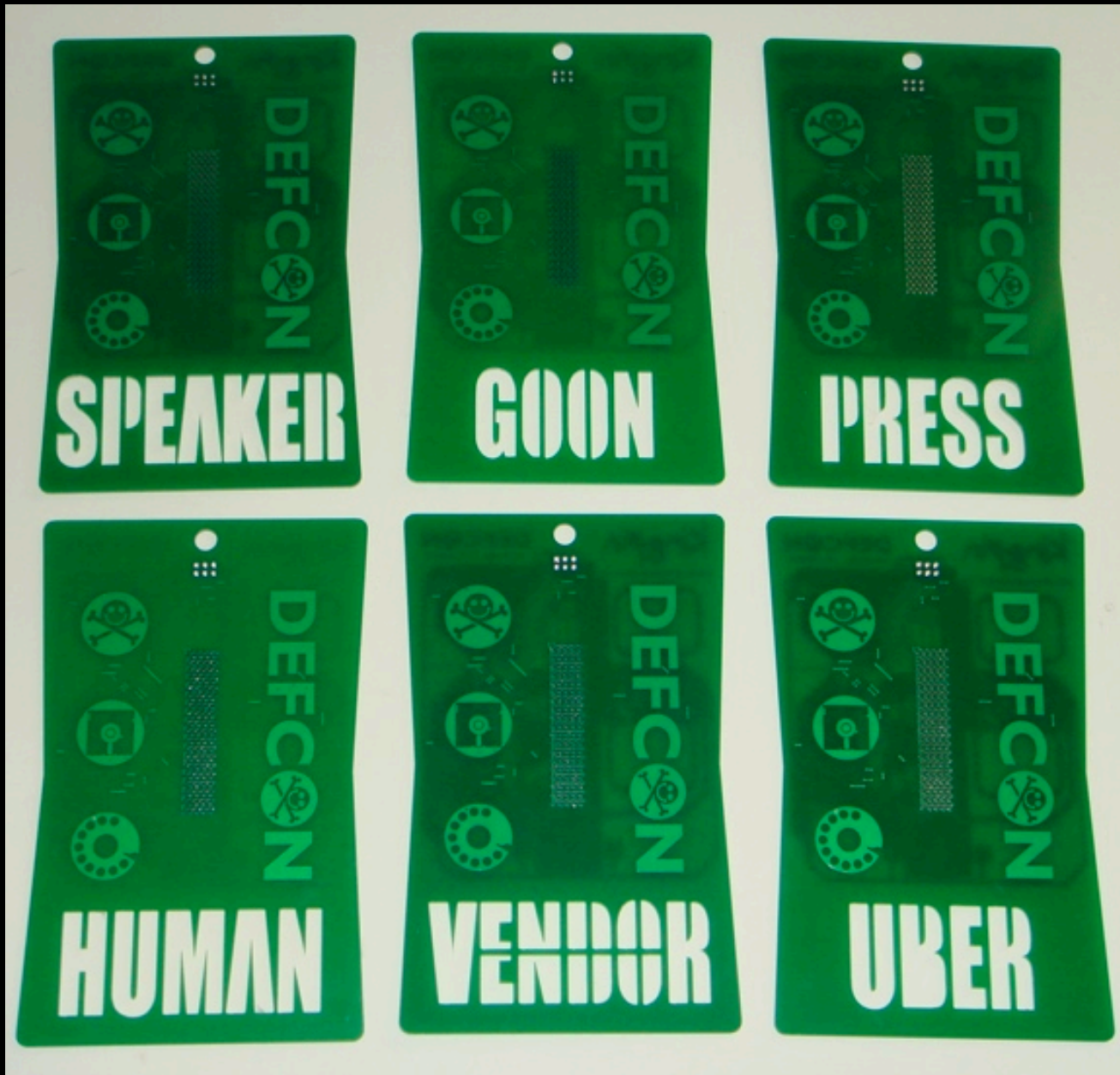
Orange: Shape of the board
 Yellow: Tracer or silkscreen
 White: Cut-out areas.



- ✓ human - white badge - 7200 → 6000
- ✓ goon - red badge - 200
- ✓ press - green - 125
- ✓ vendor - purple - 150
- ✓ speaker - blue - 225
- ✓ uber - black - 100

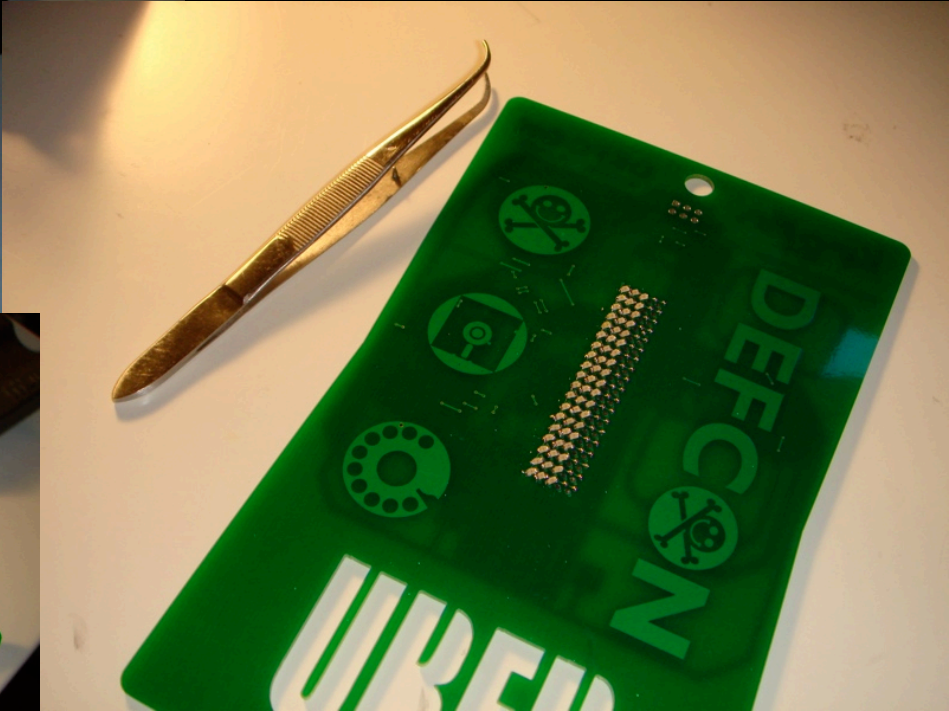
Kingpin

The first set of prototypes arrive...



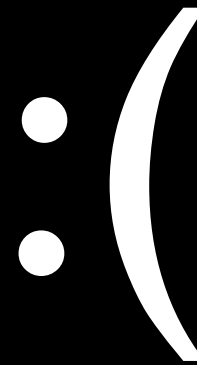
Kingpin

Hand-assembled
with love!



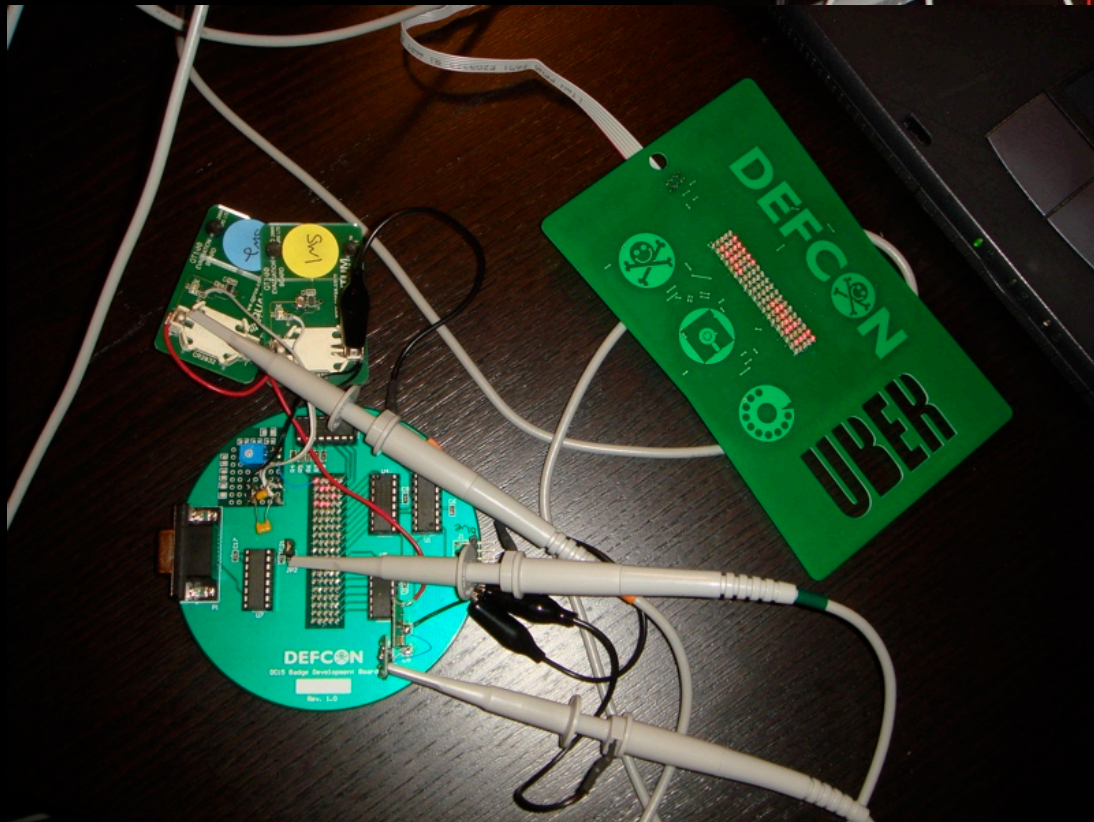
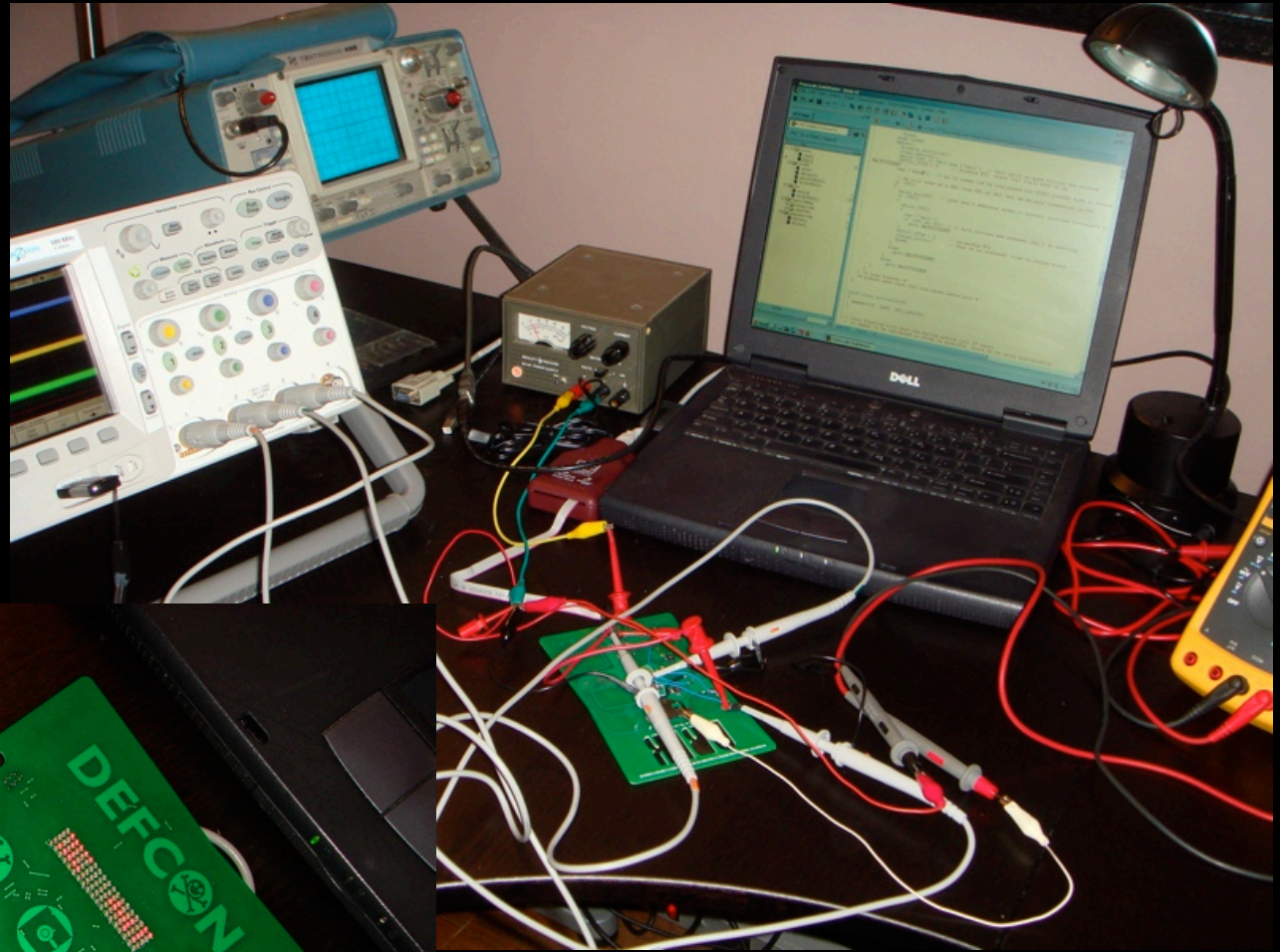
kingpin

But, there was a problem...



kingpin

Capacitive sensors unreliable when running on battery...

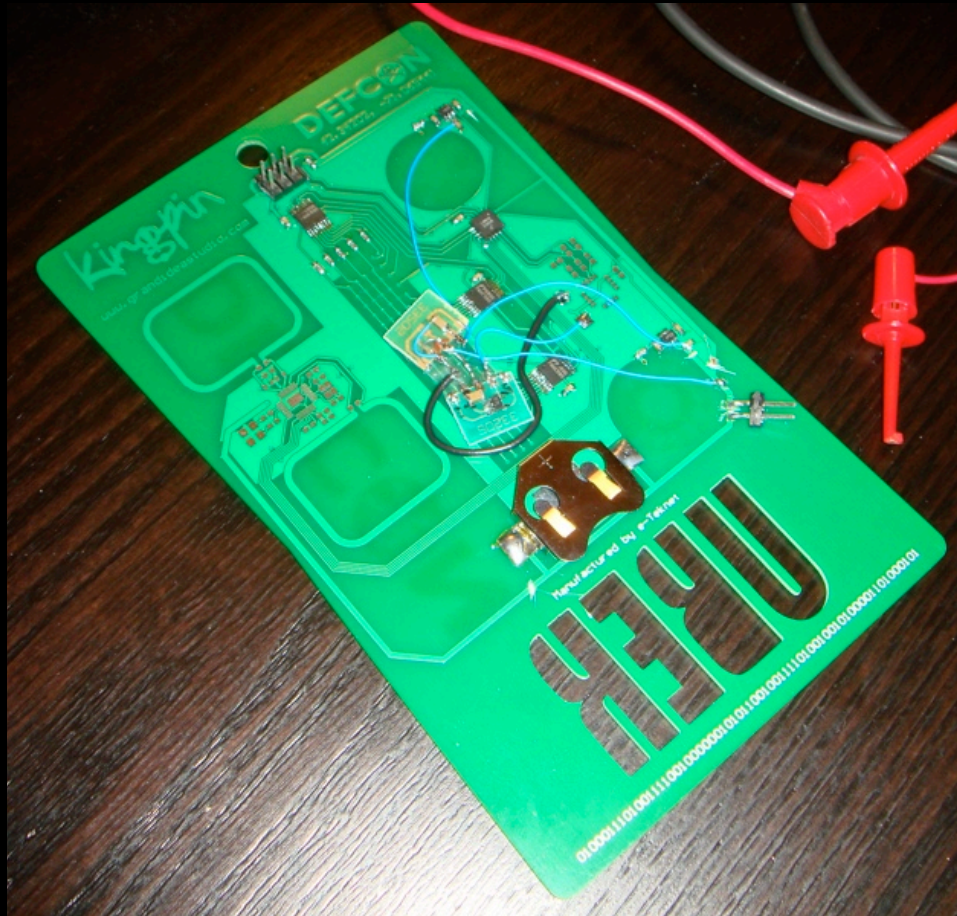


WTF!?

kingpin

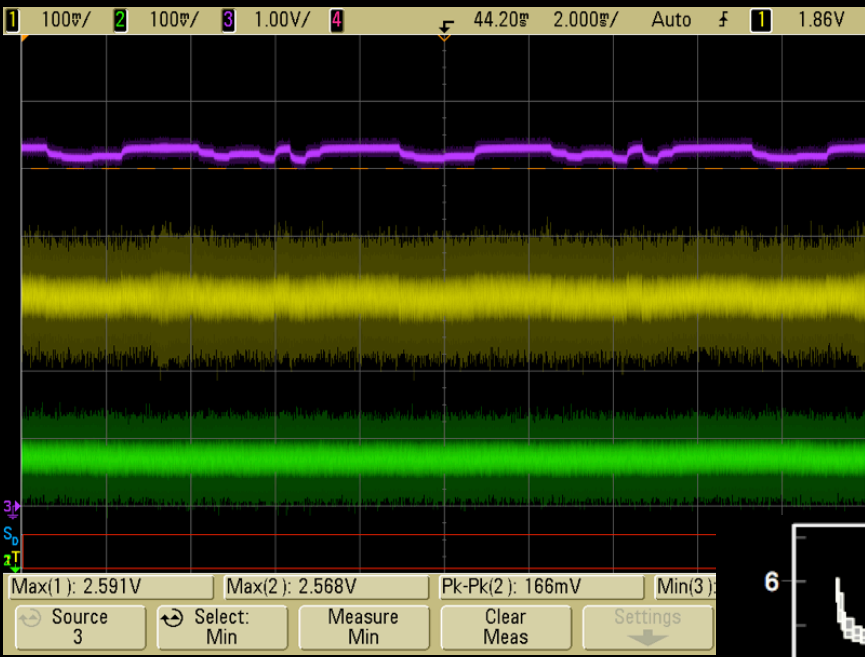
The fix...

- Additional 3V coin cell to bring VBATT to 6V
- Two 2.5V LDO regulators to create isolated supply lines for capacitive sensors and rest of circuitry

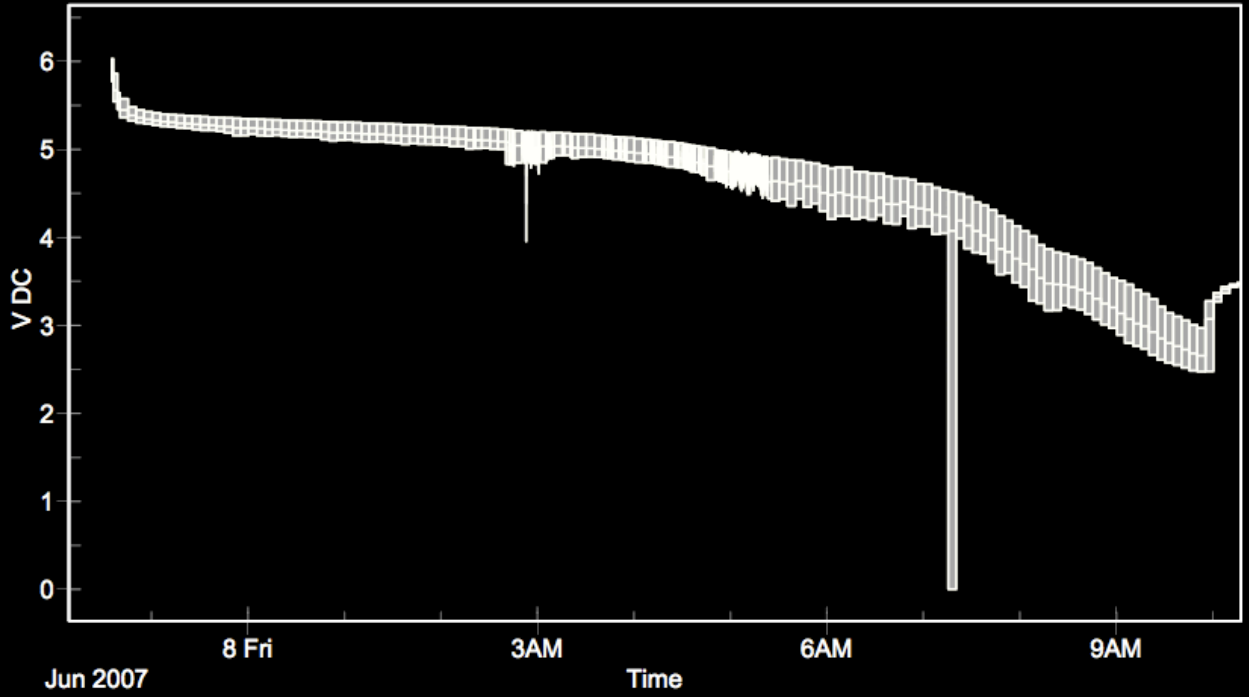
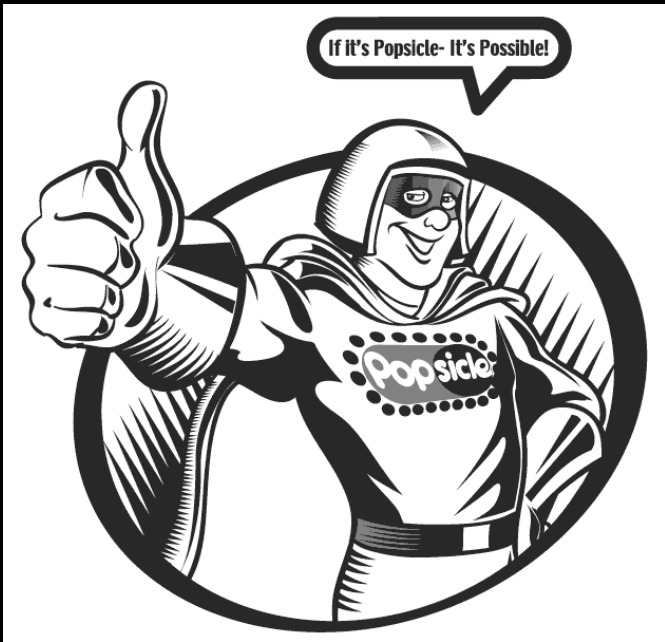


Moral: RTFM!

kingpin



Noisy input
 ↓
 Smoooooth outputs!

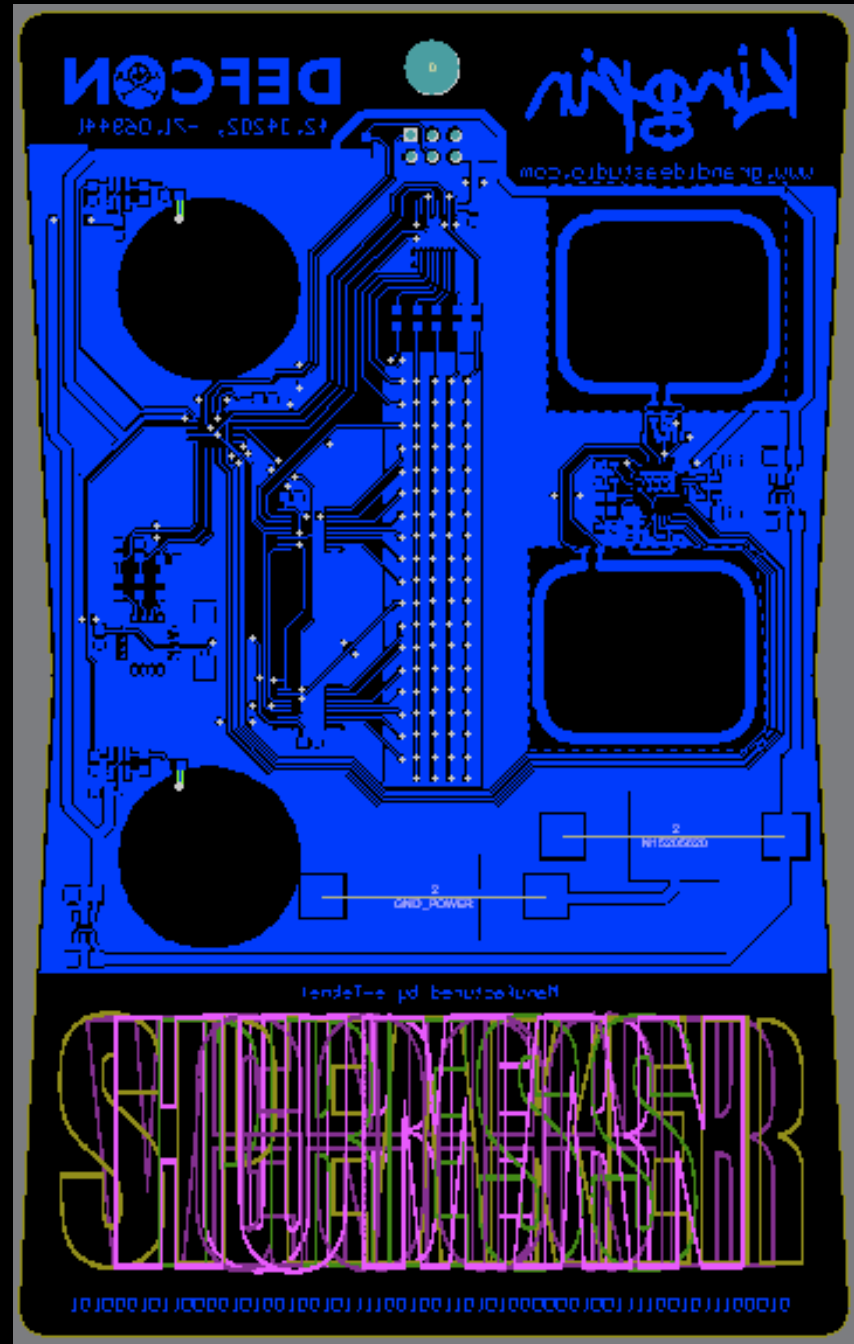
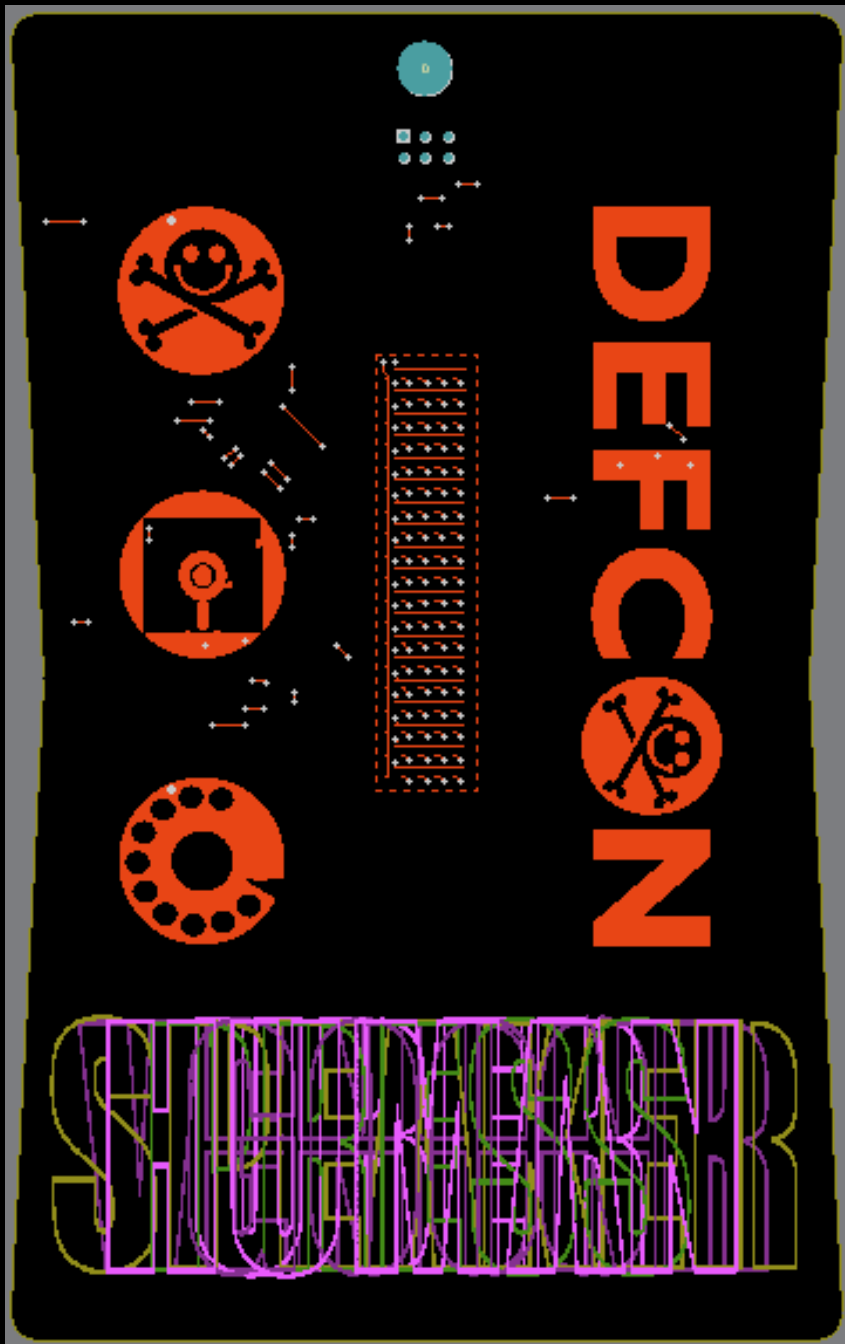


Comments

Initial battery voltage, no load, 2x CR2032 cells = 6.3V
 Elapsed time to 3.07V avg. (2.48V low) = 11.5 hours

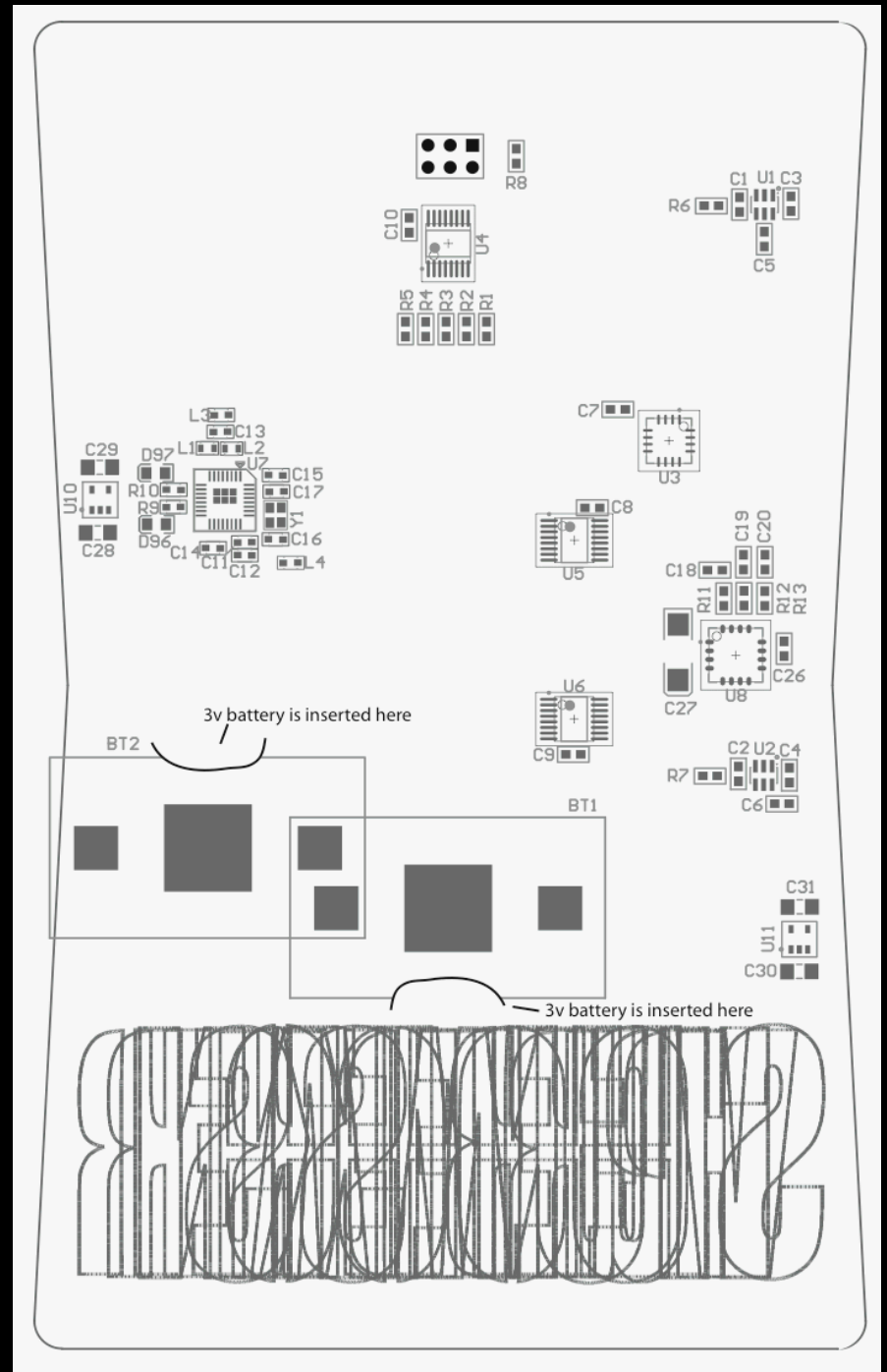
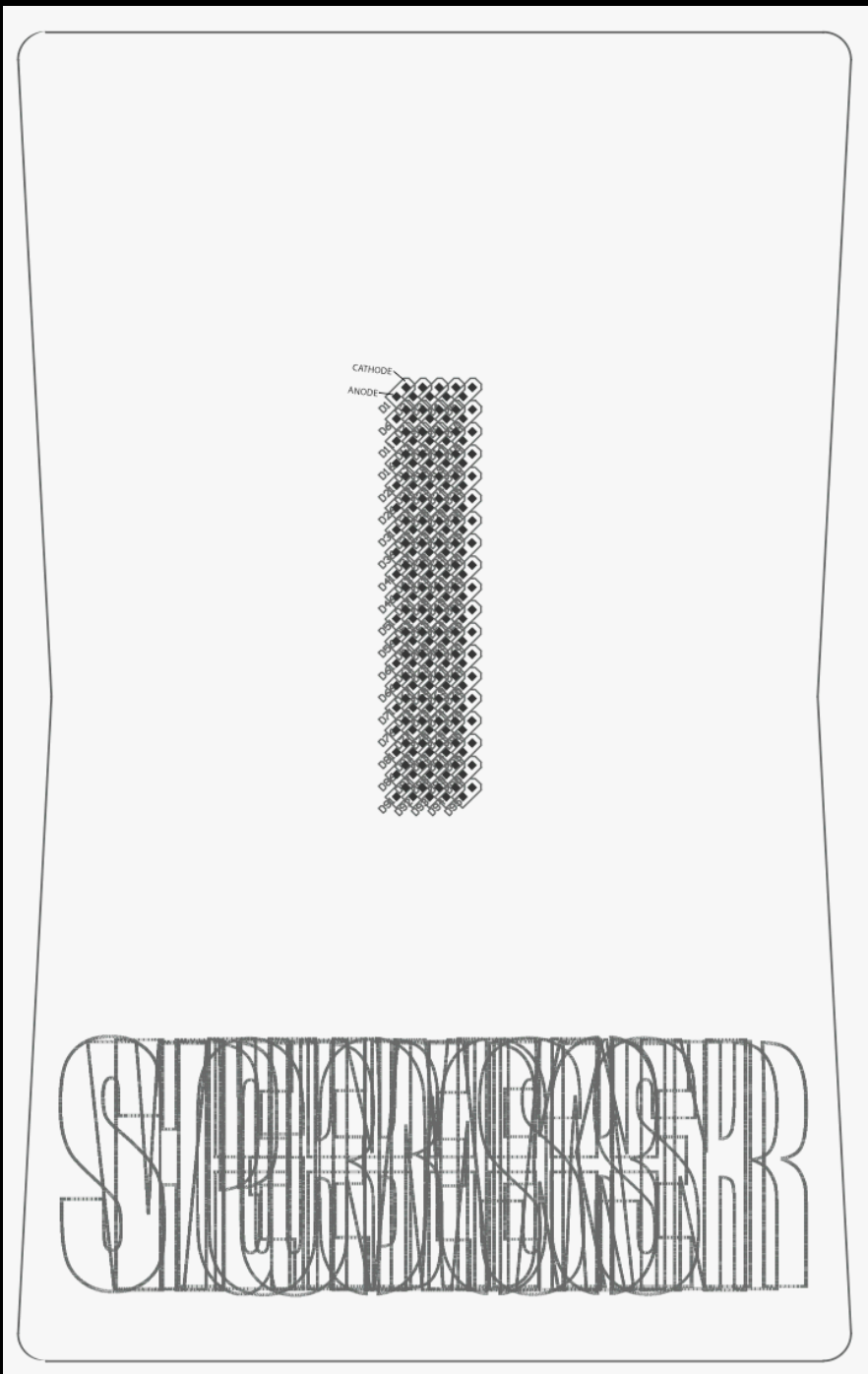
Lithium cells do not like constant high discharge current - will get longer battery life if cell allowed to recover
CONCLUSION: For maximum battery life, go to SLEEP mode when badge not in use!

kingpin



Final PCB layout...

kingpin



Assembly drawings...

kingpin

Finalized Schematic and BOM...

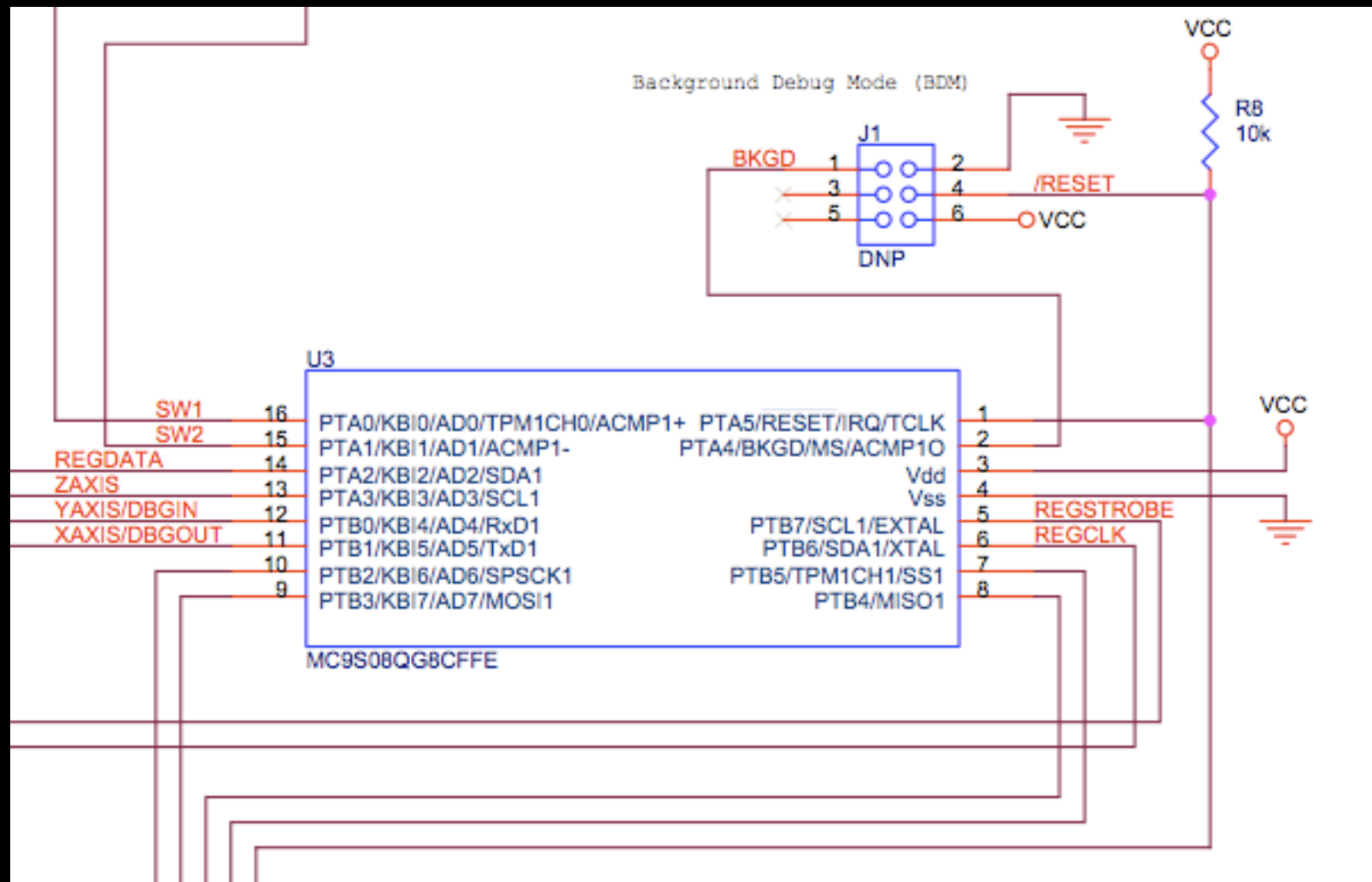
DEFCON 15 Circuit Board Badge Bill-of-Materials

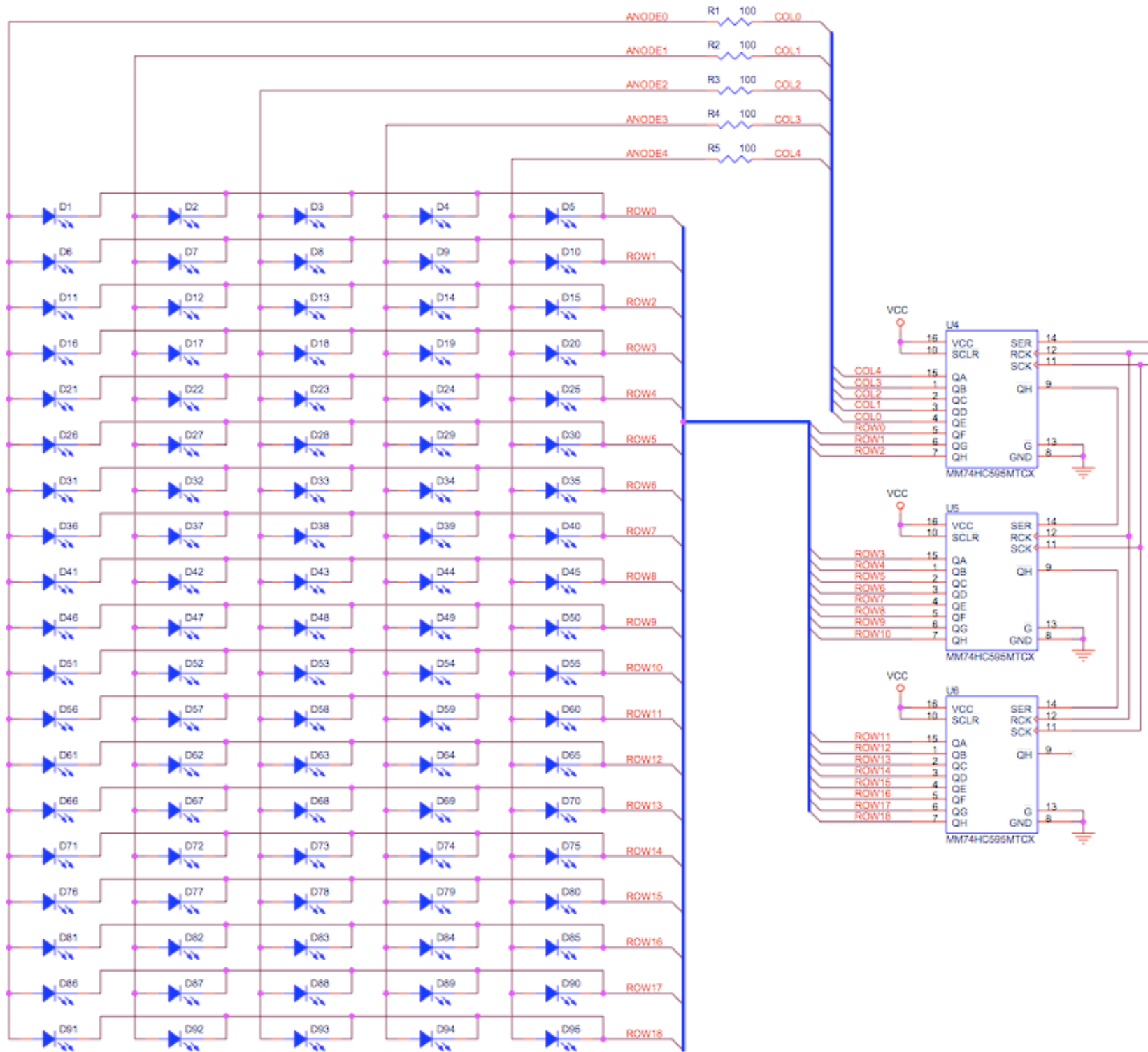
Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	2	BT1,BT2	Keystone	3002	FAI	3002	Battery holder, 20mm coin cell, SMD
1a	2	N/A	Renata Batteries	CR2032	FAI	CR2032	CR2032 Lithium 3V Coin Cell Battery (225mAh)
2	2	C1,C2	TDK	C1608X7R1H471K	Digi-Key	445-1307-2-ND	470pF ceramic capacitor, 10%, X7R (PPS OK), 50V, 0603
3	8	C3,C4,C5,C6,C7,C8,C9,C10	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603
4	4	C28,C29,C30,C31	Murata	GRM31MR71H105KA88L	FAI	GRM31MR71H105KA88L	1uF ceramic capacitor, 50V, X7R, 1206
5	95	D1-D95	Avago	HSMH-C192	FAI	HSMH-C192	Red LED, 0603, 1.8Vf, 17mcd @ 20mA
6	5	R1,R2,R3,R4,R5	Rohm	MCR03EZJ101	FAI	MCR03EZJ101	100 ohm, 5%, 1/10W, 0603
7	3	R6,R7,R8	Dale	CRCW060310K0JNEA	FAI	CRCW060310K0JNEA	10k, 5%, 1/10W, 0603
8	2	U1,U2	Quantum Research	QT100-ISG	Saelig	QT100-ISG	Charge-Transfer QTouch Sensor, SOT23-6
9	1	U3	Freescale	MC9S08QG8CFFE	Arrow	MC9S08QG8CFFE	Microcontroller, QFN16
9a	1	N/A	N/A	N/A	Arrow	N/A	Microcontroller programming service
10	3	U4,U5,U6	Fairchild	MM74HC595MTCX	FAI	MM74HC595MTCX	Logic, 8-bit Shift Register, TSSOP16
11	2	U10,U11	Sipex	SP6201EM5-L-2-5	FAI	SP6201EM5-L-2-5	Linear Regulator LDO, 2.5V fixed output, SOT23-5
12	1	PCB	e-Teknet	DC15 1.0	N/A	N/A	PCB (includes assembly and testing)



kingpin

Microprocessor...

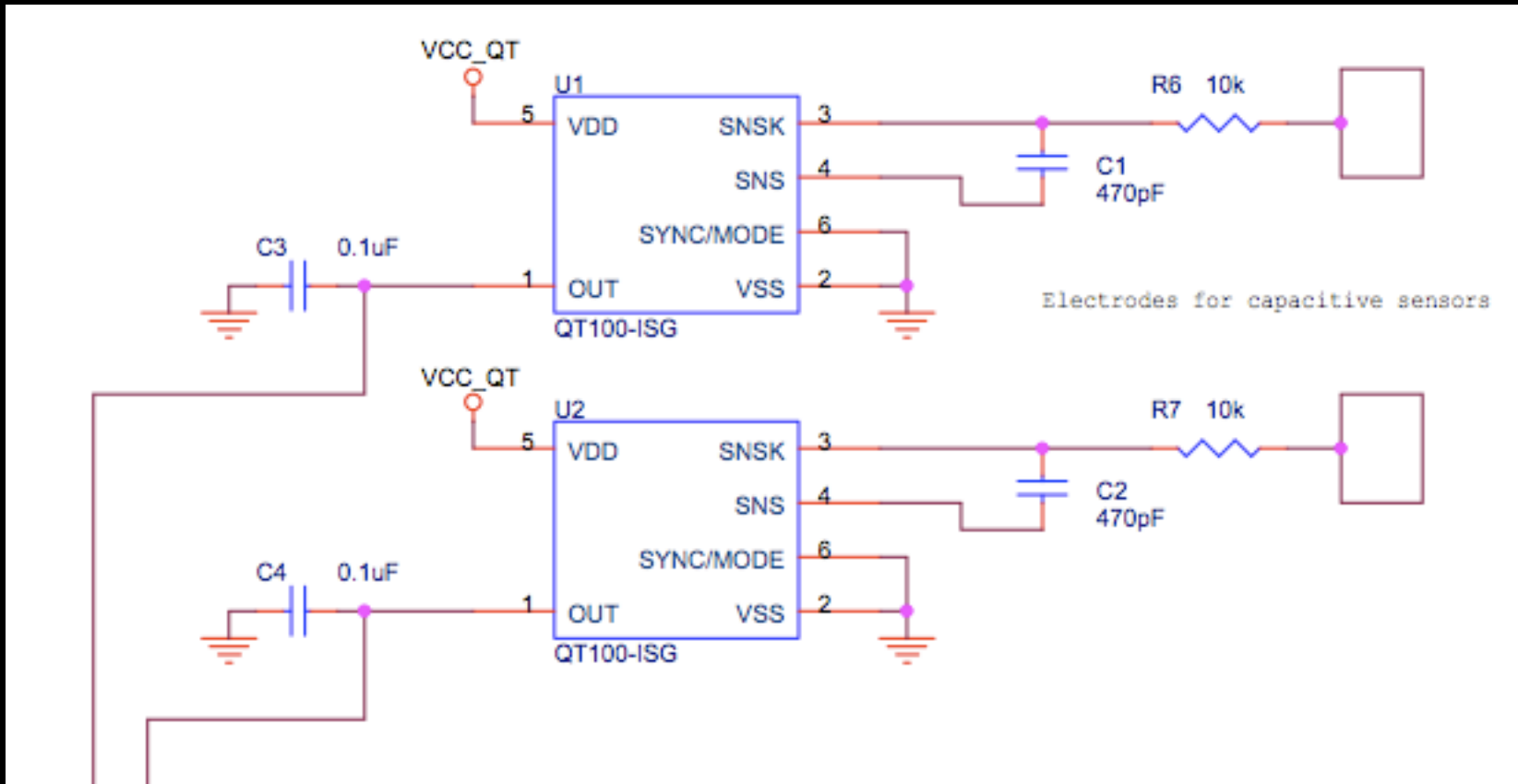


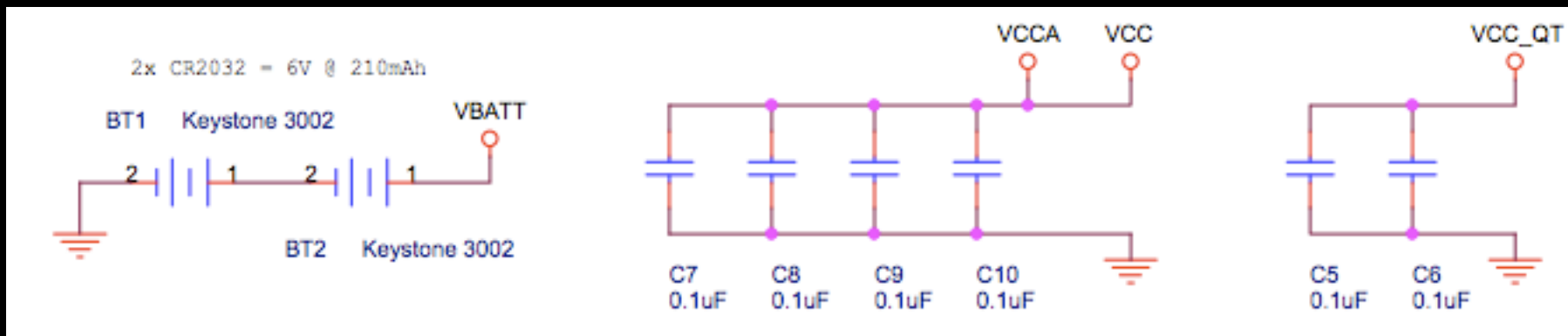
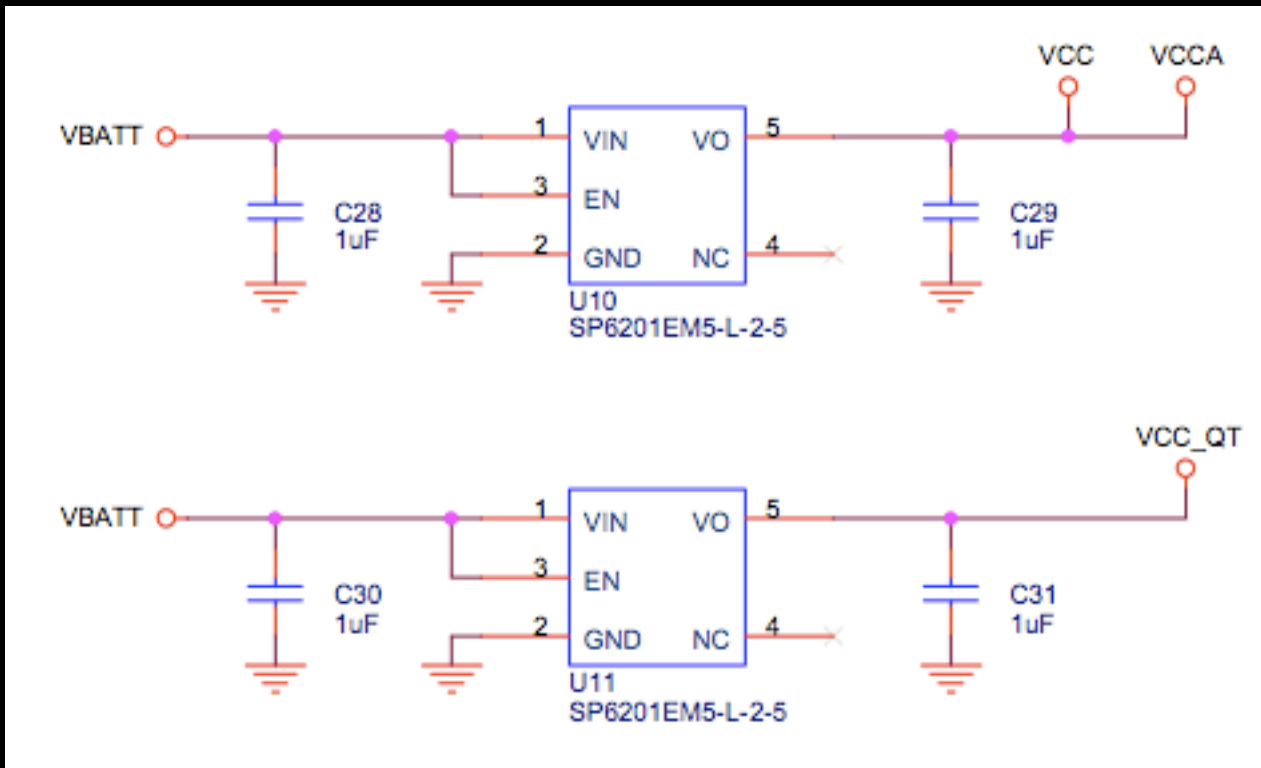


LED Matrix...

kingpin

Capacitive touch sensors...

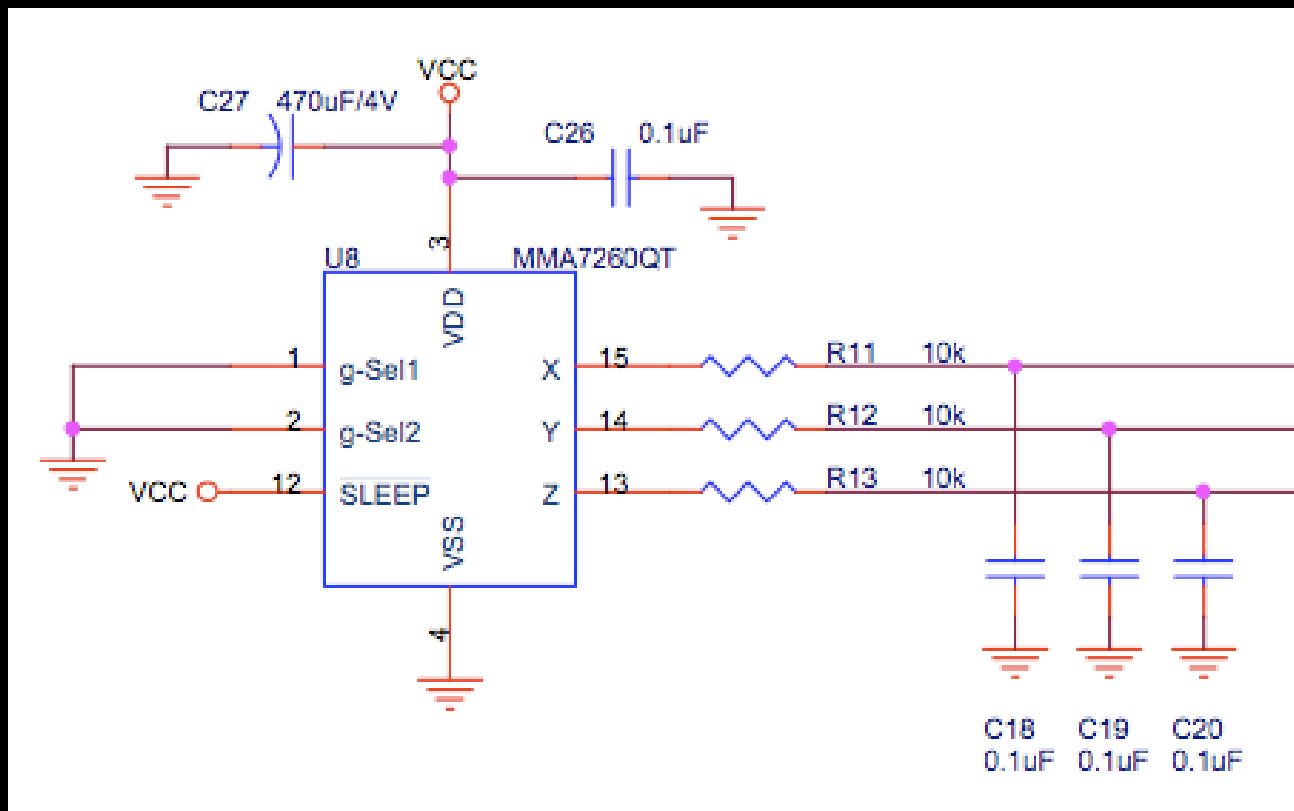




Power supply & conditioning...

kingpin

3-axis accelerometer...



3-Axis Accelerometer Components

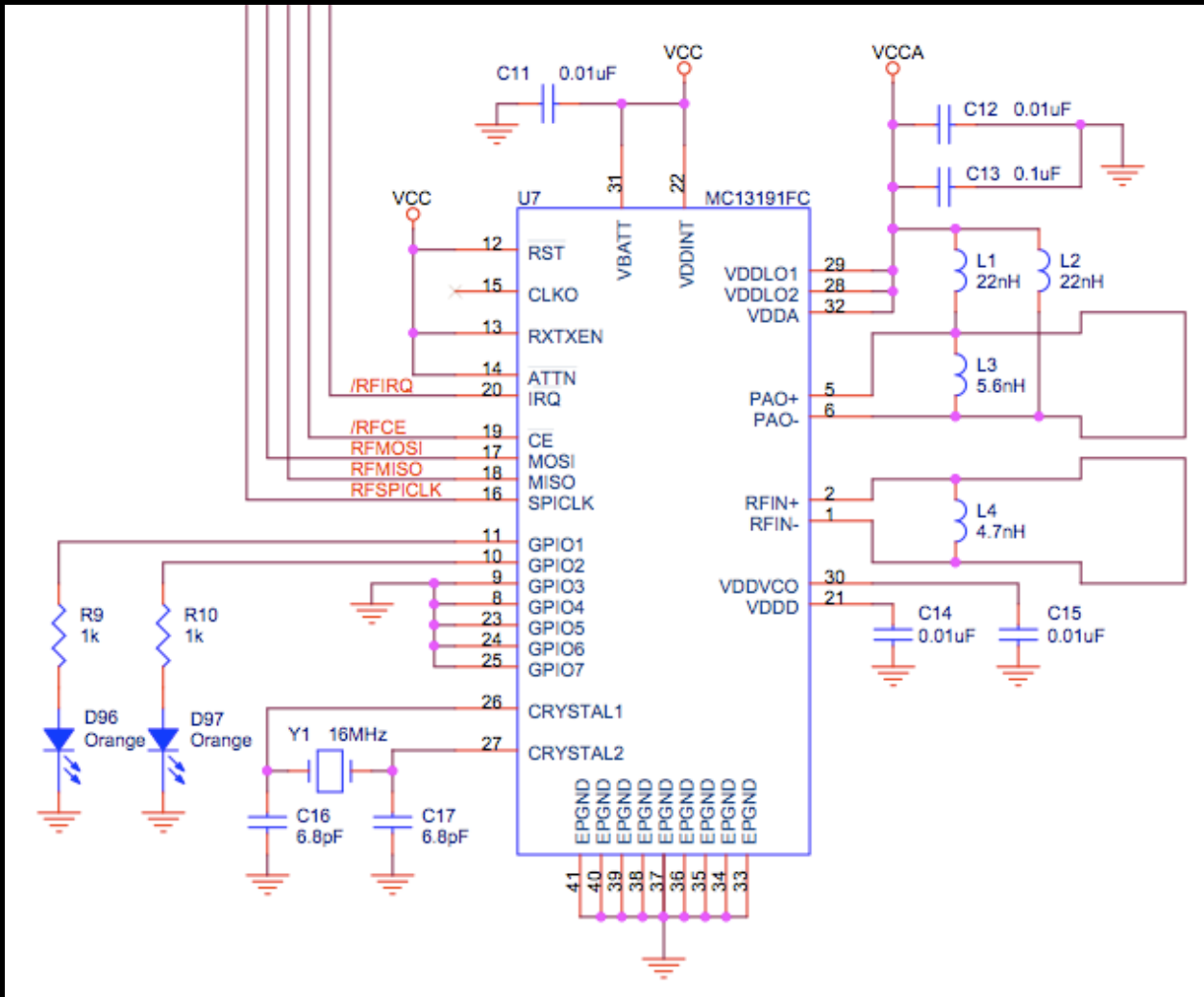
Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	4	C18,C19,C20,C26	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603
2	1	C27	Sprague	594D477X9004C2T	FAI	594D477X9004C2T	470uF, 4V, tantalum, size D
3	3	R11,R12,R13	NIC	NRC06J103TRF	FAI	CRCW0603-103JRT1	10k, 5%, 1/10W, 0603
4	1	U8	Freescale	MMA7260QT	FAI	MMA7260QT	Accelerometer, 3-axis, adjustable g (1.5/2/4/6), QFN16

(unpopulated)

kingpin

802.15.4 Wireless Components

Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	4	C11,C12,C14,C15	AVX	0603YC103JAT2A	FAI	0603YC103JAT2A	0.01uF, 16V, X7R, 0603
2	1	C13	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603
3	2	C16,C17	Murata	GRM1885C1H6R8DZ01D	NewarkInOne	38K1691	6.8pF, 50V, 0603
4	2	D96,D97	Kingbright	KP-1608SEC	NewarkInOne	38K3373	Orange LED, 0603, 2.0Vf, 200mcd @ 30mA
5	2	R9,R10	Any	Any	FAI	CRCW0603-102JRT1	1.0k, 5%, 1/10W, 0603
6	2	L1,L2	Murata	LQW18AN22NG00D	Mouser	81-LQW18AN22NG00D	Inductor, 22nH, 500mA, 0.17 ohm 0603
7	1	L3	Murata	LQW18AN5N6D00D	Mouser	81-LQW18AN5N6D00D	Inductor, 5.6nH, 750mA, 0.082 ohm 0603
8	1	L4	Murata	LQW18AN4N7D00D	Mouser	81-LQW18AN4N7D00D	Inductor, 4.7nH, 850mA, 0.059 ohm 0603
9	1	U7	Freescale	MC13191FC	Digikey	MC13191FC-ND	RF Transceiver, 802.15.4/ZigBee, 2.4GHz, QFN32
10	1	Y1	NDK	NX2520SA-16MHz	Digikey	644-1059-1-ND	16MHz Crystal Oscillator, 10pF, SMD



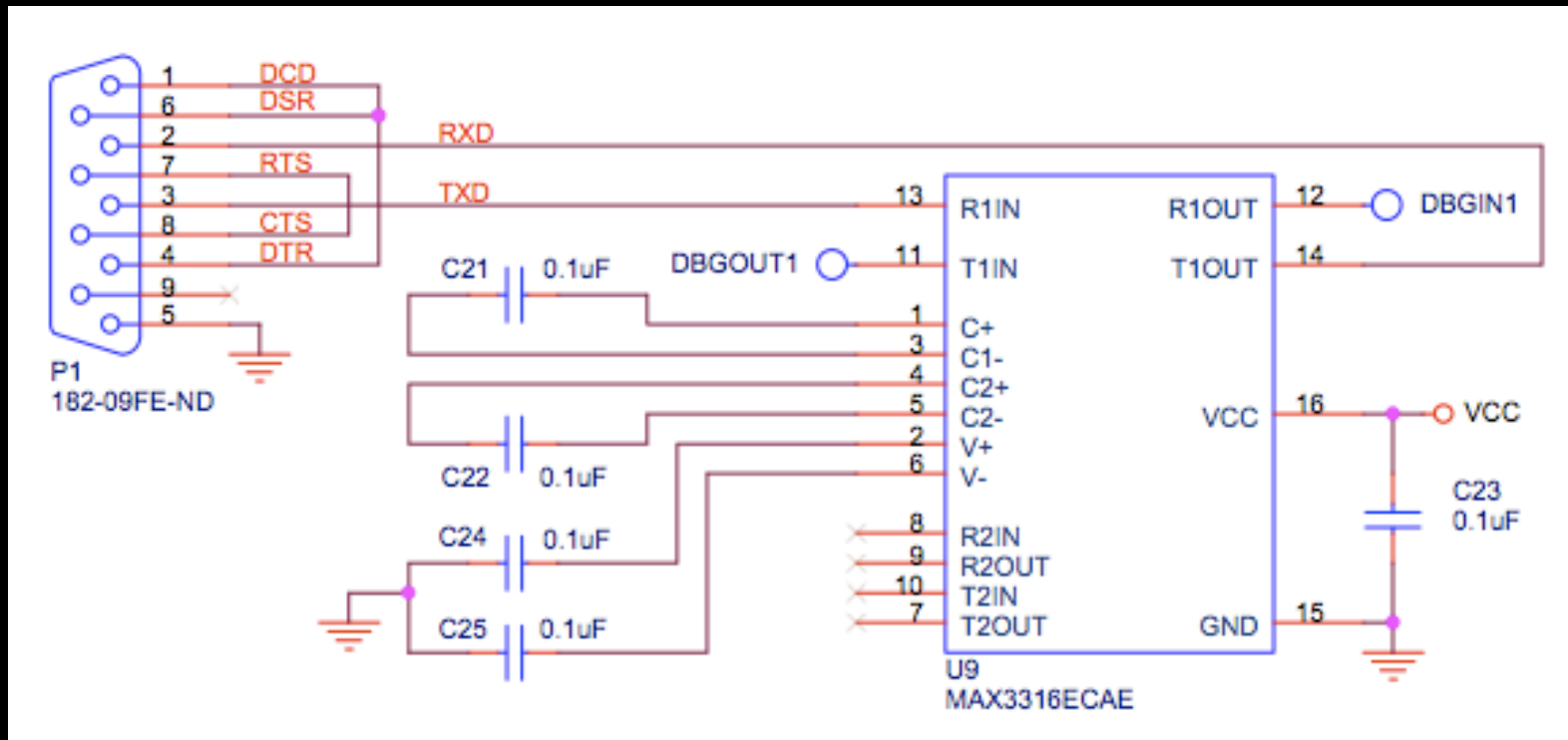
(unpopulated)

*Beckit: Check release for SMT, 802.15.4 & ZigBee
by -board, Free
www.freescale.com/ZigBee*

2.4GHz wireless transceiver
(802.15.4/SMAC/ZigBee)

Kingpin

Serial port/level shifter interface...



PC Serial Port Interface (No Footprints on PCB)

Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	5	C21,C22,C23,C24,C25	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603
2	1	P1	Norcomp	182-009-213R531	Digikey	182-09FE-ND	Connector, DB9 Female, R/A, PCB Mount
3	1	U9	Maxim	MAX3316ECAE	N/A	N/A	RS232 Transceiver, 2.5V, SSOP16

(Not designed onto PCB)

COMPONENTS TO eTEKNET

6/15/07 →

Lots and lots of parts to deal with...

JUNE 15/2007

Box 1:	200K	HSMH-C192
Box 2:	200K	HSMH-C192
Box 3:	120K	HSMH-C192
Box 4:	11,599	HSMH-C192
	16K	VJ0603Y822JXX
	60K	0603YC104JAT2
	35K	MUR03E2HJ10
	25K	CRCW060310K0JME
	15K	QT100-156 U1-
Box 5:	120K	HSMH-C192
	8K	3002 BT1
	20,470	MM74HCS95MTGX

D1-D95

SENT BACK 6/30/07



JUNE 16/2007

Box 6:	5,600	3002 BT1-B72
	27,710	GRM31MR71H10SKA88L C28-C31
	5,000	SP6701EMS-L-2-5/TR U10-U11

JULY 5/2007

Box 7:	15,990	C1608X7R1H471K C1-C2
	2,500	SP6701EMS-L-2-5/TR U10-U11
	1	MC9508018CRFC U3

Programmed micros almost didn't arrive in time!

kingpin

Badge Assembly!



Applying solder paste...



Placing LEDs...

kingpin

Pick-and-place... (back side)





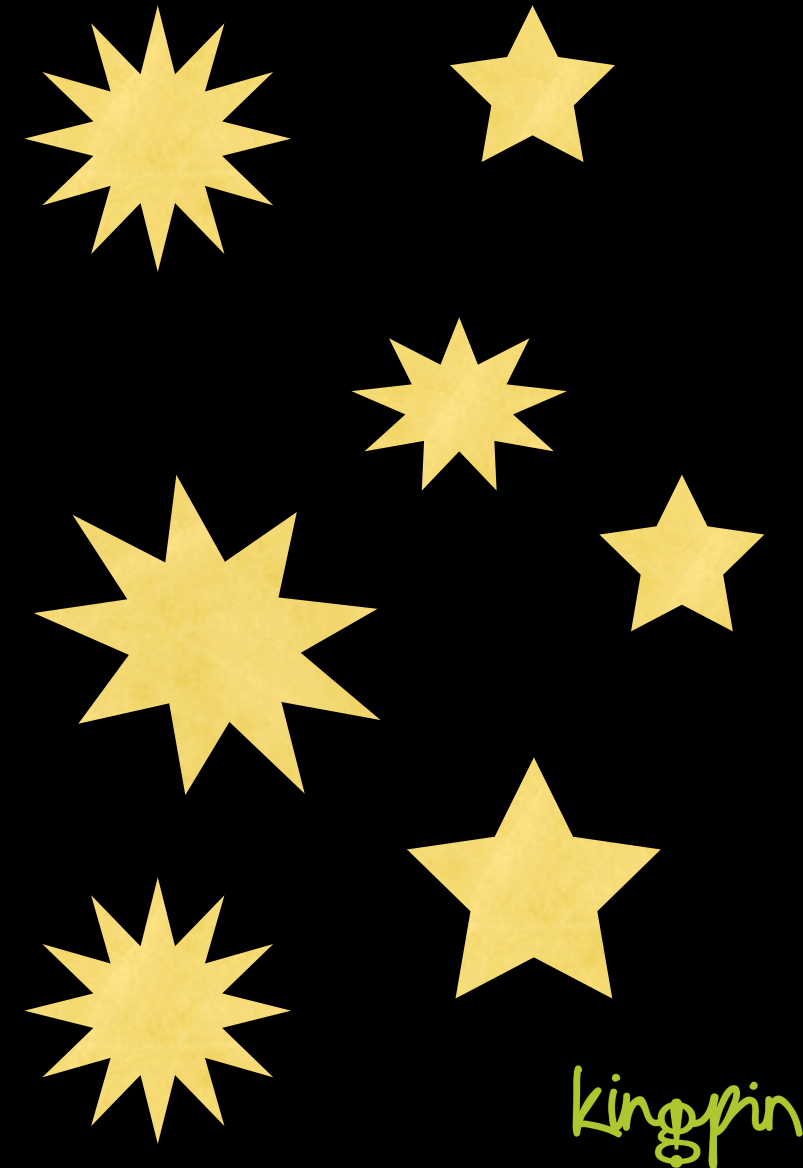
Reflow...

Final inspection...



kingpin

e-Teknet pulled it off in just a few weeks!
(Final batch of boards arrived this Wednesday)
(Yes, 2 days ago...)

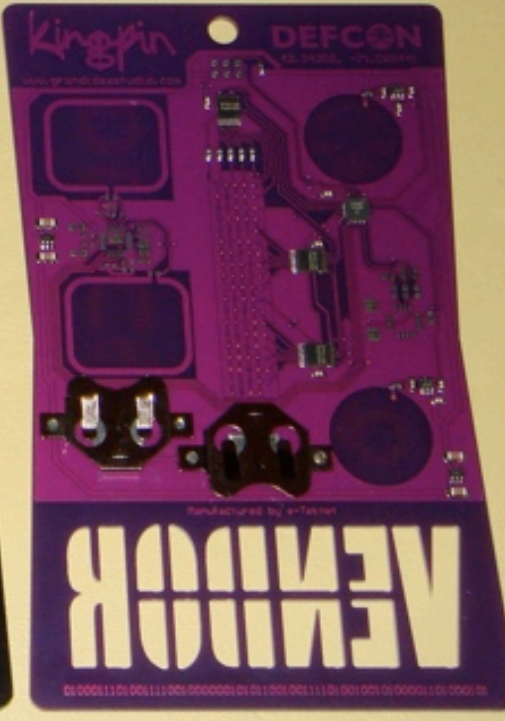
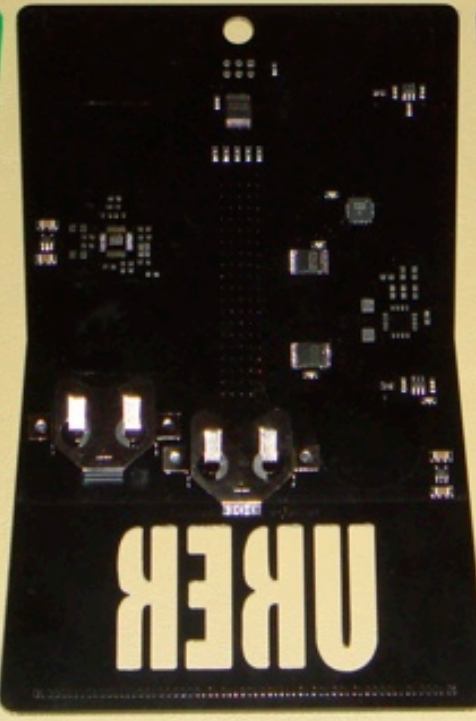


kingpin



Beauty shots...

kingpin



Kingpin

Badge hacking contest!



Visit table @ vendor area:
Source, schematics, etc. on CD

Soldering iron, tools, extra components, Freescale engineering support, development/coding station

Submissions due by 2pm Sunday

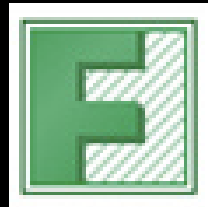
(Also, what can you do by DC16? Yes, a year!)

Wear it, use it, modify it, break it, learn from it.

kingpin

Hugs and kisses to:

Freescale (esp. Jim Barlow,
Angel Galarza, Oggie Kim)



Future Electronics (esp. Melissa Maynard) -
Parts sourcing and good pricing

Arrow Electronics - Microprocessor programming

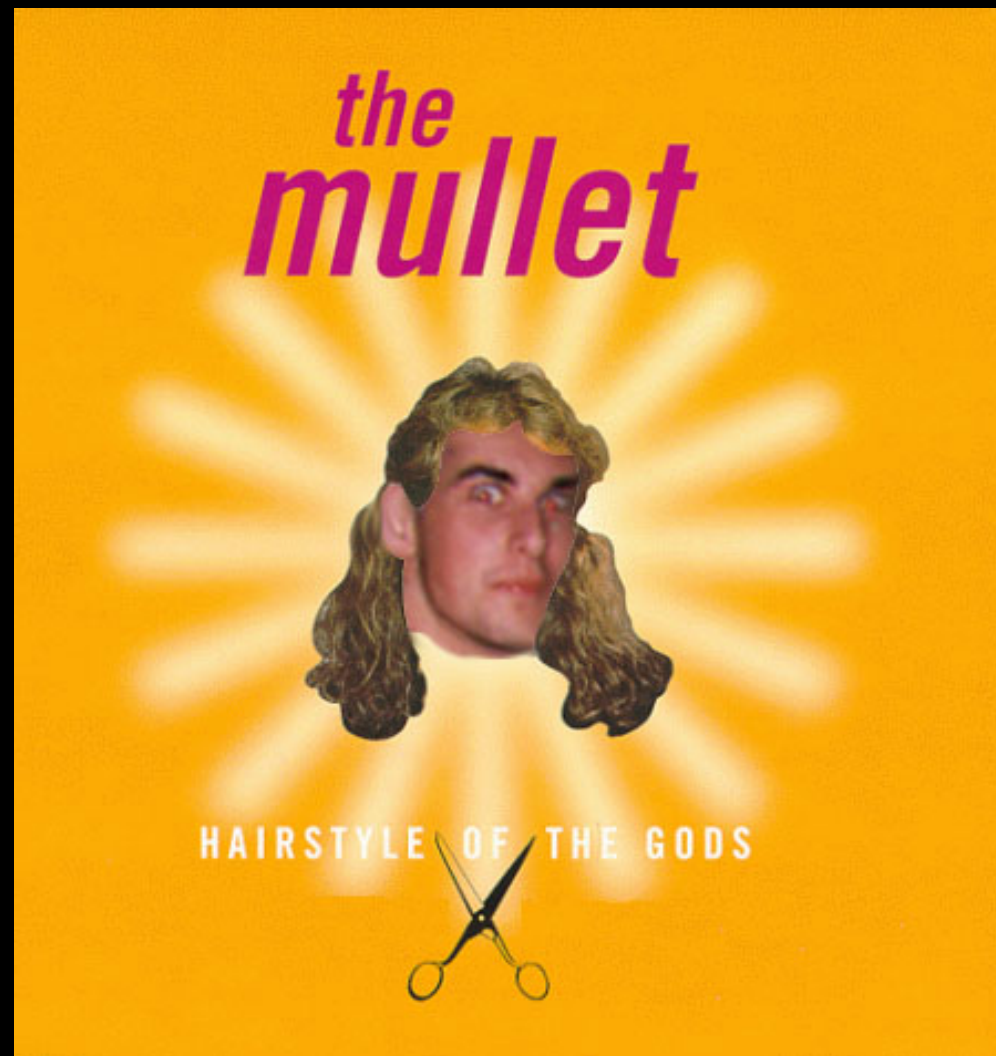


e-Teknet - PCB manufacturing and assembly

The Dark Tangent, Ping, and all BH/DC staff

kingpin

brought to you by joe grand.



[joe@grandideastudio.com]