Behind the Scenes of the DEFCON Badge

DEFCON 14

Friday, August 4

Joe Grand (Kingpin)

joe@grandideastudio.com

Thanks for Waking Up Early!

- We had to keep actual session title a secret until the badge was released
- We'll look at the entire development process of the badge from conception to production units
- Read the short story in the DEFCON program
- Sorry if you were looking for a different kind of hardware hacking!
- Interrupt me and ask questions!

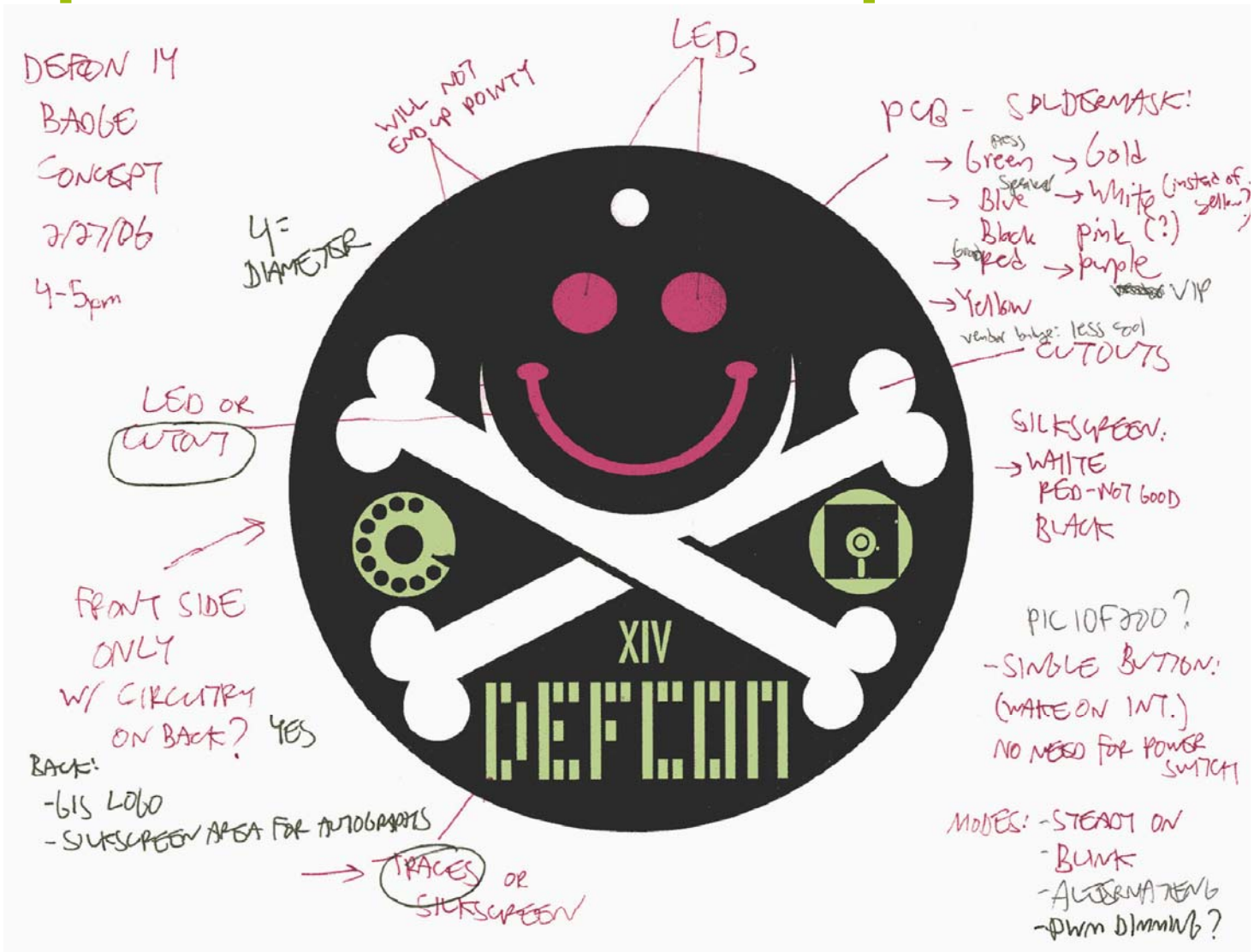
Development Process in a Nutshell

- Define the Specifications
- Preliminary Schematic
- Initial Breadboarding
- Code Development
- Final Schematic
- Create Bill-of-Materials
- Printed Circuit Board (PCB) Design
- Prototype Testing
- Parts Sourcing/Acquisition
- Place the Quantity Order

Specifications: Initial Proposal

- The Dark Tangent and Ping had a good idea of what they wanted before they called me
  - Quantity of 6,055 (that's a lot!)
  - Total cost of under $5
  - Badge in the shape of DEFCON logo
  - Blinky LEDs
  - Battery needs to last at least the length of DEFCON
  - Must look wicked pissah (east coast) and/or totally rad (west coast)

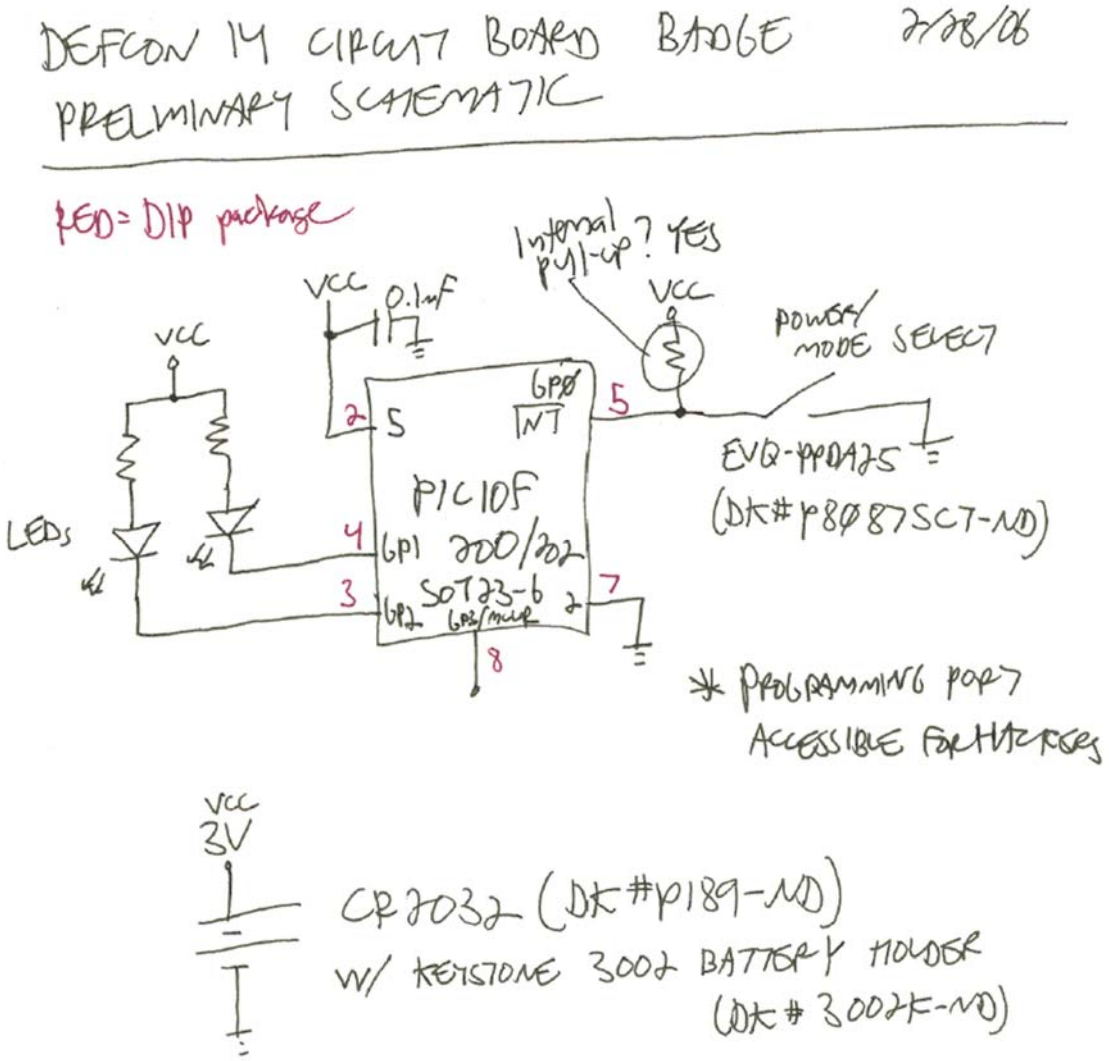
Specifications: Concept Sketch



Specifications: Defined Feature Set

- After some back-and-forth discussions, we settled on the functionality and artistic elements:
  - DEFCON logo and icons on top copper layer
  - Crossbones and smile to be cutout
  - Different soldermask colors for different DEFCON clientele
  - Single button for user control (no power switch)
  - Multiple LED states:
    - Both Steady On
    - Both Blink
    - Alternating
    - Random (Pseudo-random, actually)

Preliminary Schematic

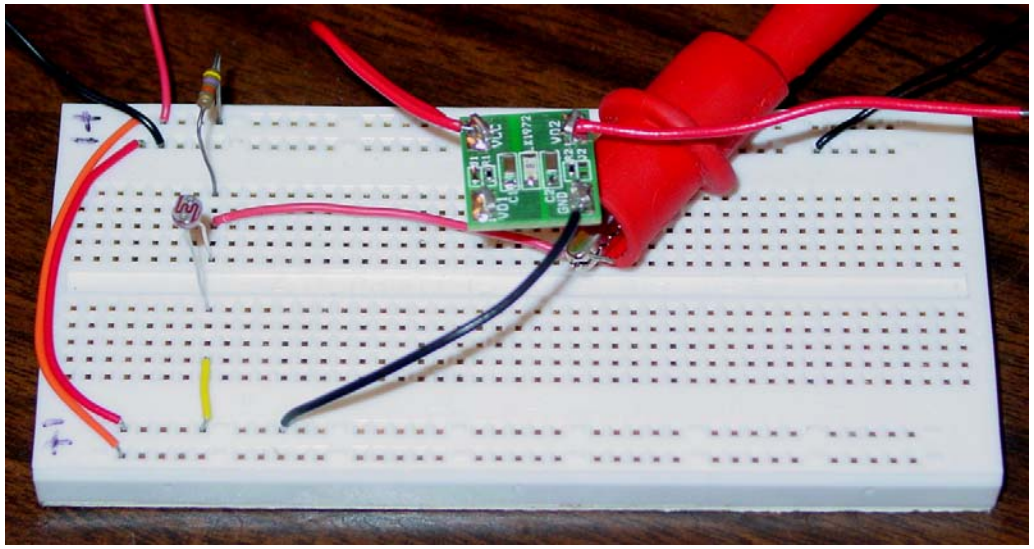


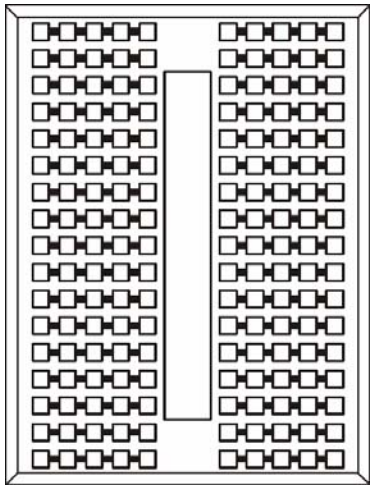
Breadboarding/Code Development

1. Turn preliminary sketch into something physical
2. Evaluate different types of LEDs
3. Write the embedded code for the Microchip PIC10F202 processor
4. Fine-tune and tweak hardware and code until it functions as specified

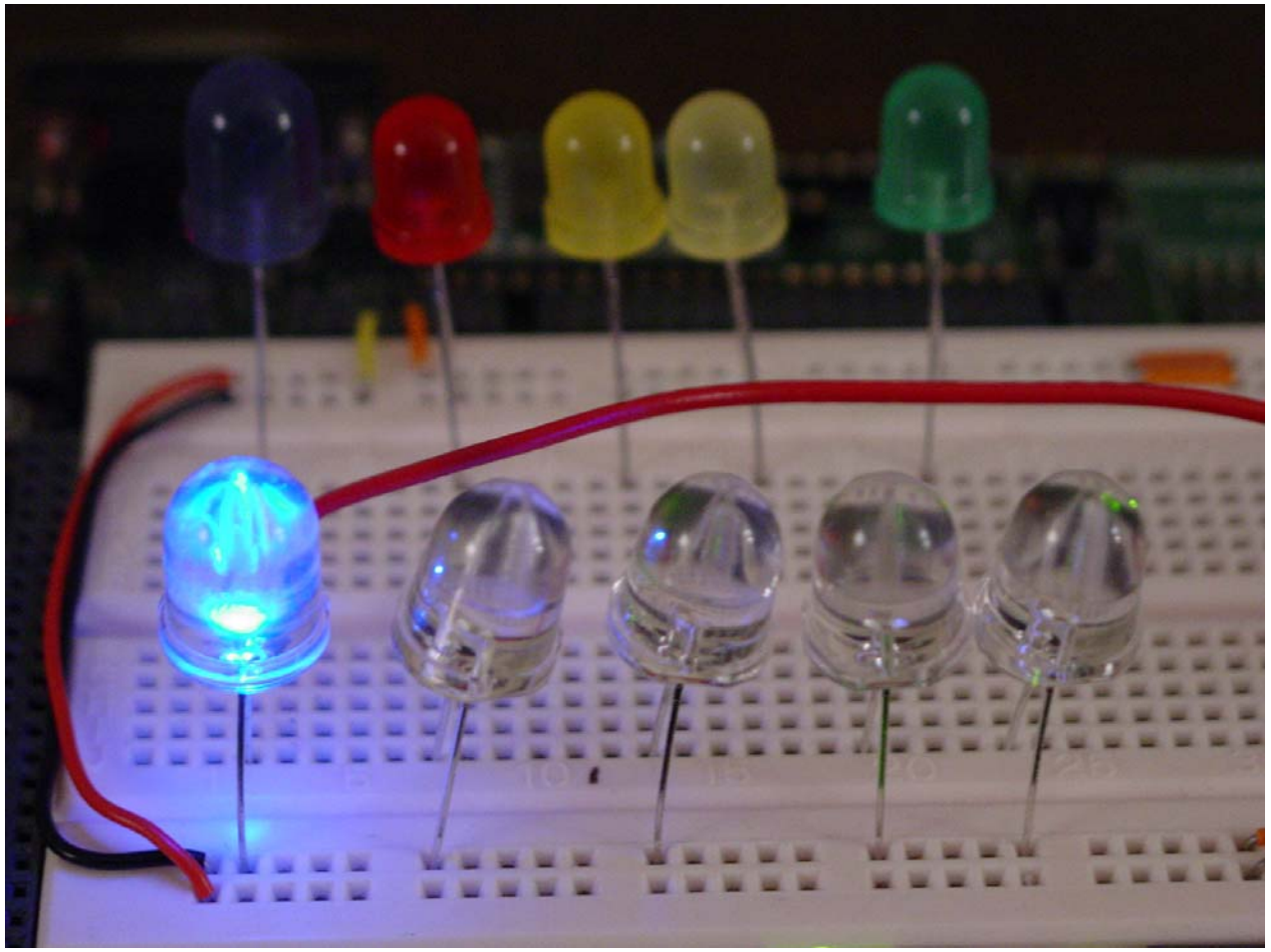
Breadboarding

- Breadboarding: A method to build circuits without soldering or creating custom PCBs
  - The ideal method of prototyping
  - Utilizes a plug board and 24AWG solid wire
  - Not recommended for high frequency/RF circuits

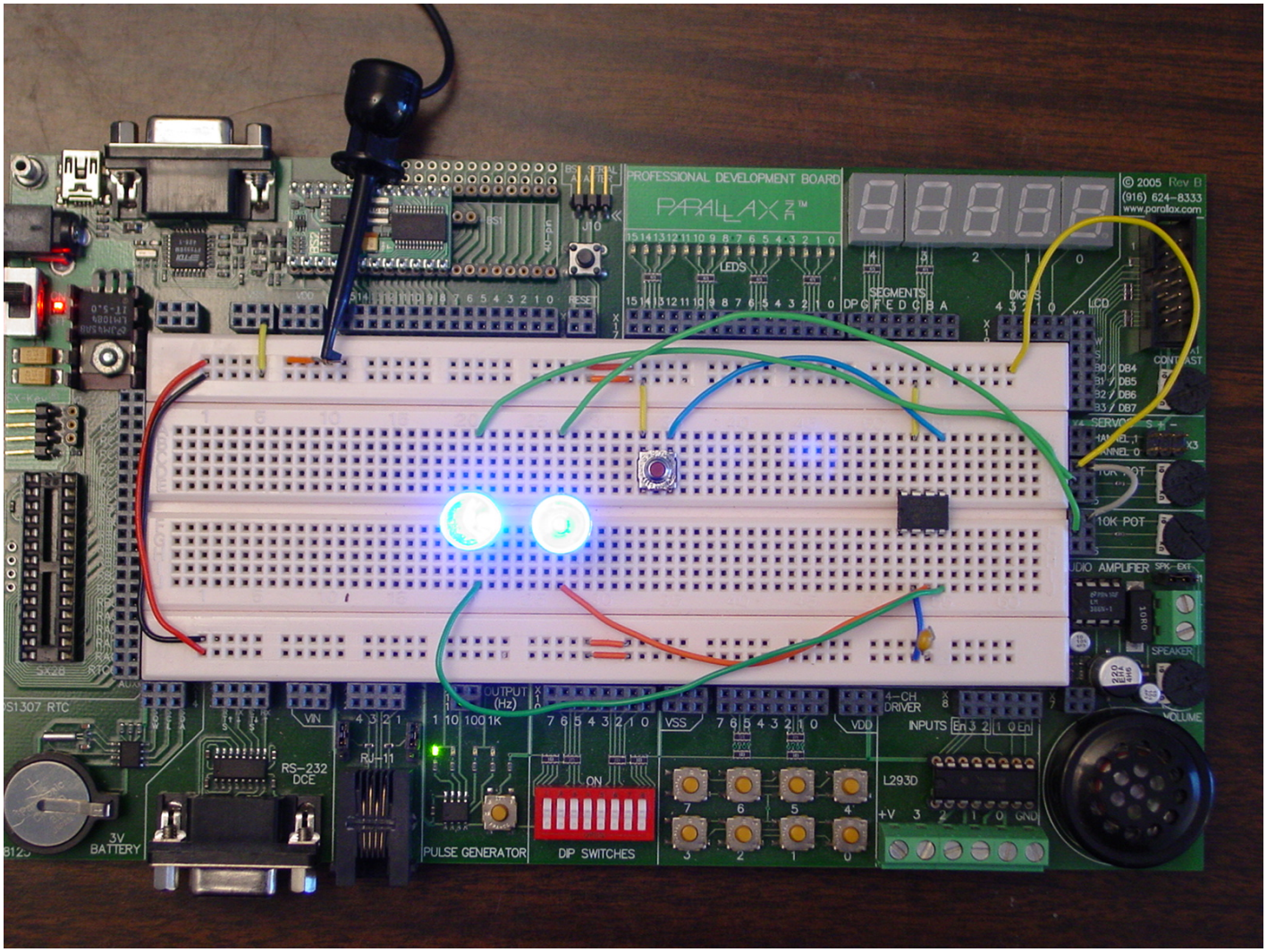




Breadboarding: LED Evaluation



Breadboarding: Prototype Circuitry

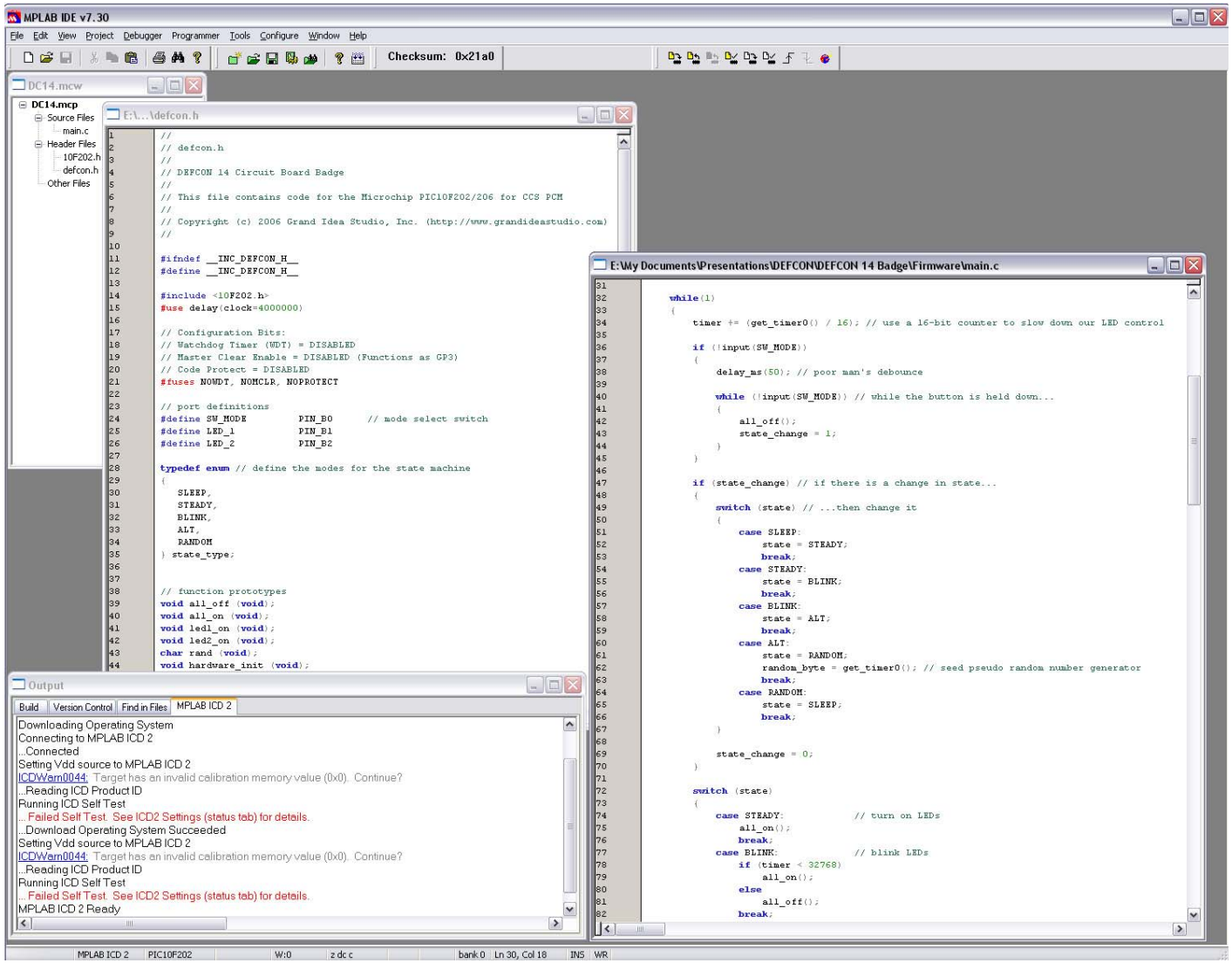


Code Development

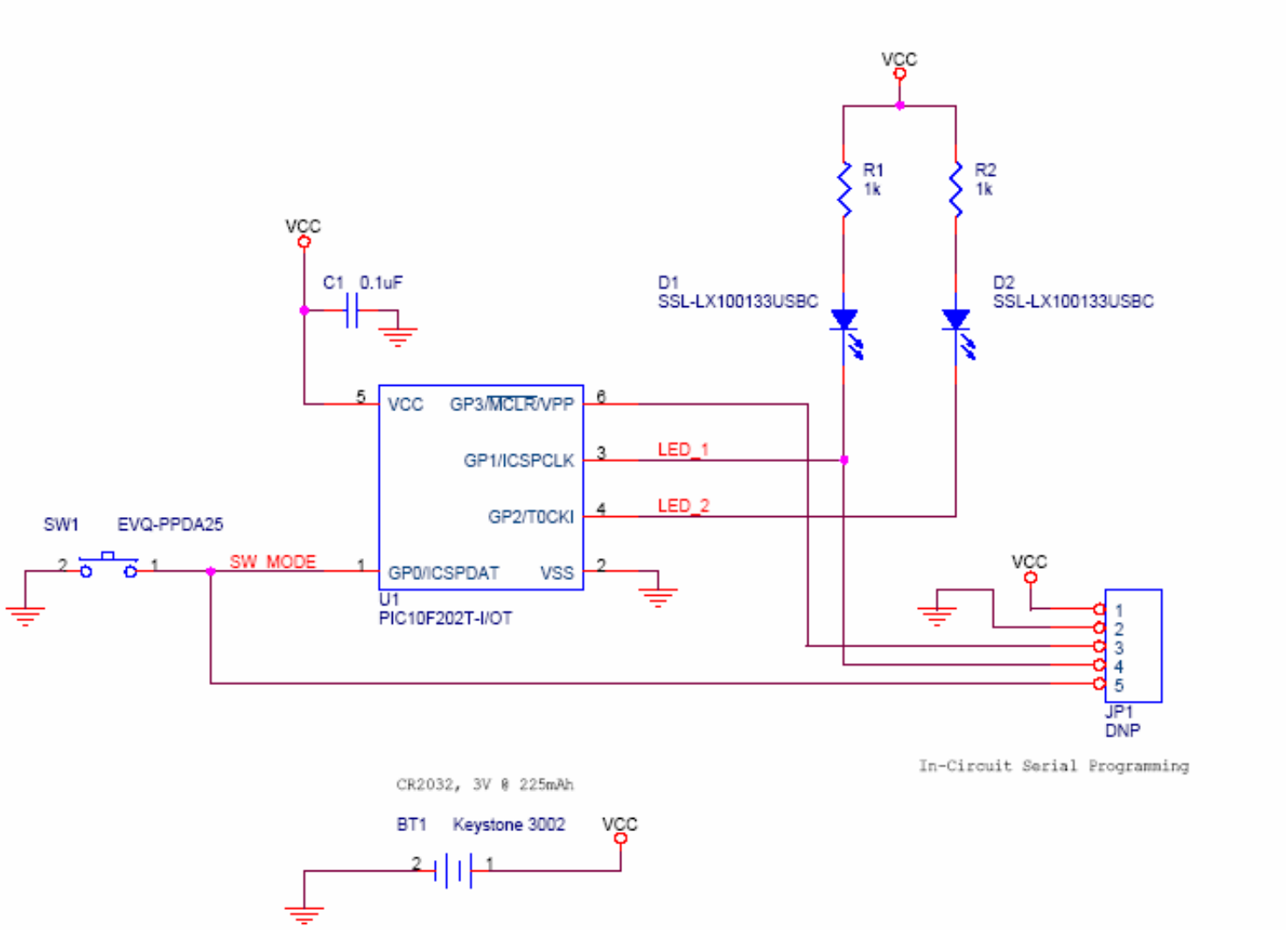
- Used CCS PCM compiler for Microchip PIC10F202 with MPLAB IDE v7.30
  - Ex.: **`www.ccsinfo.com`**
  - Free development tools are available, too (**`www.microchip.com`**)
- Simple state machine

```
typedef enum
{
   SLEEP,
   STEADY,
   BLINK,
   ALT,
   RANDOM
} state_type;
```


Code Development 2



Final Schematic



Drawing Schematics

- Many professional tools available, mostly in the $5k-$10k range
  - Ex.: Cadence/OrCAD Capture, **`www.orcad.com`**
  - Ex.: Altium/Protel DXP, **`www.altium.com`**
- Demo licenses for some professional tools
  - Usually expire after 30 days
- Some fully-free software available
  - Ex.: gEDA, **`http://geda.seul.org`**, complete open-source PCB, schematic capture, and simulation for Unix platforms

Drawing Schematics 2

- Microsoft Visio can perform rudimentary schematic capture using common symbols
  - Cannot easily create custom parts
  - Cannot export a Netlist for use with PCB design

Bill-of-Materials

- Cost issues (had to keep around $5/unit total)
- Had to make sure that all selected components were available in large quantities
- Used trusty Digi-Key and Mouser catalogs to create first draft BOM
- Enlisted Future Electronics to help with cost reduction and large quantity ordering
  - Typically 30% of the cost of Digi-Key, Mouser, etc.
  - More on this later…

Bill-of-Materials 2

GRAND idea studio

DEFCON 14 Circuit Board Badge
Bill-of-Materials
Document Version 1.3, April 17, 2006

Note: BOM is for budgetary purposes only and does not include shipping costs or taxes

Build Quantity 6055

Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description	Unit Price	Per Build	MIN/ MULT	Extended Price
1	1	BT1	Keystone	3002TR	FAI	3002TR	Battery holder, 20mm coin cell, SMD	$0.1050	6000	500/ 500	$630.00
					Mouser	534-3002TR		$0.6100	60		$36.60
1a	1	N/A	Renata Batteries	CR2032	FAI	CR2032	CR2032 Lithium 3V Coin Cell Battery (225mAh)	$0.2500	6075	500/ 25	$1,518.75
2	1	C1	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603	$0.0095	8000	4000/ 4000	$76.00
3	2	D1,D2	Lumex	SSL-LX100133USBC	FAI	SSL-LX100133USBC	10mm LED, Blue water clear, 800mcd, 3.5V	$0.7000	12200	100/ 100	$8,540.00
4	2	R1,R2	Any	CRCW0603-102JRT1	FAI	CRCW0603-102JRT1	1.0k, 5%, 1/10W, 0603	$0.0016	15000	5000/ 5000	$24.00
5	1	SW1	Panasonic	EVQ-PPDA25	Digi-Key	P8087STR-ND	SPST momentary pushbutton switch, 240gf, 50mA, SMD	$0.3250	6060		$1,969.50
6	1	U1	Microchip	PIC10F202T-I/OT	Digi-Key	PIC10F202T-I/OTTR-ND	PIC Microcontroller, SOT23-6 (includes programming)	$0.9416	6055		$5,701.39
7	1	PCB	e-Teknet	DEFCON 1.0	e-Teknet		PCB (includes assembly and testing)	$2.3100	6055		$13,987.05

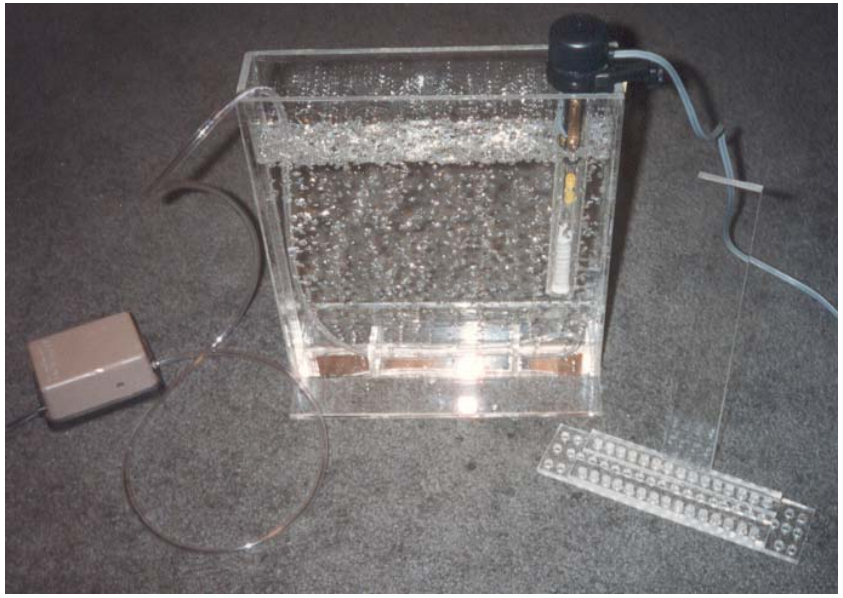
Total **$32,483.29**
Approximate Per Unit Cost **$5.36**

PCB Design

- Three general methods to create custom PCBs:
  1. Homebrew w/ PCB etching kit
  2. PCB prototyping systems
  3. Professional fabrication
- Printed Circuit Board (PCB) etching kit
  - Low-cost method for quick homebrew hacks (practically instant gratification)
  - Uses hazardous chemicals (ferric chloride) which etch away any copper on the circuit board that isn't protected by resistant ink or toner
  - Ex.: MAKE Magazine issue 2

PCB Design 2

November 1993



April 2000

PCB Design 3

- PCB prototyping systems
  - Highly specialized, accurate CNC machine
  - Allows quick in-house creation of prototype PCBs
  - > $10k for a decent system
  - Not practical for most hardware hacking purposes
  - Ex.: LPKF Laser & Electronics (**`www.lpkf.com`**) and T-Tech (**`www.t-tech.com`**)

PCB Design 4

- Professional fabrication
  - More convenient and better quality than homebrew, why bother with dangerous chemicals anymore?
  - Can handle very fine pitch, tight tolerances, etc.
  - Prototype and production quantities
  - Competition between firms leads to good deals for us
    - Prototype specials
    - On-time guarantees
    - Price matching
  - 2-layer board costs ~$20-30 each (~$1-$5 in quantity)
  - 4-layer board costs ~$50 each (~$3-$10 in quantity)

PCB Design 5

- Many production houses available online
  - e-Teknet, **`www.e-teknet.com`**
  - Advanced Circuits, **`www.4pcb.com`**
  - Sierra Proto Express, **`www.sierraprotoexpress.com`**
  - AP Circuits, **`www.apcircuits.com`**
  - Express PCB, **`www.expresspcb.com`**
- e-Teknet fabricated and assembled the prototype and production DEFCON badges
  - Check them out in the exhibitor area…
  - (No, I didn't get paid to put this in here!)

PCB Design 6

- Design tools…
  - Many professional tools available, some upwards of $5k-$10k
    - Ex.: Altium/Protel DXP, **`www.altium.com`**
    - Ex.: McCAD EDS, **`www.mccad.com`**, 200 pin limit for free
  - Some fully-free software available
    - Ex.: gEDA, **`http://geda.seul.org`**, complete open-source PCB, schematic capture, and simulation for Unix platforms
    - Ex.: Protel EasyTrax, **`www.protel.com/downloads/files/easytrax.zip`**, DOS freeware version, complete PCB layout package with output support for printers and Gerber
    - Ex.: Express PCB offers a free captive design tool for use with their own manufacturing

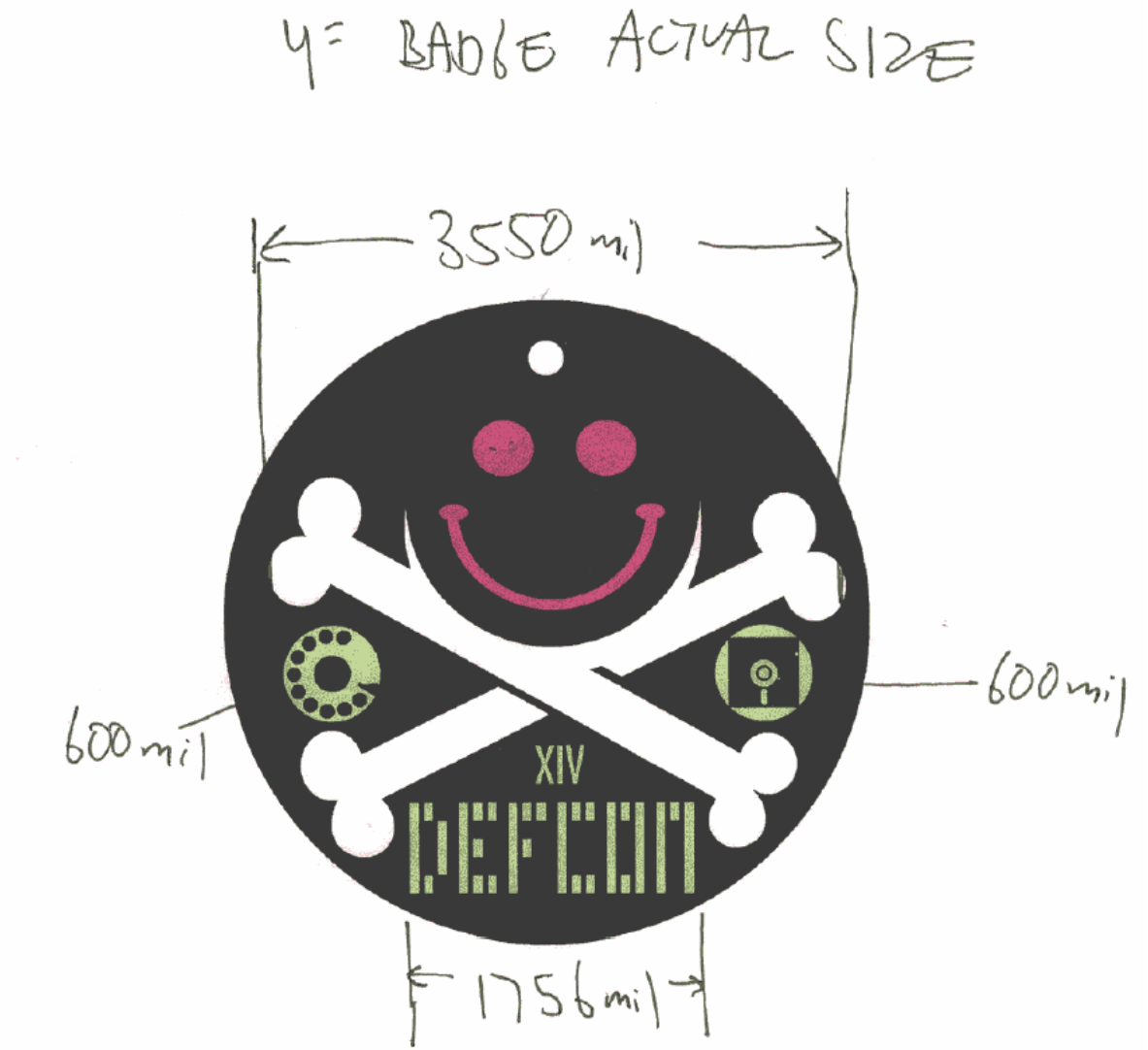
PCB Design 7

- High-level process:
  1. Create schematic
  2. Output Netlist
  3. Import Netlist into PCB design software
  4. Create PCB
  5. Output Gerber plots
  6. Submit Gerber plots to PCB fab house

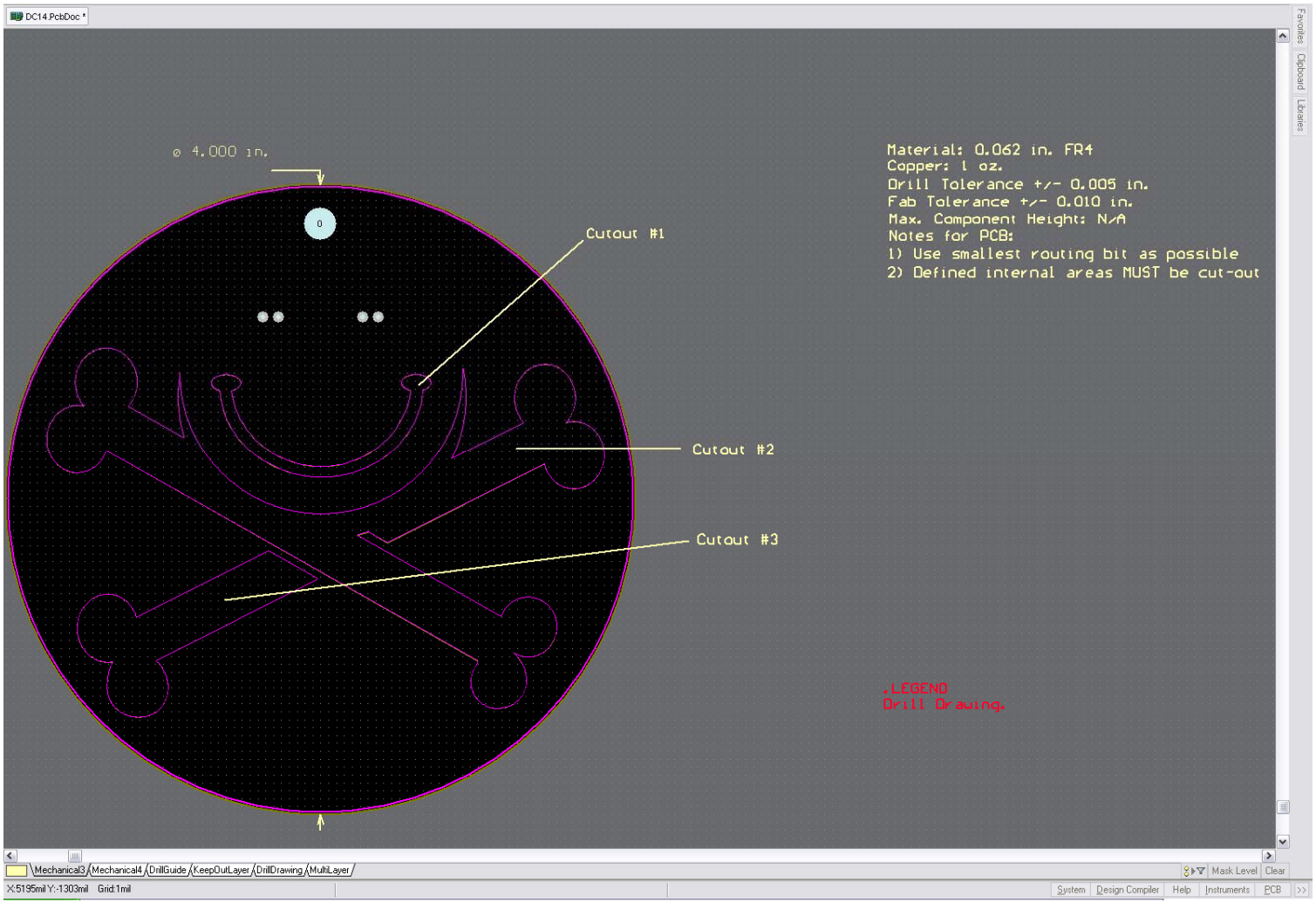
Badge PCB Design: Process

1. Verify desired size of badge & artistic elements
2. Create mechanical outline of board
3. Add logos to top side copper
4. Place components in desired locations
5. Import Netlist (based on final schematic)
6. Route board (keep all traces on bottom side)
7. Add logos to bottom side silkscreen
8. Run verification tests
9. Output Gerber plots

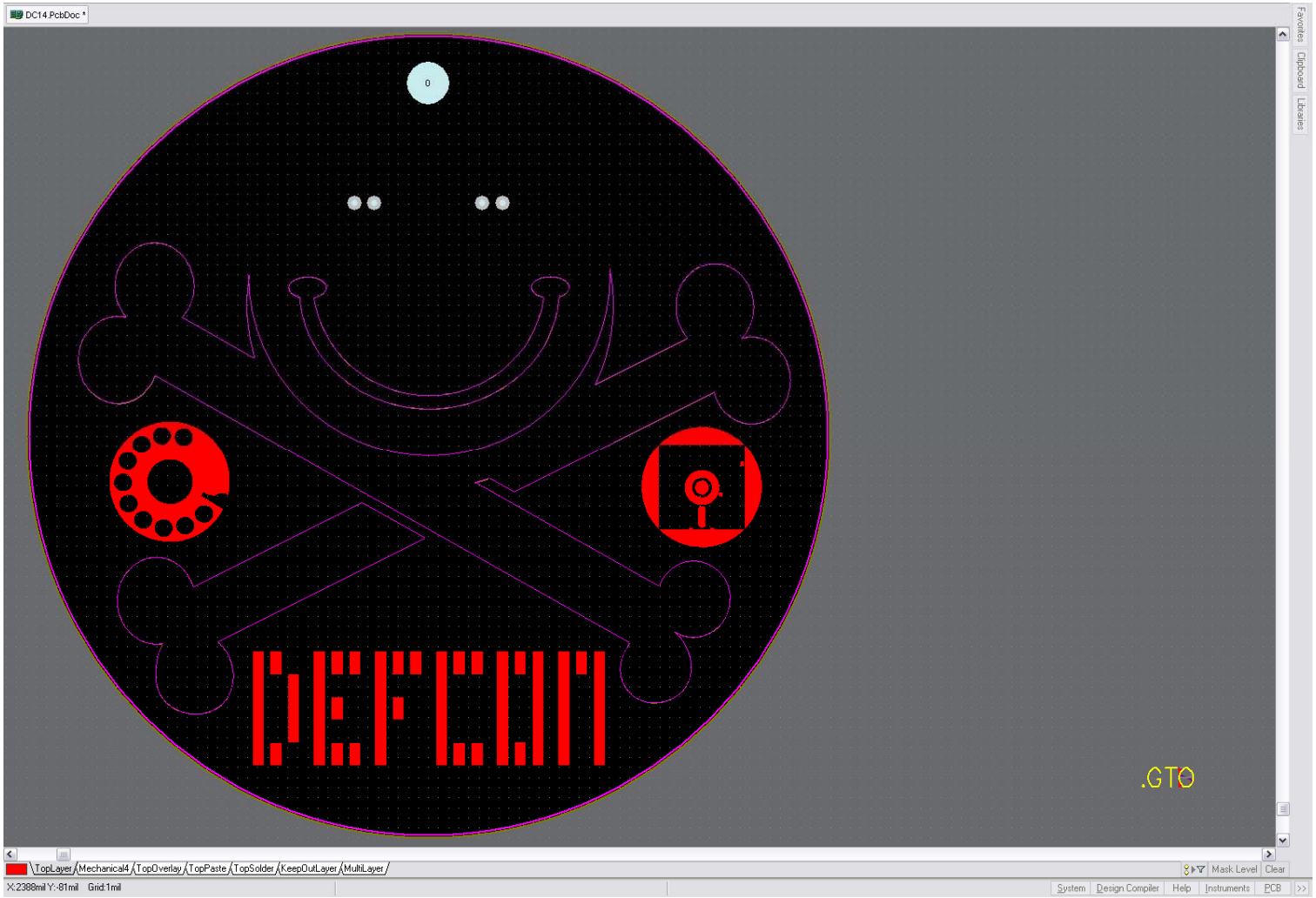
Badge PCB Design: Verifying Sizes



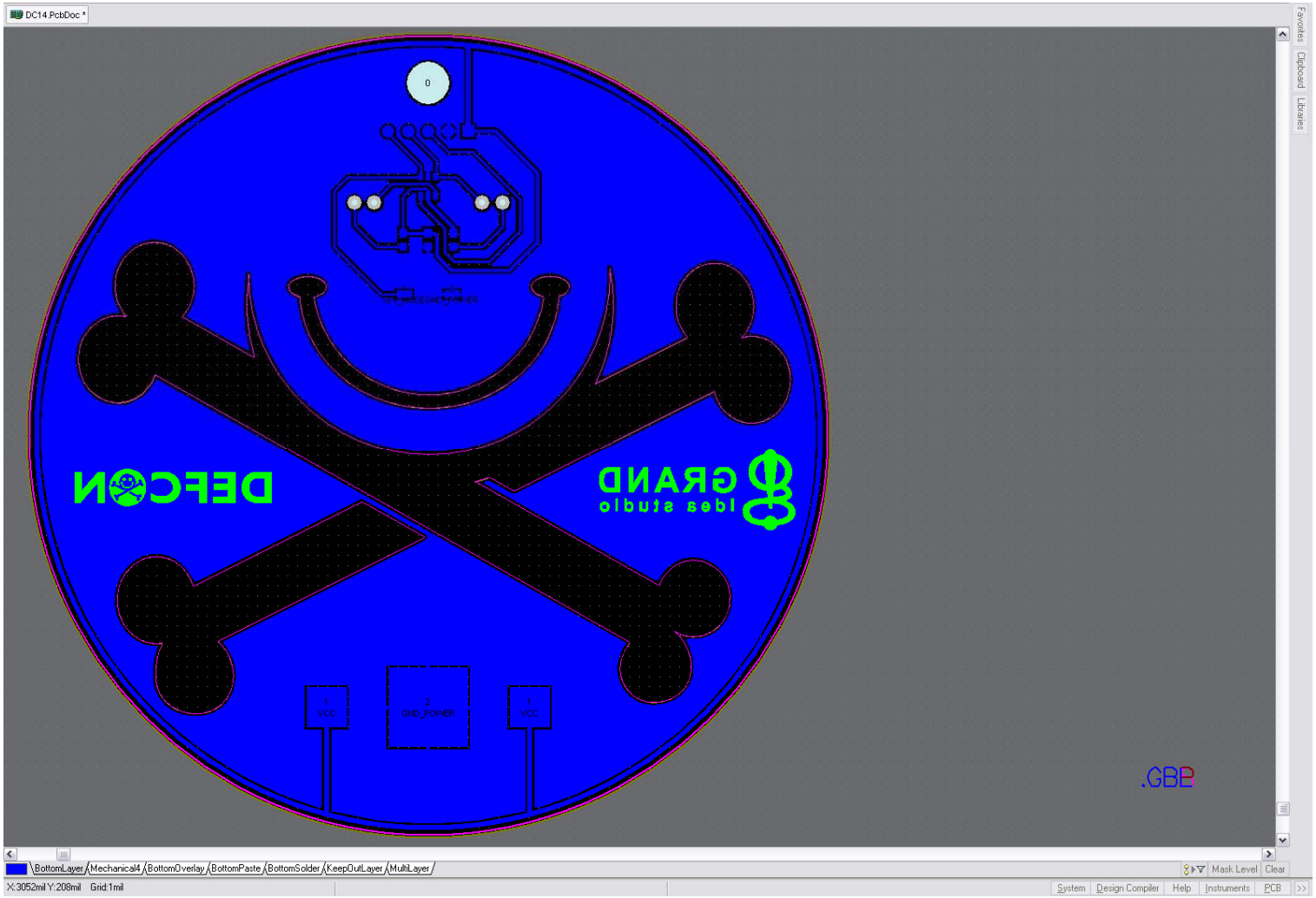
Badge PCB Design: Mechanical Layer



Badge PCB Design: Top Layer



Badge PCB Design: Bottom Layer

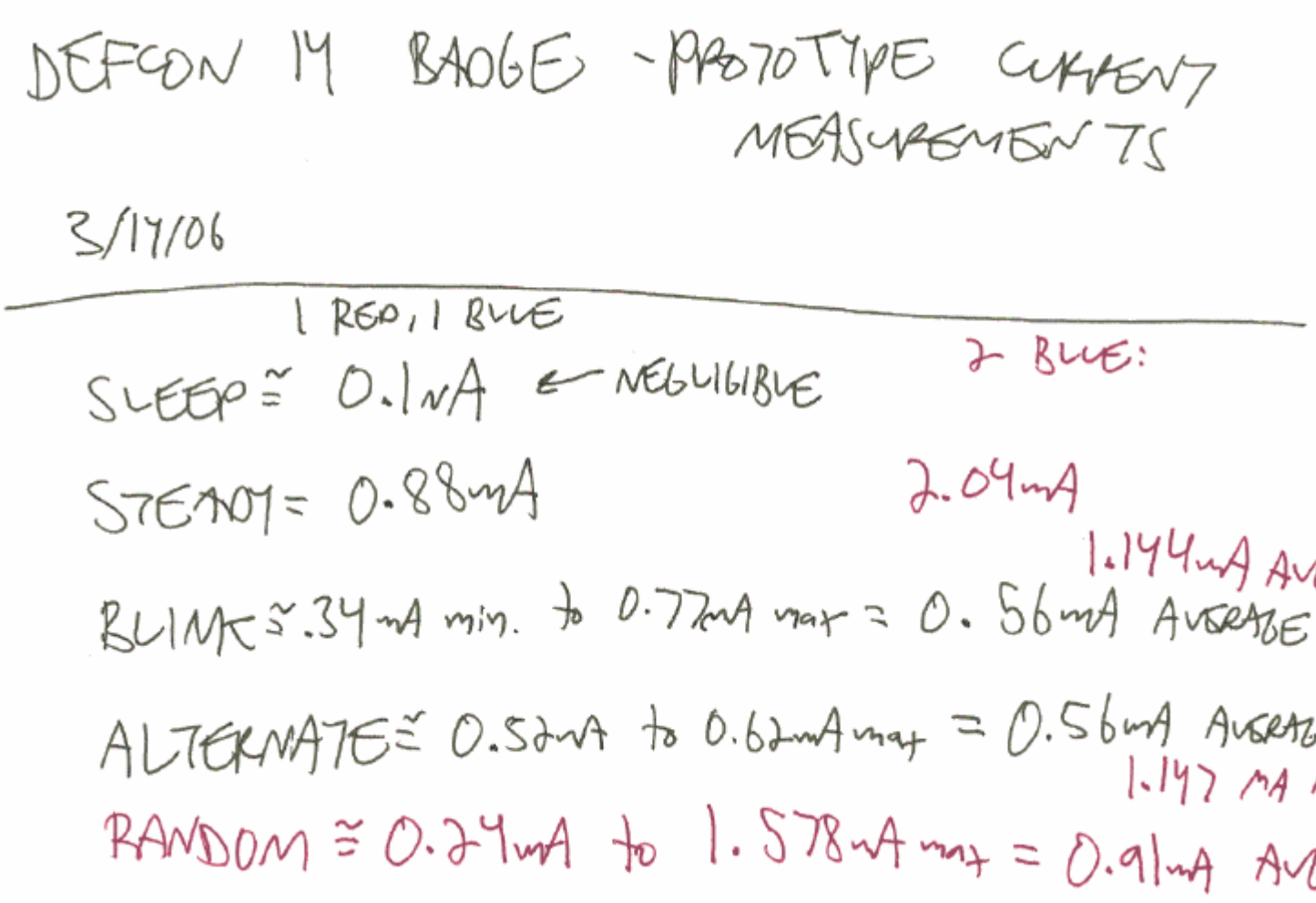


Badge PCB Design: Mock-up

Prototype Testing

- Before placing large order of PCBs, need to verify that the design functions as expected
- Ordered a few bare prototype PCBs from e-Teknet
  - Had careful discussions with them to ensure that our complicated cutout areas and features were conveyed properly to their Chinese factory
  - I'm sure they're sick of me by now! ☺
- Hand-assembled some boards
- Sent to The Dark Tangent and Ping for final sign-off

Prototype Testing: Current Measurements



Prototype Testing: Current Measurements 2

CR2032 = 3V @ 225mAh to 2V

BASED ON IDEAL CONDITIONS; CONTINUOUS USE:

SLEEP = 256.8 YEARS → Battery would self-discharge before then!*

STEADY = 255.7 HOURS = 10.6 DAYS 110.3 HOURS = 4.6 DAYS

BLINK/ALTERNATE = 401.78 HOURS = 16.7 DAYS 196.7 HOURS = 8.2 DAYS

RANDOM = 247.25 HOURS = 10.3 DAYS

Joe says “A-OK!”

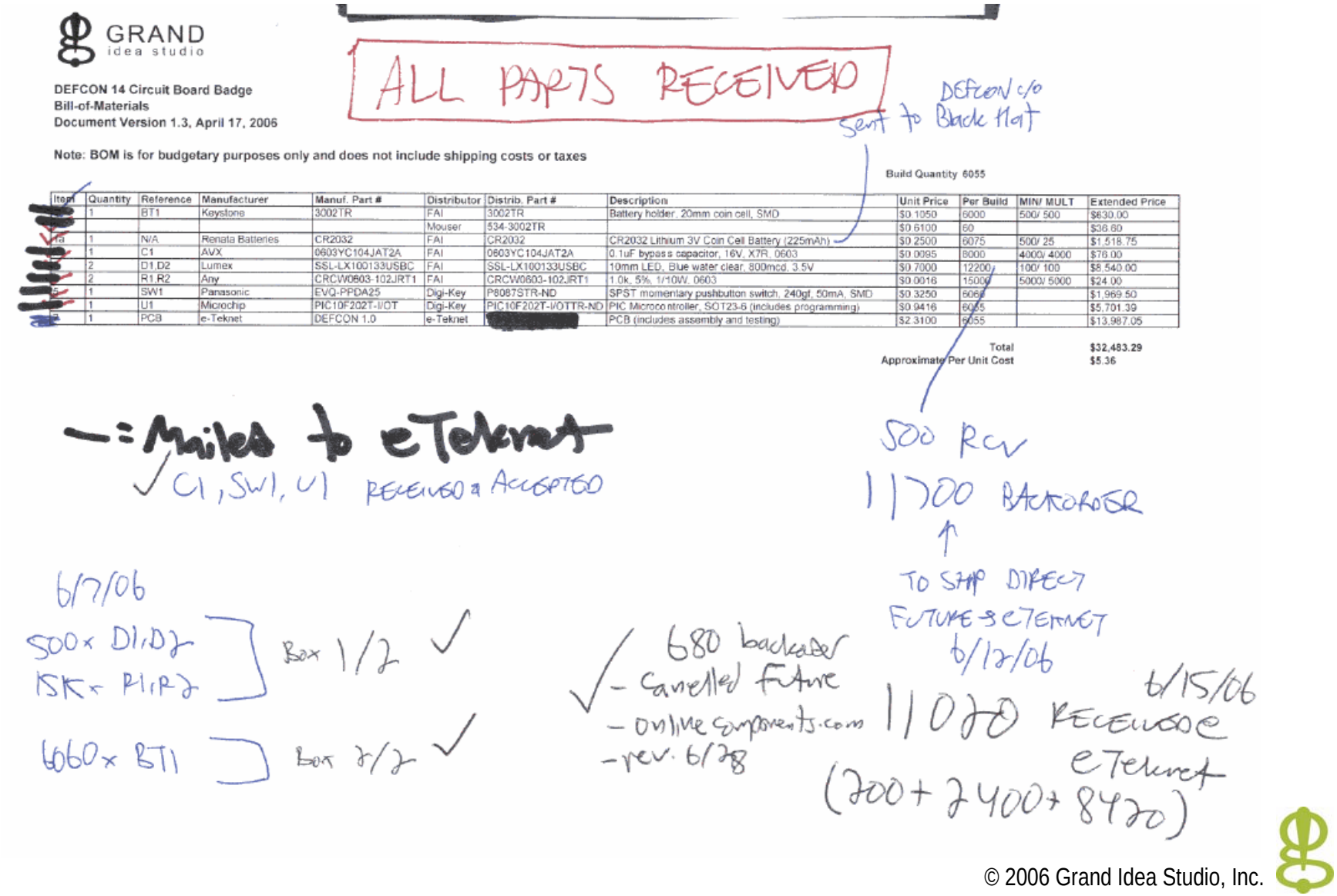
Parts Sourcing

- Ended up being the most difficult/time consuming part of the process
- On strict deadline to obtain parts for 6,055 units and ship to e-Teknet to begin assembly
  - No parts == No badges for DEFCON! ☹
- Placed all quantity orders with Future Electronics
- Since Future (and most large distributors) has minimums and multiple requirements, ordered remaining pieces from Digi-Key & Mouser
- Used Digi-Key to purchase and program code into PIC10F202s

Parts Sourcing 2

- Issues w/ Future:
  - Misquoted leadtimes
    - “They’ll be here in 3 weeks” – parts arrive after 6
  - “Lost” parts
    - Only 500 LEDs were shipped – sales couldn’t find the other 11,700!?
  - Slow shipping
    - What part of “I need these parts tomorrow” do you not understand?
- After much pressure, I was “upgraded” to a more competent sales contact
- All problems were finally resolved!

Parts Sourcing 3



GRAND idea studio

DEFCON 14 Circuit Board Badge
Bill-of-Materials
Document Version 1.3, April 17, 2006

ALL PARTS RECEIVED

Sent to Black Hat DEFCON c/o

Note: BOM is for budgetary purposes only and does not include shipping costs or taxes

Build Quantity 6055

Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description	Unit Price	Per Build	MIN/ MULT	Extended Price
[redacted]	1	BT1	Keystone	3002TR	FAI	3002TR	Battery holder, 20mm coin cell, SMD	$0.1050	6000	500/ 500	$630.00
					Mouser	534-3002TR		$0.6100	60		$36.60
[redacted]	1	N/A	Renata Batteries	CR2032	FAI	CR2032	CR2032 Lithium 3V Coin Cell Battery (225mAh)	$0.2500	6075	500/ 25	$1,518.75
[redacted]	1	C1	AVX	0603YC104JAT2A	FAI	0603YC104JAT2A	0.1uF bypass capacitor, 16V, X7R, 0603	$0.0095	8000	4000/ 4000	$76.00
[redacted]	2	D1,D2	Lumex	SSL-LX100133USBC	FAI	SSL-LX100133USBC	10mm LED, Blue water clear, 800mcd, 3.5V	$0.7000	12200	100/ 100	$8,540.00
[redacted]	2	R1,R2	Any	CRCW0603-102JRT1	FAI	CRCW0603-102JRT1	1.0k, 5%, 1/10W, 0603	$0.0016	15000	5000/ 5000	$24.00
[redacted]	1	SW1	Panasonic	EVQ-PPDA25	Digi-Key	P8087STR-ND	SPST momentary pushbutton switch, 240gf, 50mA, SMD	$0.3250	6060		$1,969.50
[redacted]	1	U1	Microchip	PIC10F202T-I/OT	Digi-Key	PIC10F202T-I/OTTR-ND	PIC Microcontroller, SOT23-6 (includes programming)	$0.9416	6055		$5,701.39
[redacted]	1	PCB	e-Teknet	DEFCON 1.0	e-Teknet	[redacted]	PCB (includes assembly and testing)	$2.3100	6055		$13,987.05
							Total				$32,483.29
							Approximate Per Unit Cost				$5.36

—= Mailed to eTeknet

✓ C1, SW1, U1 RECEIVED & ACCEPTED

500 Rcv
11700 BACKORDER
↑
TO SHIP DIRECT
FUTURE - eTEKNET
6/12/06

6/7/06
500x D1,D2
15K x R1,R2
] Box 1/2 ✓

6060x BT1] Box 2/2 ✓

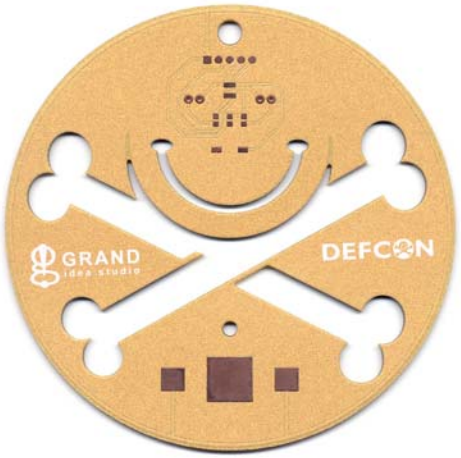
✓ 680 backorder
- Cancelled Future
- onlinecomponents.com
- rev. 6/28

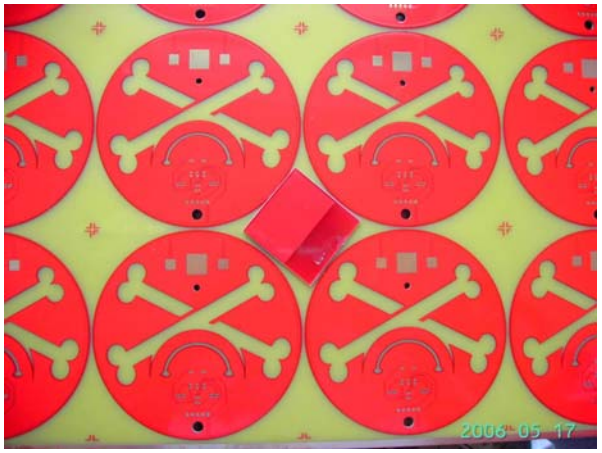
11070 RECEIVED 6/15/06
eTeknet
(700 + 2400 + 8420)

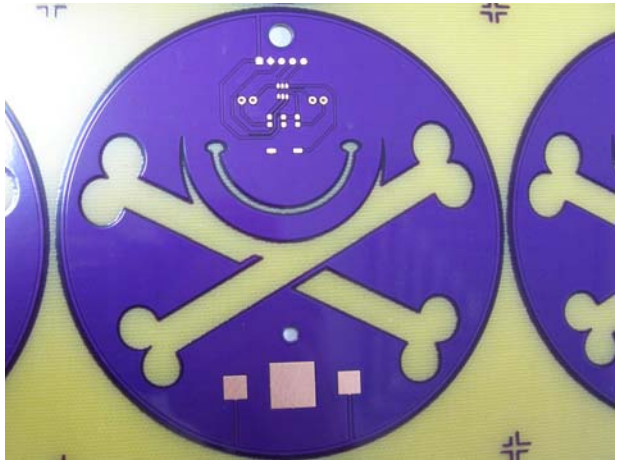
Quantity Order

- Placed 6,055 unit order with e-Teknet
- While components were being acquired, they helped us decide on the seven soldermask colors and began PCB fabrication
- Sent them BOM, Parts Placement, and Test Procedure to aid in assembly
- Tested and approved First Articles
- Pulled the trigger on the full quantity build!

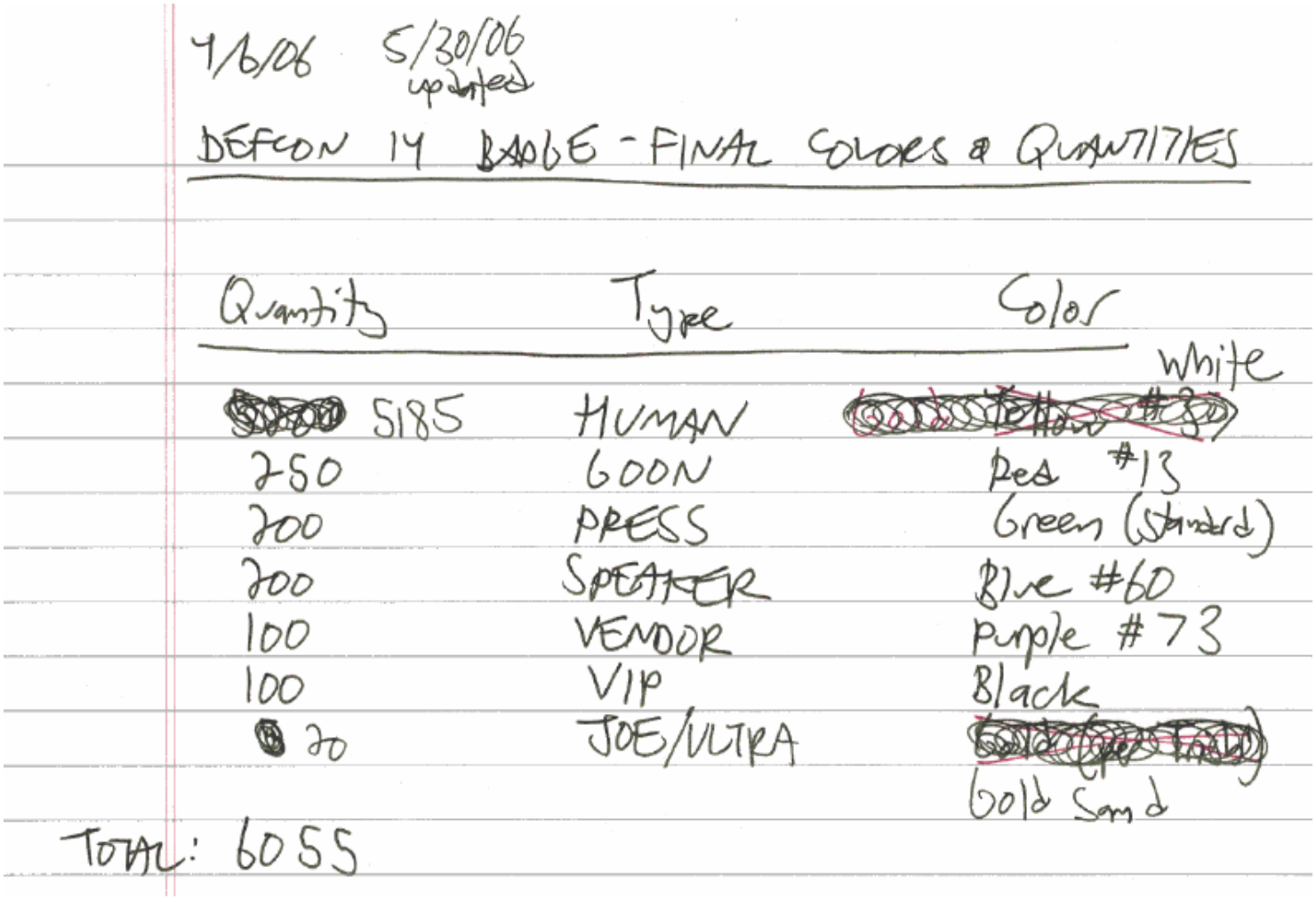
Quantity Order: Color Samples







Quantity Order: Final Colors



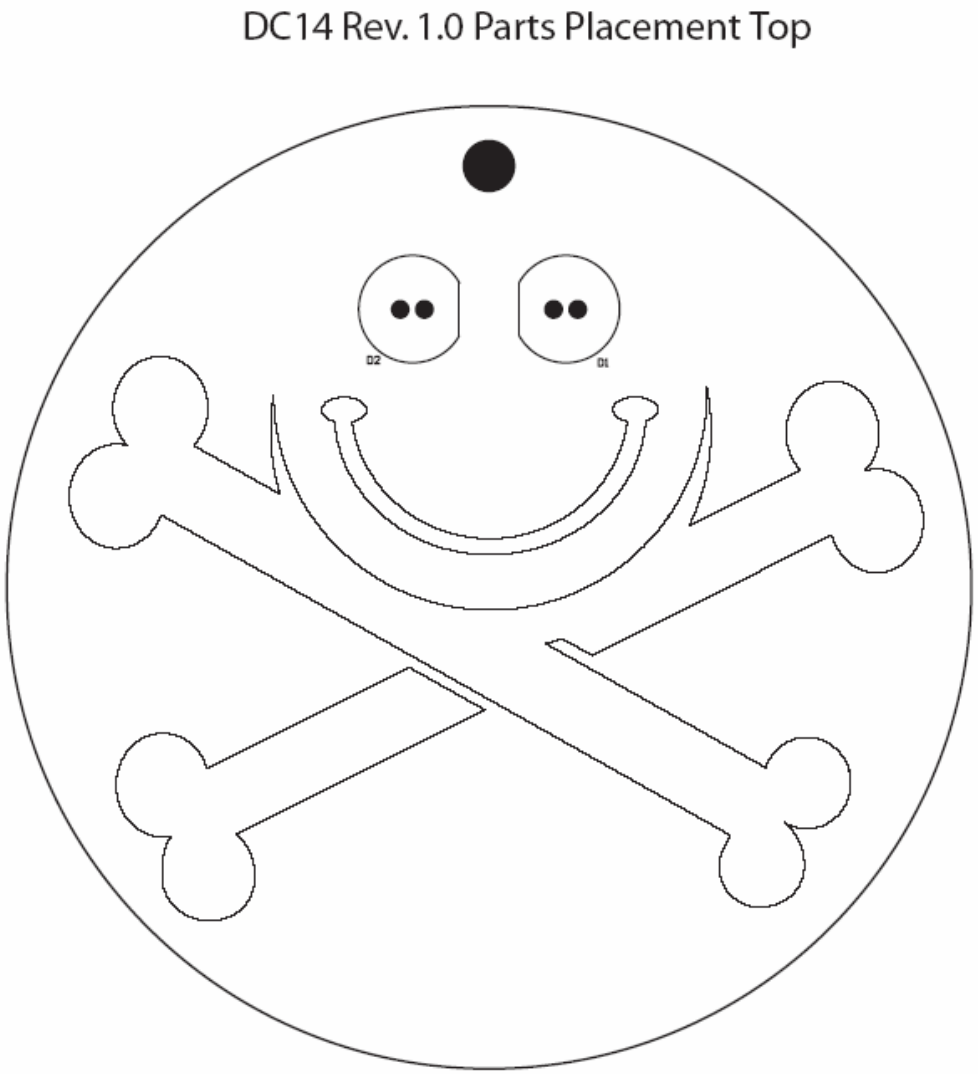
4/6/06 5/30/06 updated

DEFCON 14 BADGE - FINAL COLORS & QUANTITIES

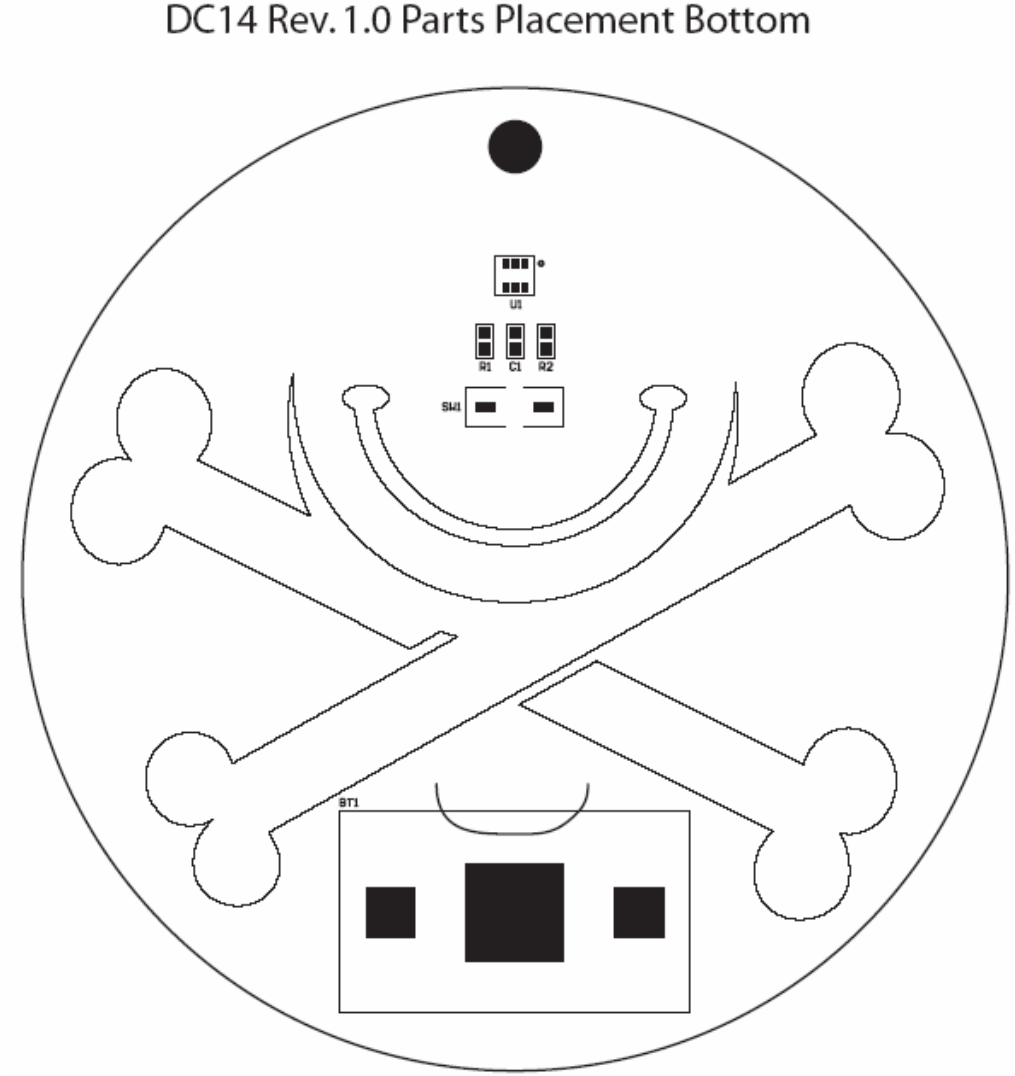
Quantity	Type	Color
[redacted] 5185	HUMAN	White [redacted]
250	GOON	Red #13
200	PRESS	Green (Standard)
200	SPEAKER	Blue #60
100	VENDOR	Purple #73
100	VIP	Black
[redacted] 20	JOE/ULTRA	[redacted] Gold Sand

TOTAL: 6055

Parts Placement



Parts Placement 2



Test Procedure

GRAND idea studio

DEFCON

DEFCON 14 Badge Revision 1.0
System Level Test Procedure

J. Grand, April 9, 2006

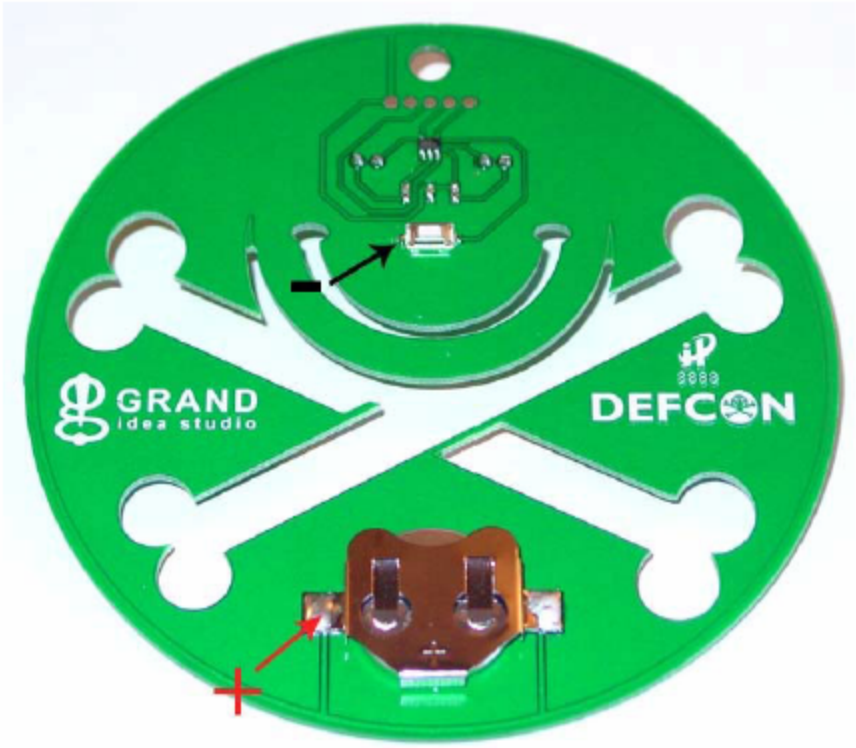
Front

Back

Test Procedure 2

Test Procedure:

1. Insert CR2032 lithium coin cell battery or apply power (+3V DC) to the following points:



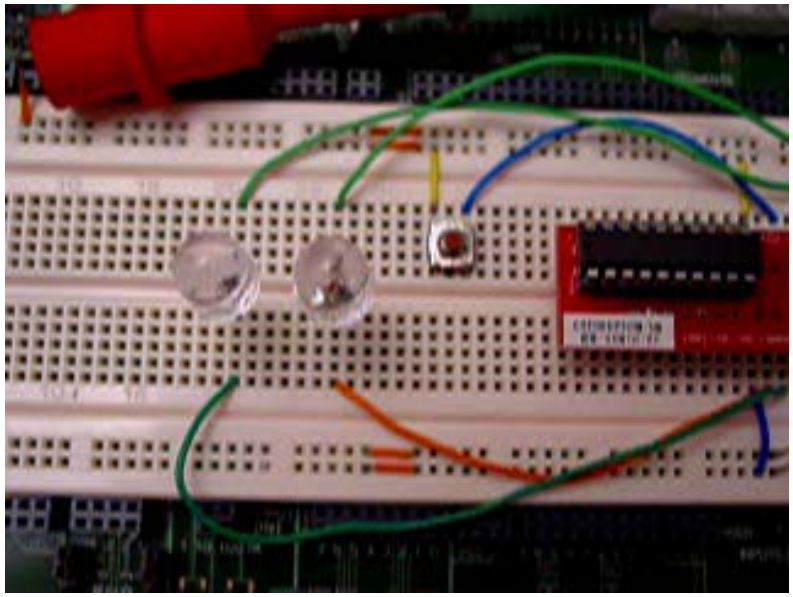
Test Procedure 3

2. Press and release momentary switch on back of PCB
3. Both LEDs on front should illuminate:

Test Procedure 4

4. Press and release momentary switch on back of PCB
5. Both LEDs on front should blink on and off together
6. Press and release momentary switch on back of PCB
7. LEDs on front should alternate on and off (left on, right on, left on, etc.)
8. Press and release momentary switch on back of PCB
9. LEDs on front should illuminate in some random order
10. Press and release momentary switch on back of PCB
11. Both LEDs on front should be off
12. Remove power
13. Test complete

Test Procedure 5



First Article Approval: Front

First Article Approval: Back

DEFCON Badge Hacking Contest

- What can **you** do with two LEDs, a switch, some discretes, and a Microchip PIC10F202?
- The most obscure, obscene, or mischievous badge hack will be recognized and awarded at the DEFCON Award Ceremonies on Sunday
- Microchip development tools are available at the show for your use
- Find me later if you want to check out what I've done to mine ☺

Thanks for Coming!

Joe Grand (Kingpin)

joe@grandideastudio.com