Making the DEFCON 16 Badge

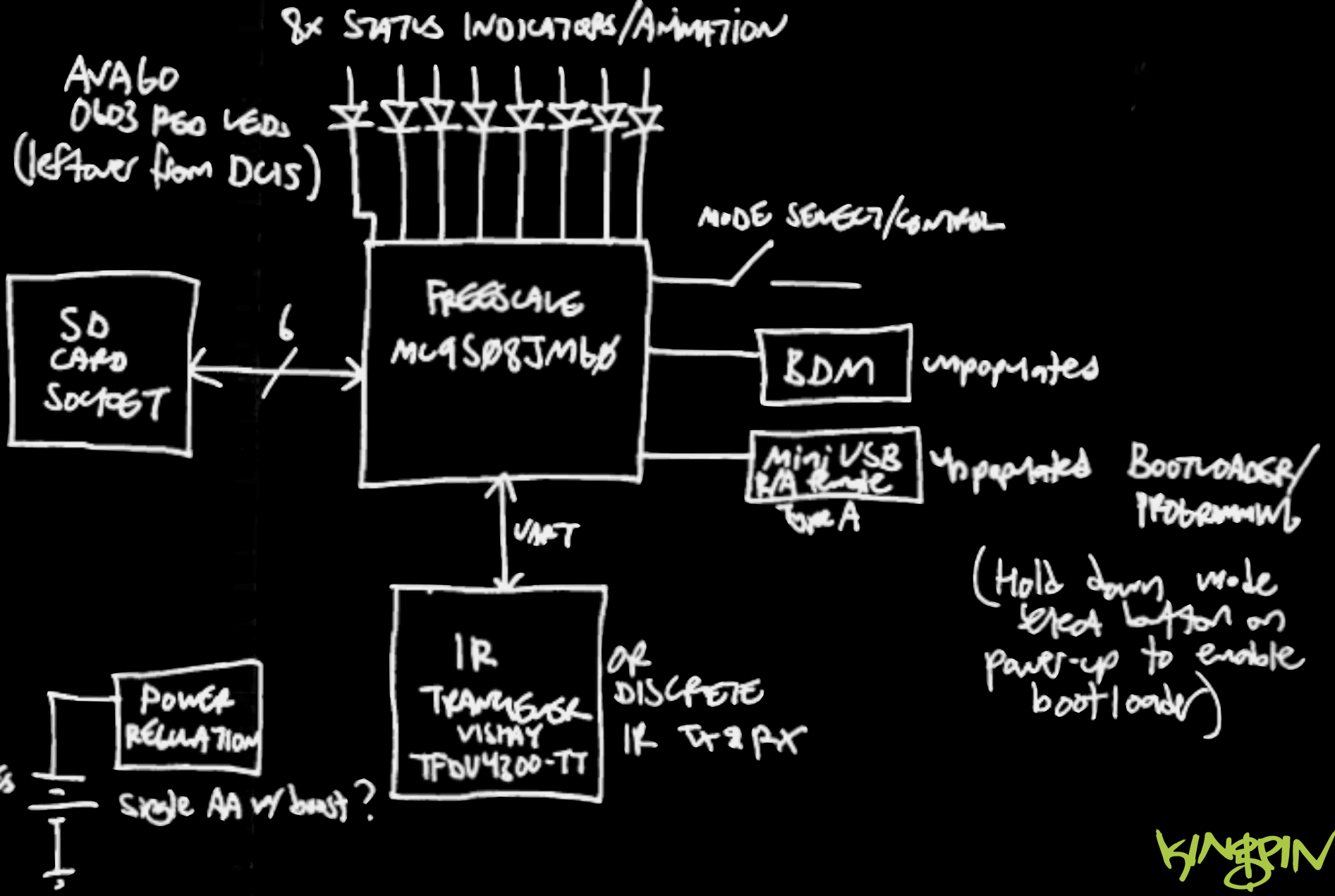
Joe Grand aka Kingpin

Hardware
Firmware
Manufacturing

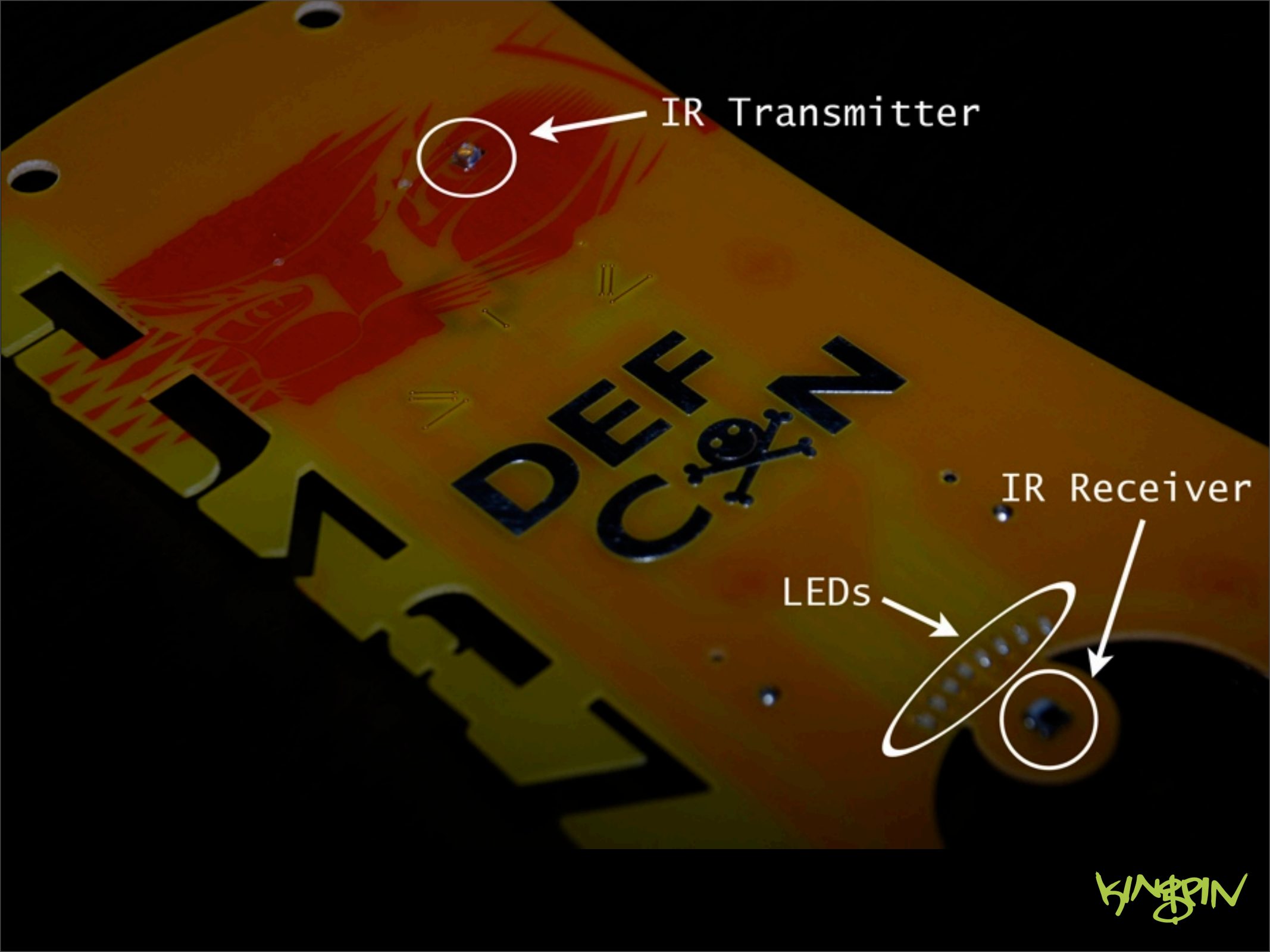
KINGPIN

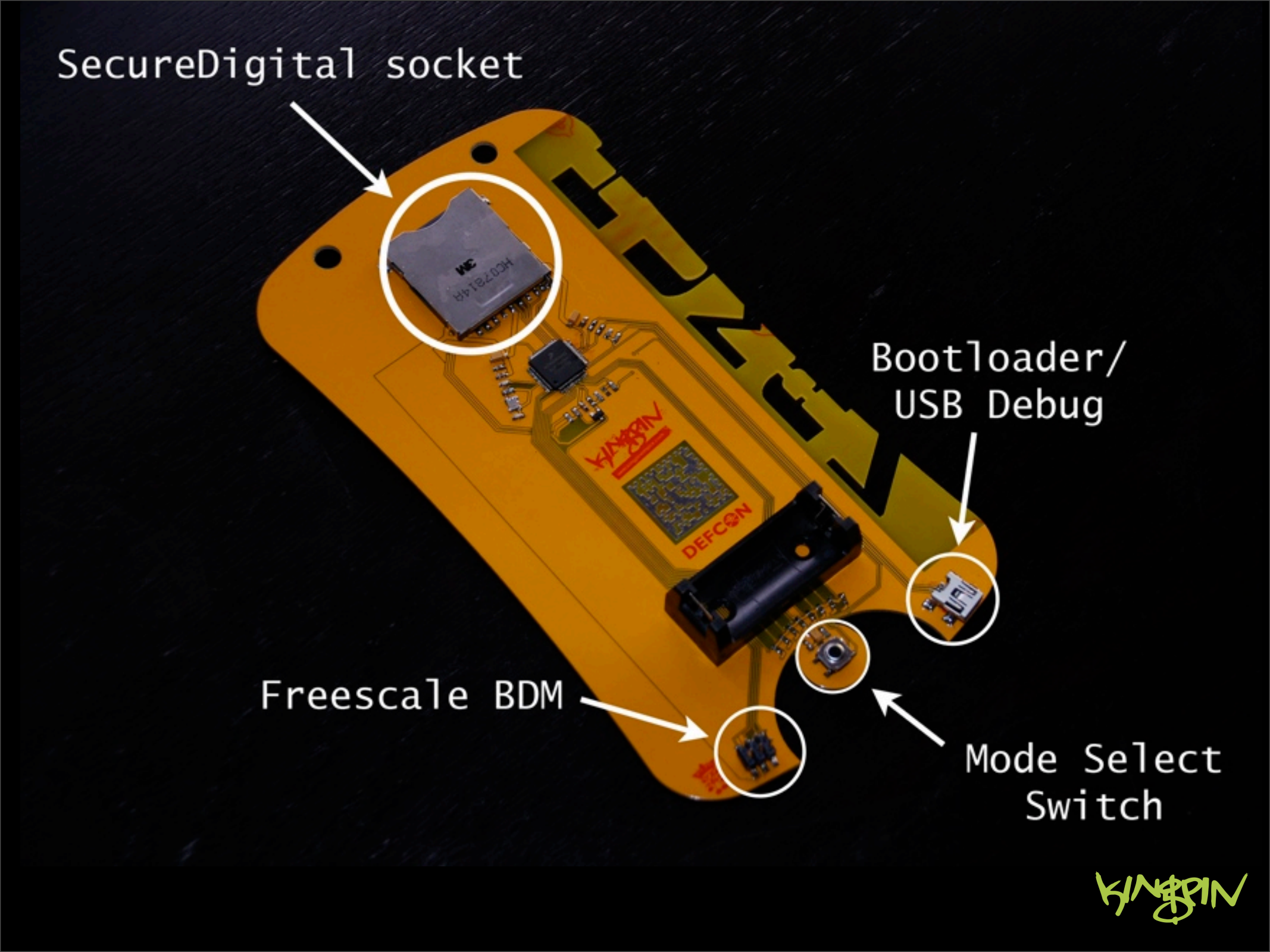
DEFCON 16 BADGE SYSTEM BLOCK DIAGRAM 4.14.08

HERE WE GO AGAIN !

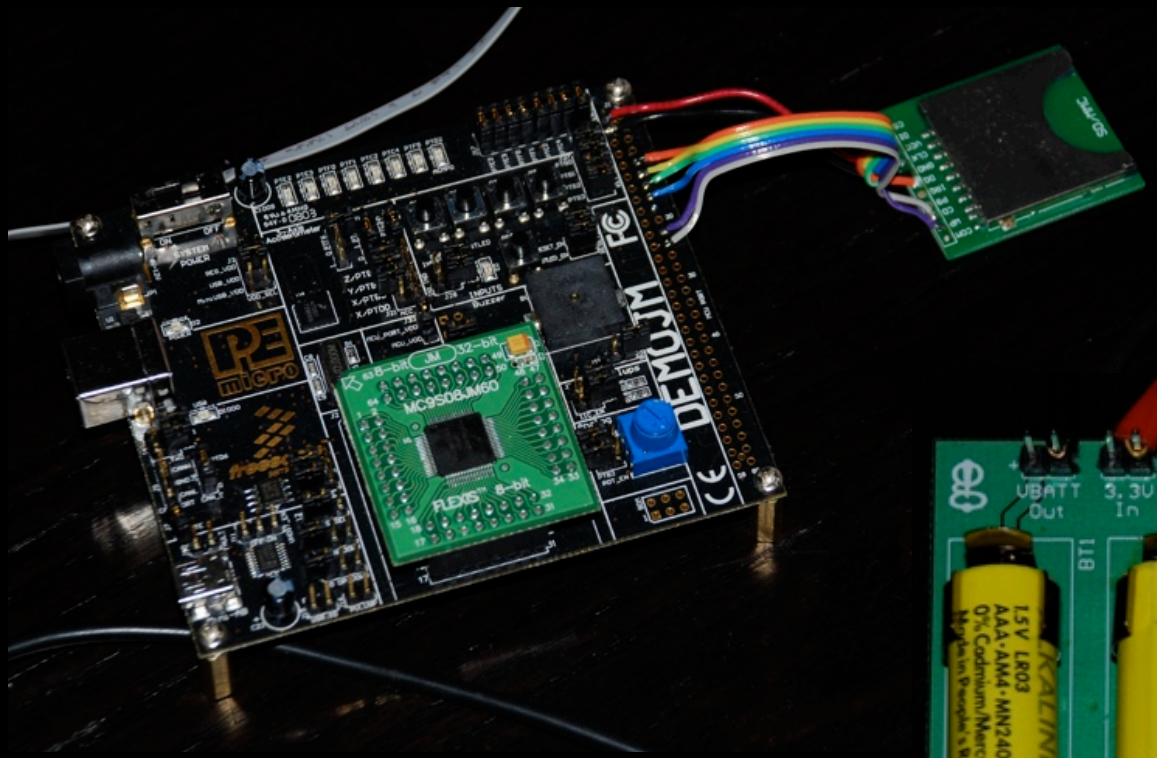


KINGPIN

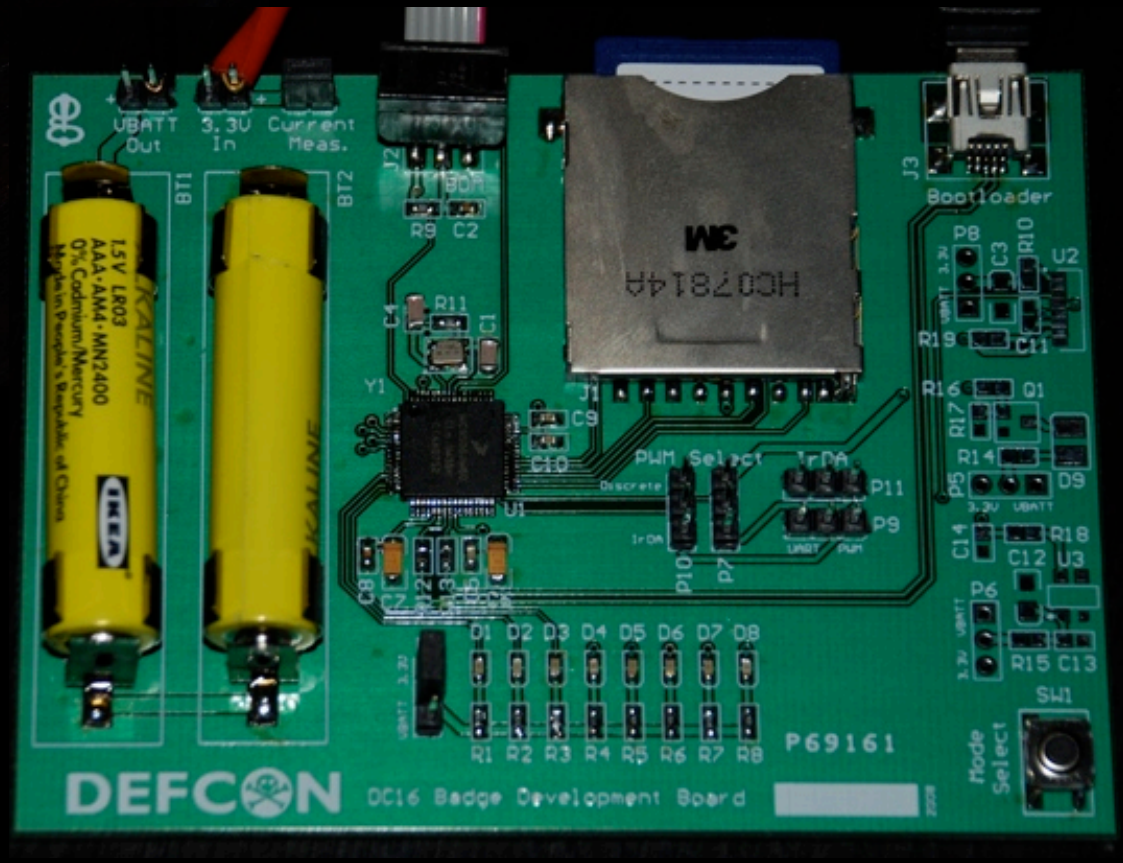

IR Transmitter
DEF CON
IR Receiver
LEDs
KINGPIN


SecureDigital socket
Bootloader/
USB Debug
Freescale BDM
Mode Select
Switch
DEFCON

Development hardware iterations

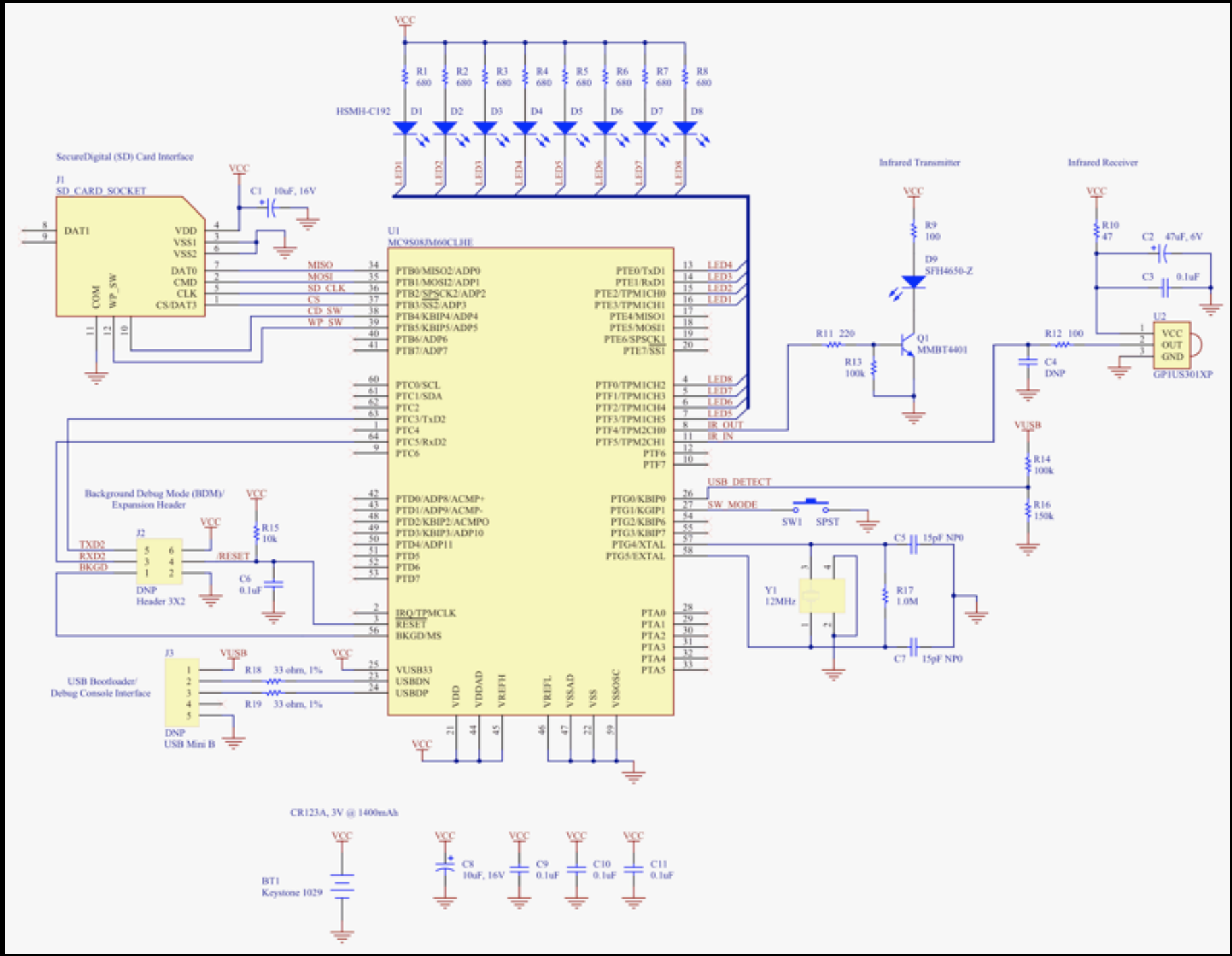


1. Freescale DEMOJM w/ MC9S08JM60 module



2. Custom development board to test & verify H/W

KINGPIN


VCC
R1 680
R2 680
R3 680
R4 680
R5 680
R6 680
R7 680
R8 680
HSMH-C192
D1
D2
D3
D4
D5
D6
D7
D8
LED1
LED2
LED3
LED4
LED5
LED6
LED7
LED8
SecureDigital (SD) Card Interface
J1
SD_CARD_SOCKET
DAT1
VDD
VSS1
VSS2
DAT0
CMD
CLK
CS/DAT3
COM
WP_SW
C1 10uF, 16V
MISO
MOSI
SD_CLK
CS
CD_SW
WP_SW
U1
MC9S08JM60CLHE
PTB0/MISO2/ADP0
PTB1/MOSI2/ADP1
PTB2/SPSCK2/ADP2
PTB3/SS2/ADP3
PTB4/KBIP4/ADP4
PTB5/KBIP5/ADP5
PTB6/ADP6
PTB7/ADP7
PTC0/SCL
PTC1/SDA
PTC2
PTC3/TxD2
PTC4
PTC5/RxD2
PTC6
PTD0/ADP8/ACMP+
PTD1/ADP9/ACMP-
PTD2/KBIP2/ACMPO
PTD3/KBIP3/ADP10
PTD4/ADP11
PTD5
PTD6
PTD7
IRQ/TPMCLK
RESET
BKGD/MS
VUSB33
USBDN
USBDP
VDD
VDDAD
VREFH
VREFL
VSSAD
VSS
VSSOSC
PTE0/TxD1
PTE1/RxD1
PTE2/TPM1CH0
PTE3/TPM1CH1
PTE4/MISO1
PTE5/MOSI1
PTE6/SPSCK1
PTE7/SS1
PTF0/TPM1CH2
PTF1/TPM1CH3
PTF2/TPM1CH4
PTF3/TPM1CH5
PTF4/TPM2CH0
PTF5/TPM2CH1
PTF6
PTF7
PTG0/KBIP0
PTG1/KGIP1
PTG2/KBIP6
PTG3/KBIP7
PTG4/XTAL
PTG5/EXTAL
PTA0
PTA1
PTA2
PTA3
PTA4
PTA5
Infrared Transmitter
R9 100
D9 SFH4650-Z
R11 220
Q1 MMBT4401
R13 100k
Infrared Receiver
R10 47
C2 47uF, 6V
C3 0.1uF
U2
VCC
OUT
GND
GP1US301XP
R12 100
C4 DNP
VUSB
R14 100k
R16 150k
USB_DETECT
SW_MODE
SW1 SPST
C5 15pF NP0
C7 15pF NP0
Y1 12MHz
R17 1.0M
Background Debug Mode (BDM)/ Expansion Header
J2
TXD2
RXD2
BKGD
/RESET
R15 10k
C6 0.1uF
DNP
Header 3X2
J3
USB Bootloader/ Debug Console Interface
R18 33 ohm, 1%
R19 33 ohm, 1%
DNP
USB Mini B
CR123A, 3V @ 1400mAh
BT1
Keystone 1029
C8 10uF, 16V
C9 0.1uF
C10 0.1uF
C11 0.1uF

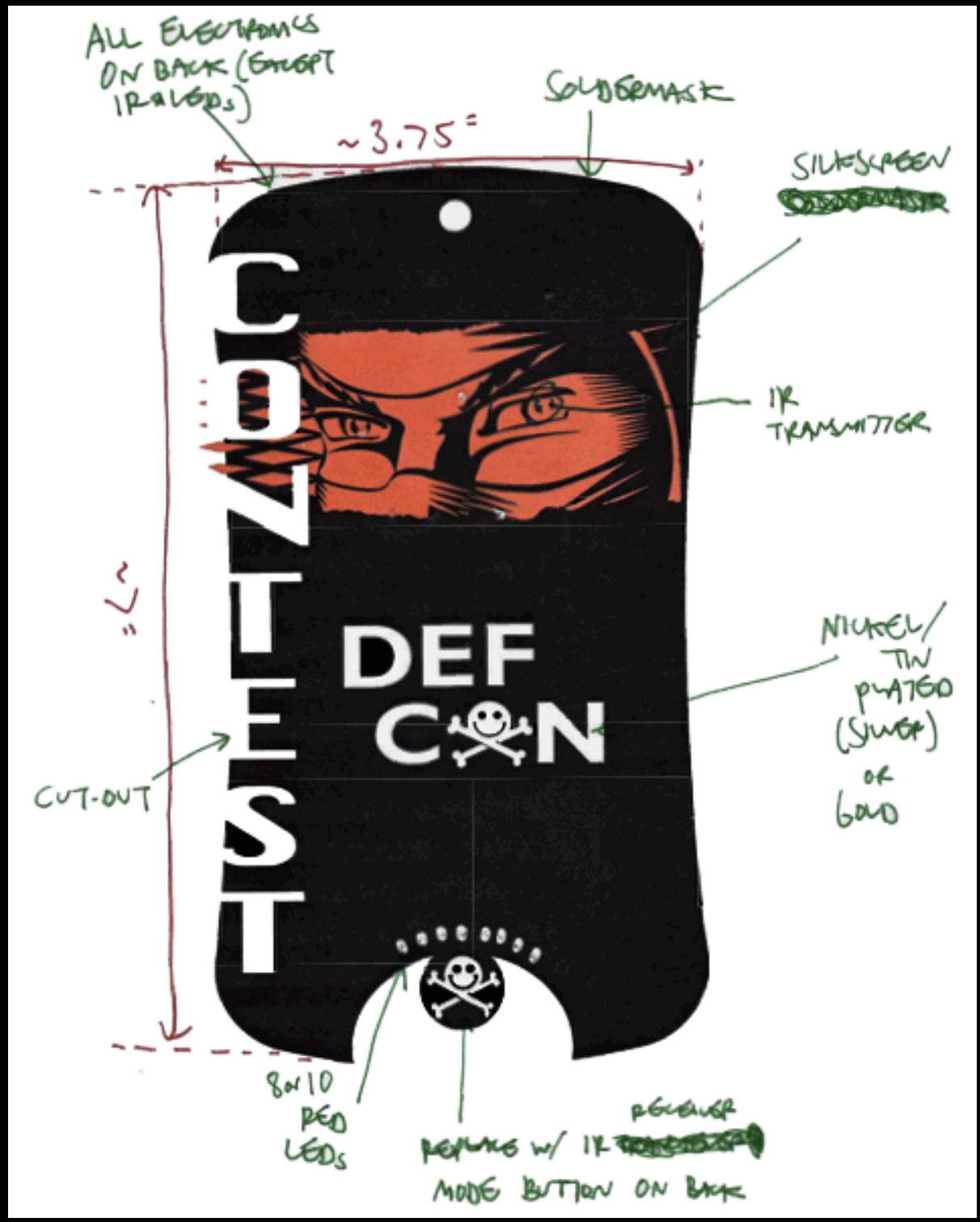
Schematic

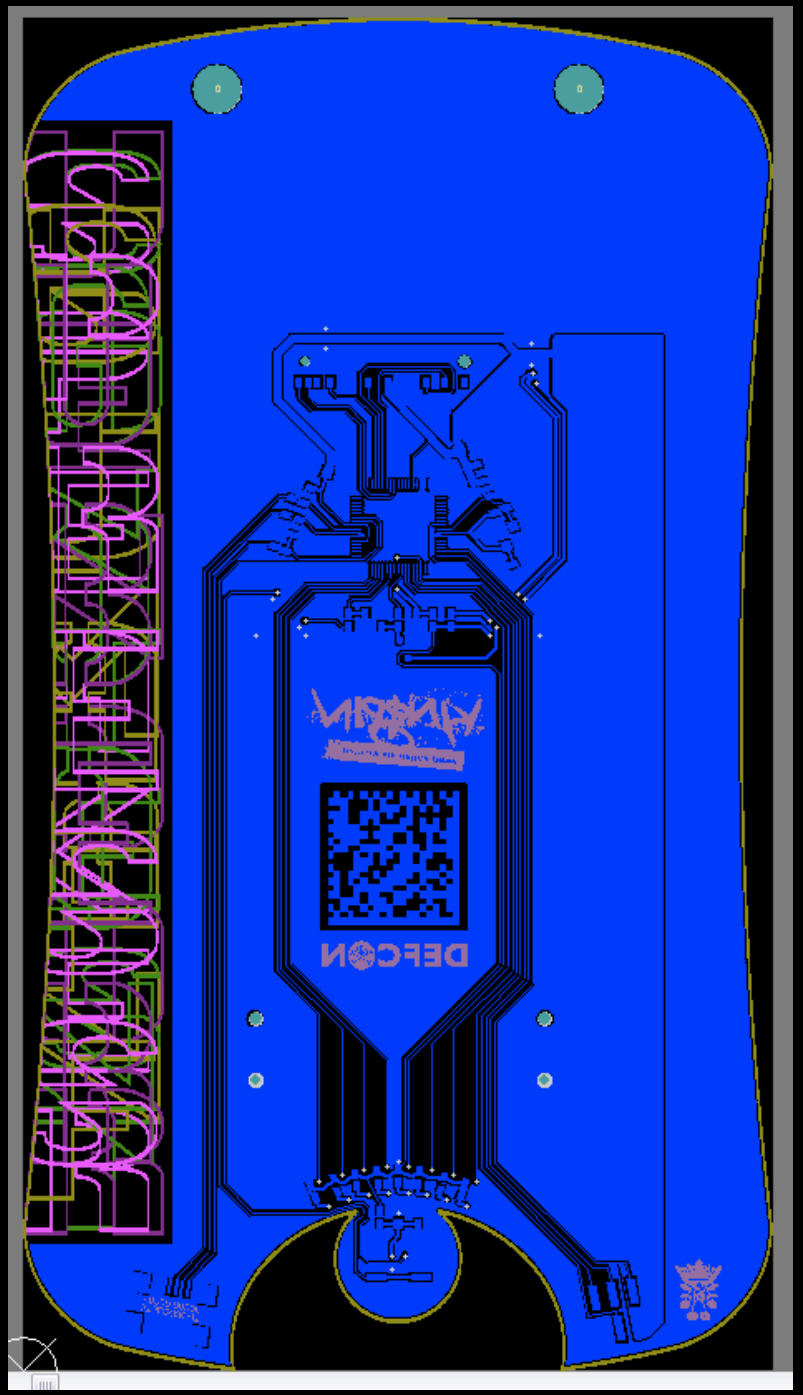
Bill-of-Materials

DEFCON 16 Circuit Board Badge
Bill-of-Materials
Document Version 2.0, June 14, 2008

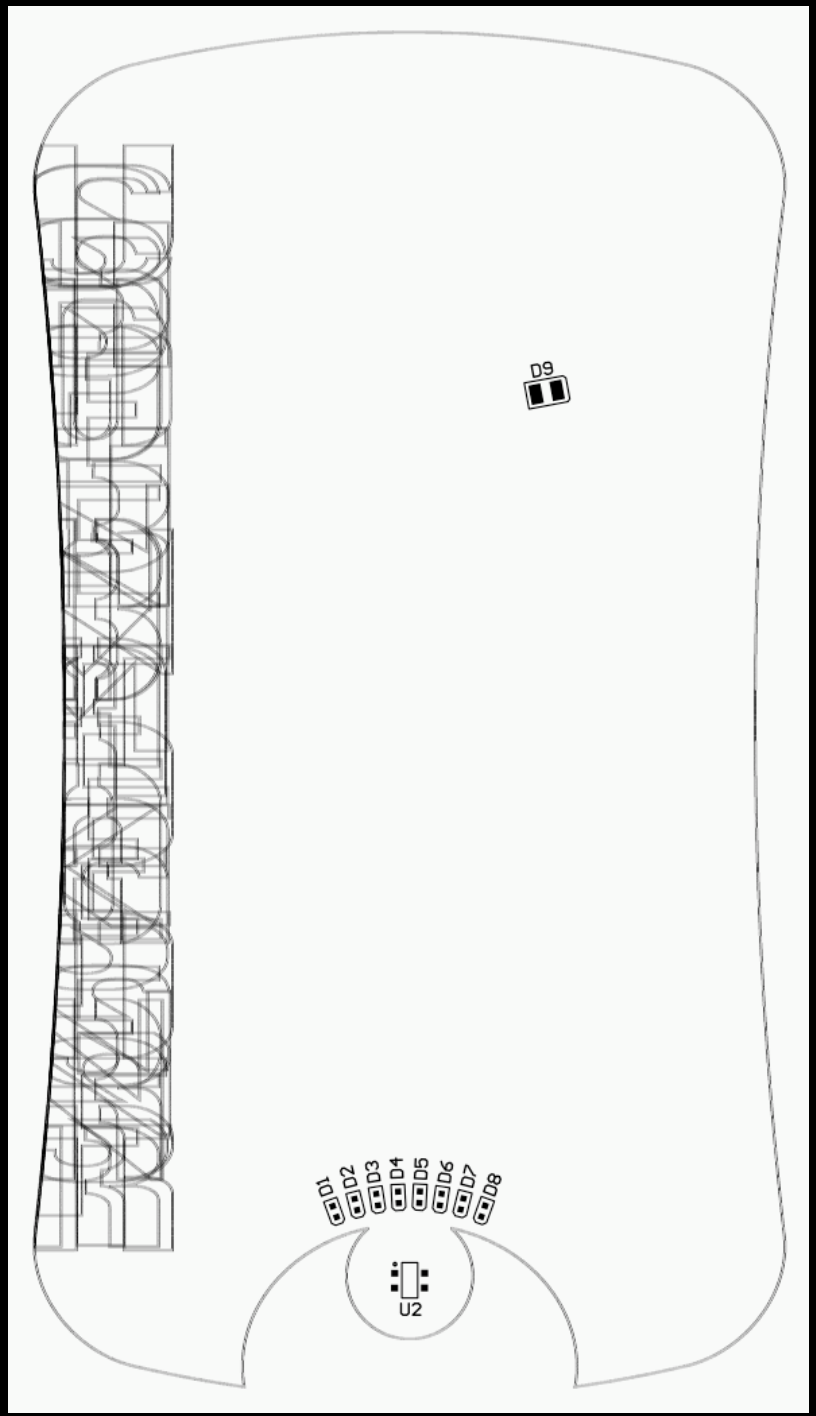
Note: Do Not Populate C4, J2, J3

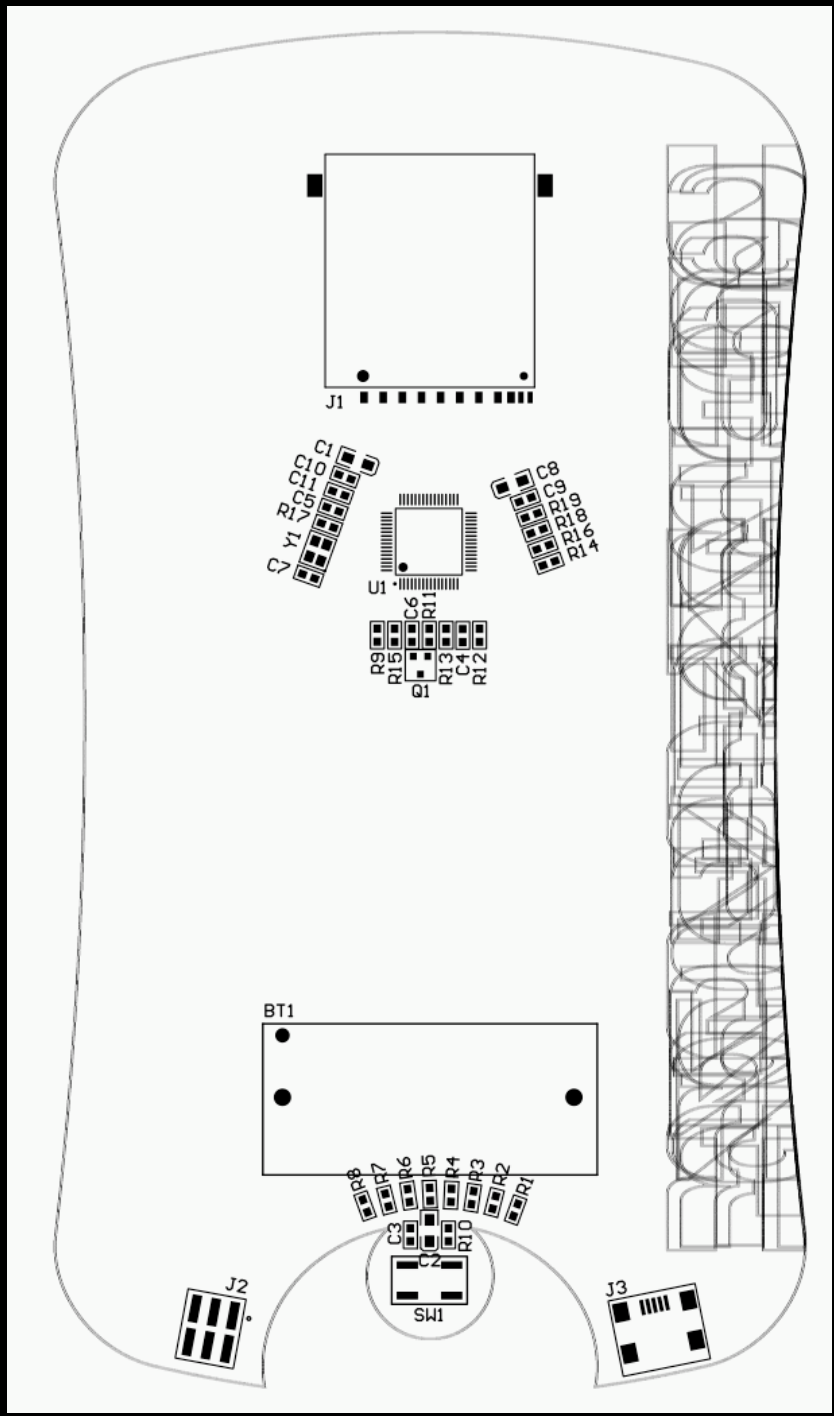
Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	1	BT1	Keystone	1029	Digi-Key	1029K-ND	Battery holder for CR/123A
2	2	C1,C8	Kemet	T491A106M016AT	Mouser	80-T491A106M016	10uF tantalum capacitor, 16V, 20%, size A
3	1	C2	Kemet	T491A476M006AT	Mouser	80-T491A476M06	47uF tantalum capacitor, 6.3V, 20%, size A
4	5	C3,C6,C9,C10,C11	Kemet	C0603C104K4RACTU	Digi-Key	399-1096-2-ND	0.1uF bypass capacitor, 16V, X7R, 0603
5	2	C5,C7	Kemet	C0603C150J5GACTU	Digi-Key	399-1051-2-ND	15pF ceramic capacitor, NP0, 50V, 0603
6	8	D1-D8	Avago	HSMH-C192	FAI	HSMH-C192	LED, Red, 0603, 1.8Vf, 17mcd @ 20mA (leftover from DC15)
7	1	D9	Osram	SFH4650-Z	Digi-Key	475-2569-2-ND	LED, Infrared, 850nm, +/-20 degree angle, 16mW @ 100mA, SMD
8	1	J1	3M	SD-RSMT-2-MQ-WF	Digi-Key	3M5646TR-ND	SecureDigital memory socket/connector, push-push, R/A, SMD
9	1	Q1	Fairchild	MMBT4401	Digi-Key	MMBT4401FSTR-ND	Transistor, general purpose, NPN, 40V, 600mA, SOT23-3
10	8	R1-R8	Rohm	MCR03EZPJ681	Digi-Key	RHM680GTR-ND	680 ohm, 5%, 1/10W, 0603
11	2	R9,R12	Panasonic	ERJ-3GEYJ101V	Digi-Key	P100GTR-ND	100 ohm, 5%, 1/10W, 0603
12	1	R10	Panasonic	ERJ-3GEYJ470V	Digi-Key	P47GTR-ND	47 ohm, 5%, 1/10W, 0603
13	1	R11	Rohm	MCR03EZPJ221	Digi-Key	RHM220GTR-ND	220 ohm, 5%, 1/10W, 0603
14	2	R13,R14	Rohm	MCR03EZPJ104	Digi-Key	RHM100KGTR-ND	100k, 5%, 1/10W, 0603
15	1	R15	Panasonic	ERJ-3GEYJ103V	Digi-Key	P10KGTR-ND	10k, 5%, 1/10W, 0603
16	1	R16	Panasonic	ERJ-3GEYJ154V	Digi-Key	P150KGTR-ND	150k, 5%, 1/10W, 0603
17	1	R17	Panasonic	ERJ-3GEYJ105V	Digi-Key	P1.0MGTR-ND	1.0M, 5%, 1/10W, 0603
18	2	R18,R19	Yageo	RC0603FR-0733RL	Digi-Key	311-33.0HRTR-ND	33 ohm, 1%, 1/10W, 0603
19	1	SW1	C&K	KSC341JLFS	Digi-Key	401-1770-2-ND	SPST tactile momentary switch, 300gf, 6.2mm x 6.2mm, SMD
20	1	U1	Freescale	MC9S08JM60CLH	FAI	MC9S08JM60CLH	Microcontroller, LQFP64
21	1	U2	Sharp	GP1US301XP	Digi-Key	425-2527-2-ND	Receiver Module, Infrared (IR), 38kHz, 2.4V-5.5V, SMD
22	1	Y1	NDK	NX3225SA-12.000000MHZ	Digi-Key	644-1047-2-ND	Crystal, 12MHz, 8pF, SMD
23	1	PCB	e-Teknet	DC16 1.0	N/A	N/A	PCB (includes assembly and testing)


ALL ELECTRONICS ON BACK (EXCEPT IR & LEDs)
~3.75"
SOLDERMASK
SILKSCREEN
IR TRANSMITTER
~4"
NICKEL/TIN PLATED (SILVER) OR GOLD
CUT-OUT
8 or 10 RED LEDs
REPLACE W/ IR
MODE BUTTON ON BACK
COOLEST
DEF CON



Final PCB layout...

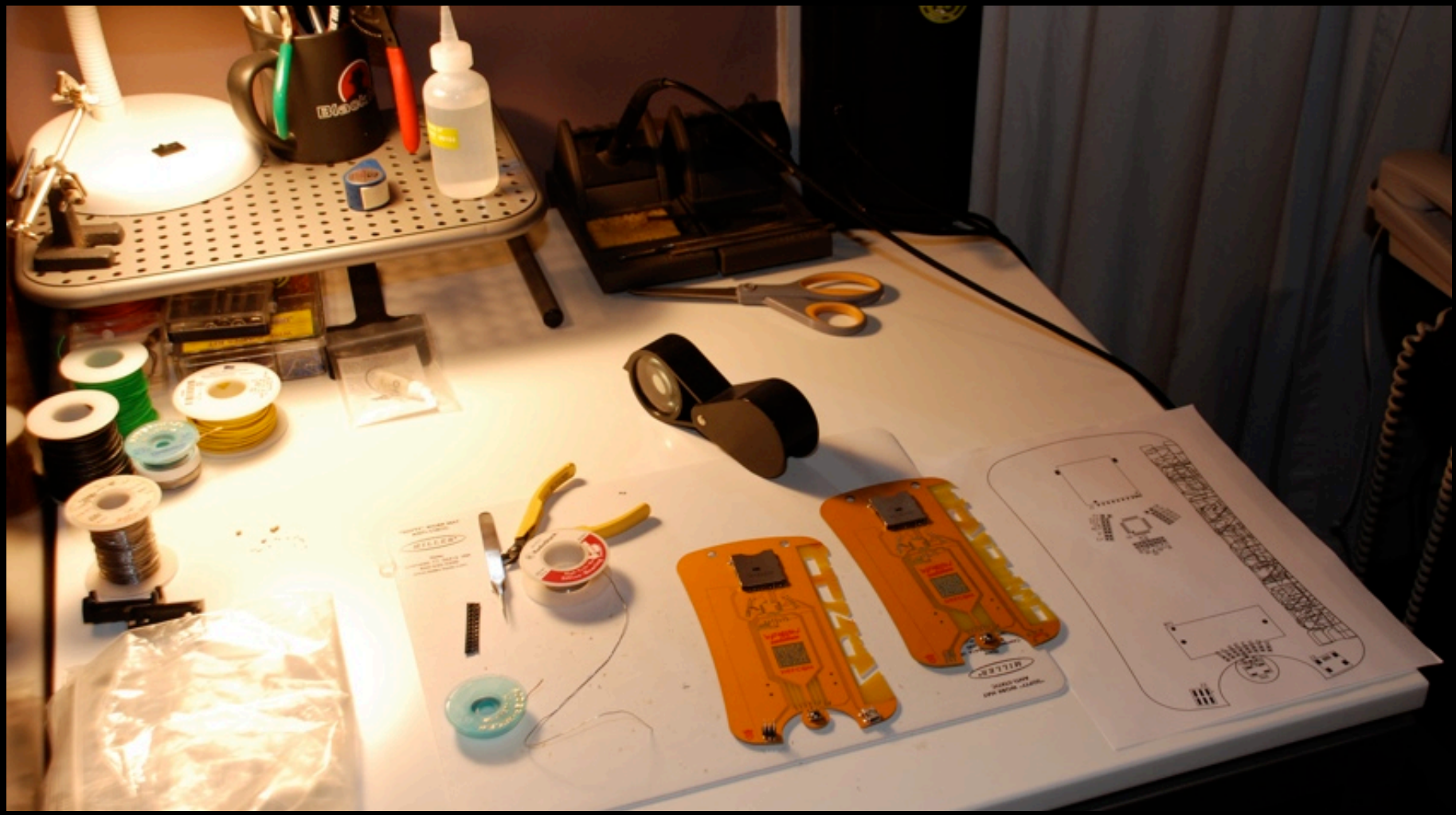




Assembly drawings...

The first set of prototypes arrive (mid-June)...

Prototype testing and verification... No problems!



DC16 BADGE TO-DO

5/17/08

HW

- ~~clean latch-up, power on reset ride (might go away w/ boost regulator)~~
- ~~select IR mesh~~
- ~~select LED current limiting resistors~~
- ~~select battery boost circuitry~~
- ~~other renaming parts~~ [redacted]
- ~~make prototype "fine to fab" PCB~~

PCB

- ~~final PCB design~~
- ~~Add easter eggs~~
  - ~~kp logo~~
  - ~~2D barcode~~
- ~~Decoupling caps/inductors direct to component, not to power/gnd plane~~
- ~~UPDATE BOTTOM PASTE LAYER (LED only)~~
- ~~UPDATE #DEFINES w/ PCB pin-out~~
- ~~USB descriptor (cdc1_usb_config.c)~~ [redacted]

FIRMWARE

- ~~Tune DELAY_MS function~~ [redacted]
- ~~Configure device & disable unused modules~~
- ~~RX IR mode~~
- ~~Ensure bootloader/entry code is protected~~
- ~~Finish LED animations~~
- ~~Sleep mode~~
- ~~Serial port debug output/USB selection~~
- ~~SD card read/write file~~
  - ~~SPI timing for 8MHz/48MHz~~
- ~~IR communications~~
- ~~SPI routines (send byte & receive byte) Sometimes hang~~ [redacted]
- ~~pwm setup, 38kHz 30%~~
- ~~Decode control bit?~~
- ~~Tx file~~
- ~~Rx file~~
- ~~Increment/decrement display to show progress~~

KINGPIN

Battery selection

AAA v. CR123A battery

- ★ Battery life (must last > DEFCON, unlike last year)
- ★ Weight
- ★ Cost
- ★ Availability
- ★ Required External Components

Current measurements @ 3.3V

SYSTEM LEVEL

NO USB (12MHz clock)

SLEEP = 0.790 mA (varies slightly if SD card is inserted)

KNIGHT RIDER LED = 5.3 mA

IR TX (continuous @ 38kHz) = 9.1 mA

SD CARD (READ/WRITE continuous) = 20 mA DANE-ELEC 1GB
35 mA PANASONIC 16MB (old)

WITH USB (48MHz clock)

SLEEP (fully WAIT) = 20.4 mA

KNIGHT RIDER LED = 24.7 mA

IR TX (continuous @ 38kHz) = 27.7 mA

SD CARD (READ/WRITE continuous) = 45 mA DANE-ELEC 1GB
60 mA PANASONIC 16MB (old)

Current consumption of SD card is unreliable & unpredictable

KINGPIN

Current measurements @ 3.3V

INDIVIDUAL COMPONENTS

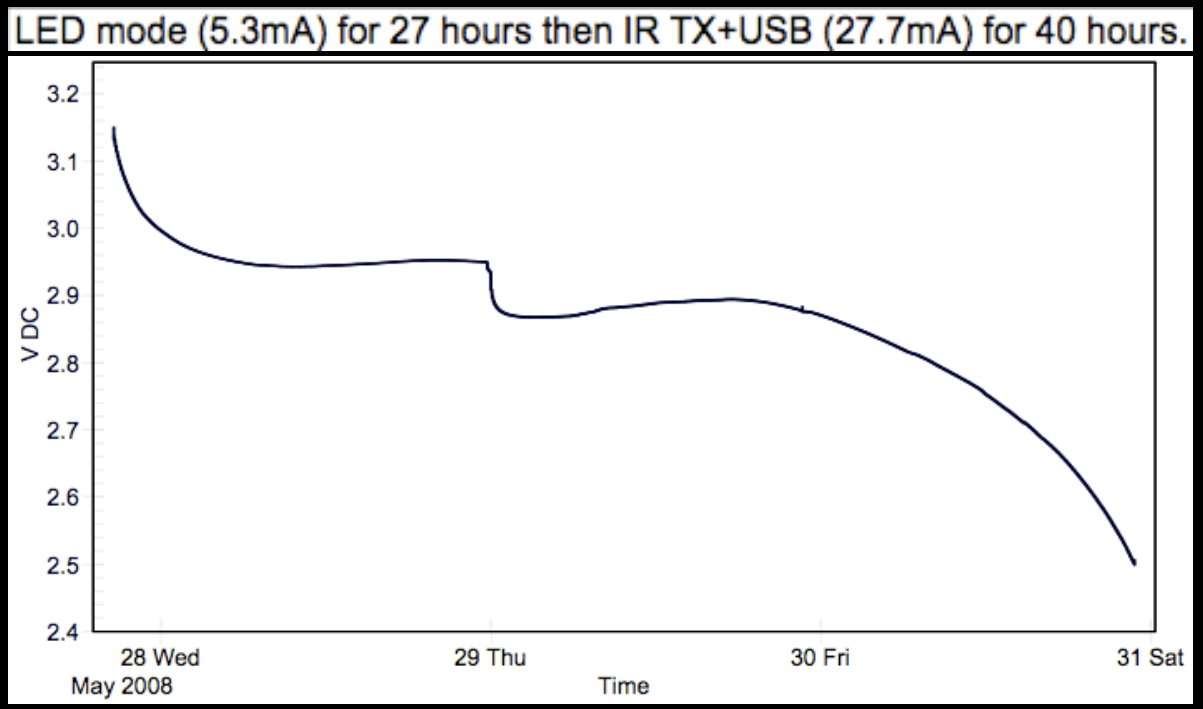
IR RECEIVER, GP1US30XP, IDLE: 0.440mA

ACTIVE (RECEIVING RC DATA) = 0.560mA

IR TRANSMITTER, SFH4650, ACTIVE (CONTINUOUS @ 38kHz, 30% D/C) = 1.3mA

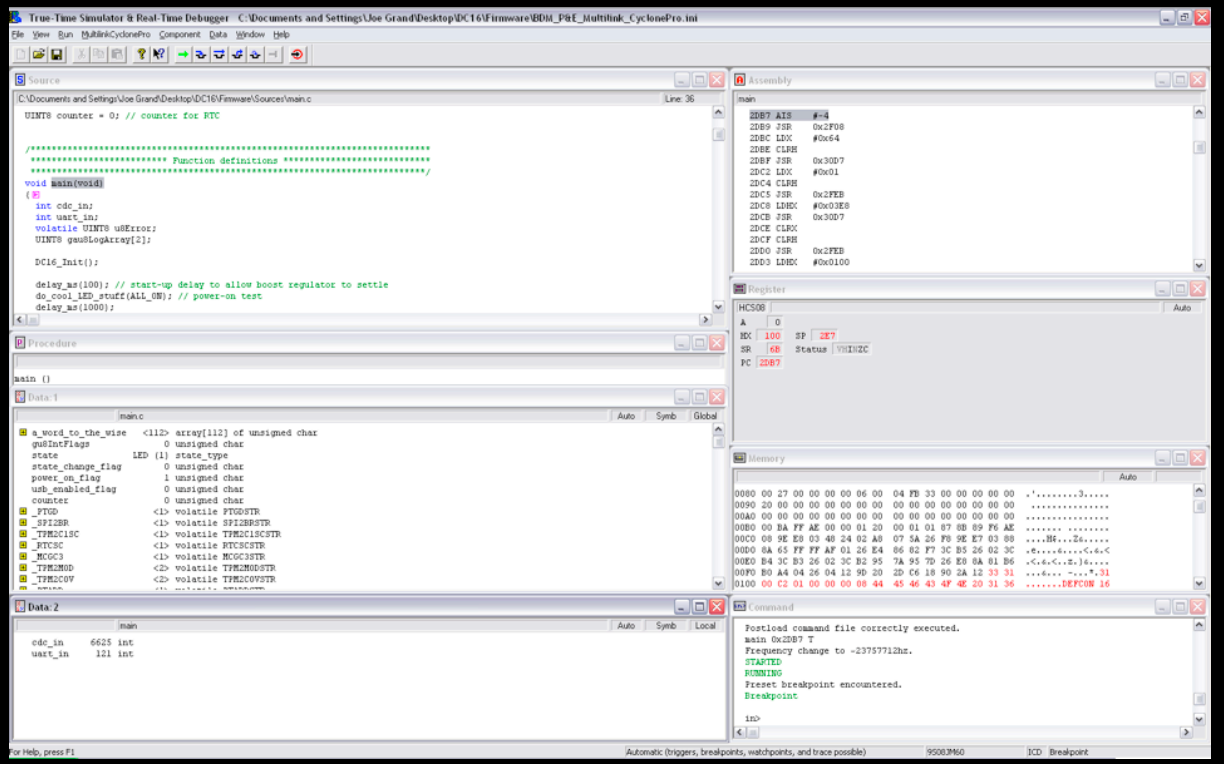
LEDs, KNIGHT RIDER = 4.4mA

ALL ON = 16.6mA



Development Environment

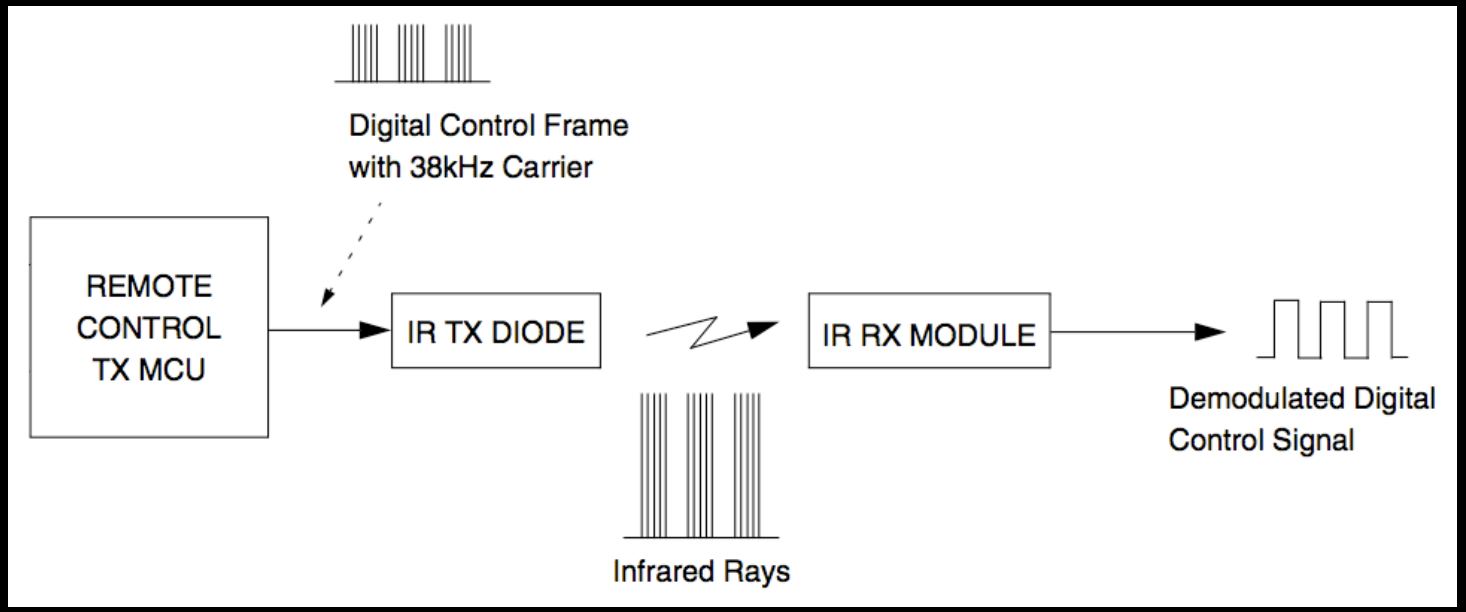
Freescale CodeWarrior 6.1 for MCUs

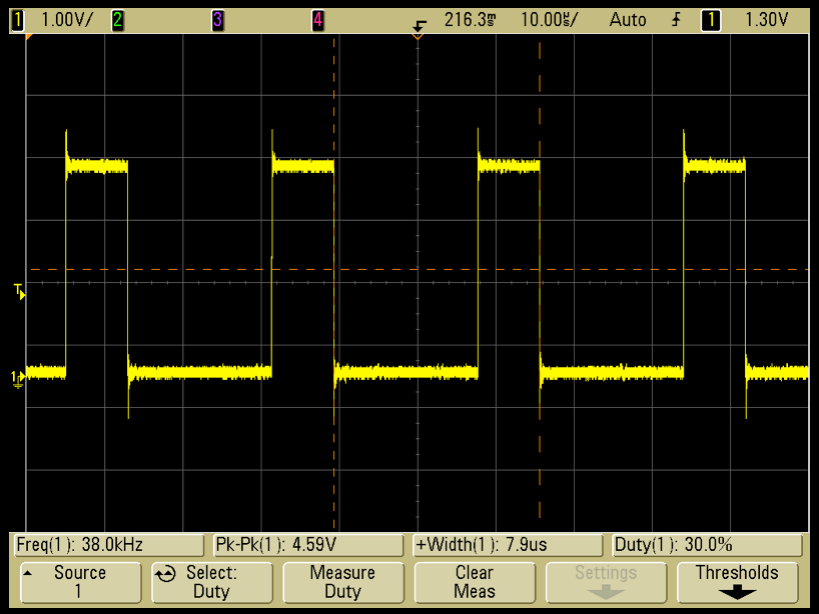


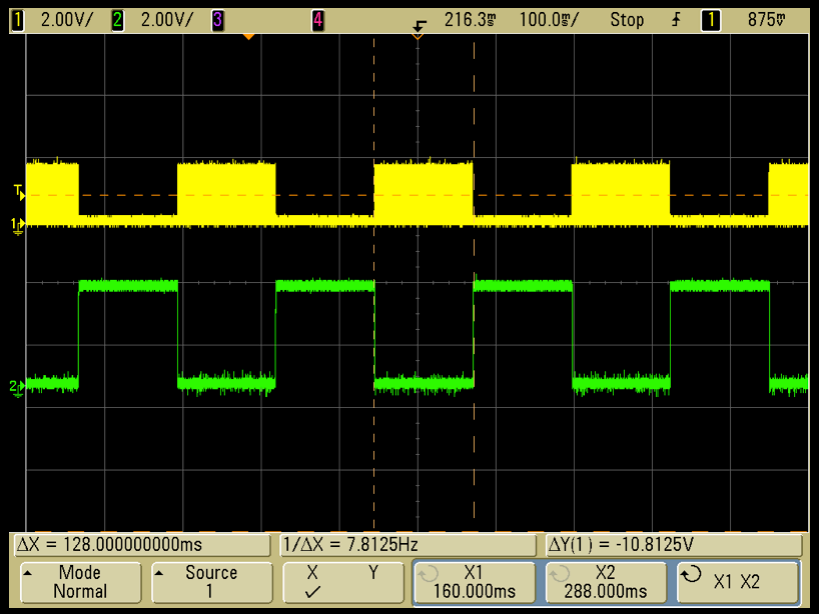
- ★ DEFCON CD: Professional Edition ($1995!) courtesy of Freescale for badge hacking, supports full 60KB of Flash, valid thru 8/20/08
- ★ Internets: Freeware version, 32KB maximum code space, `www.freescale.com/webapp/sps/site/homepage.jsp?nodeId=012726`

KINGPIN

Infrared







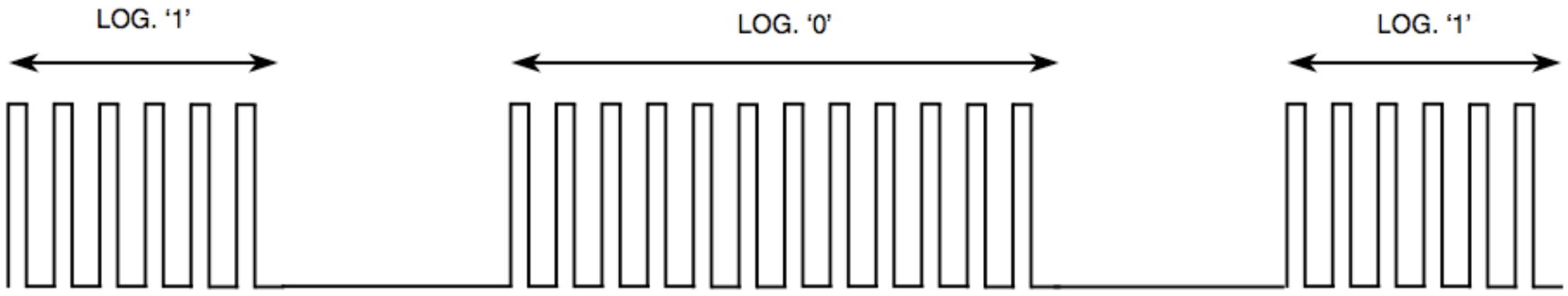
38kHz carrier @ 33% duty cycle
(generated via TPM2CH0 PWM)

IR on/off keying (OOK)
Top: IR TX
Bottom: IR RX

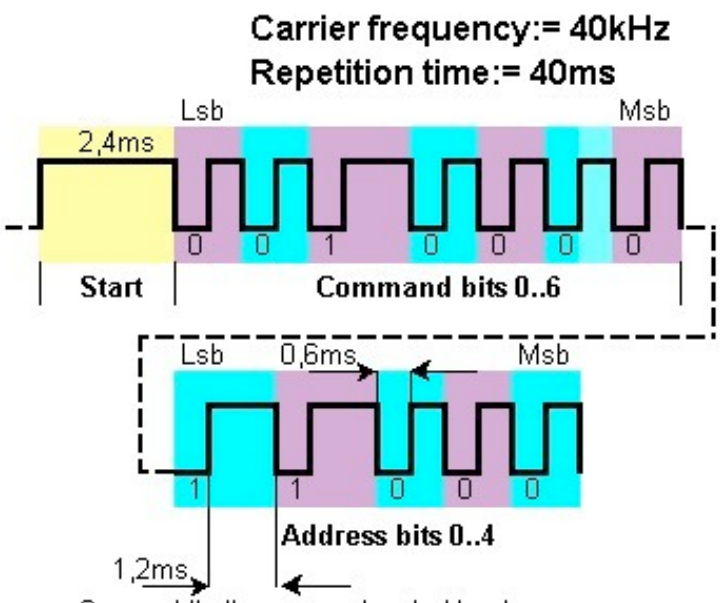
Infrared 2

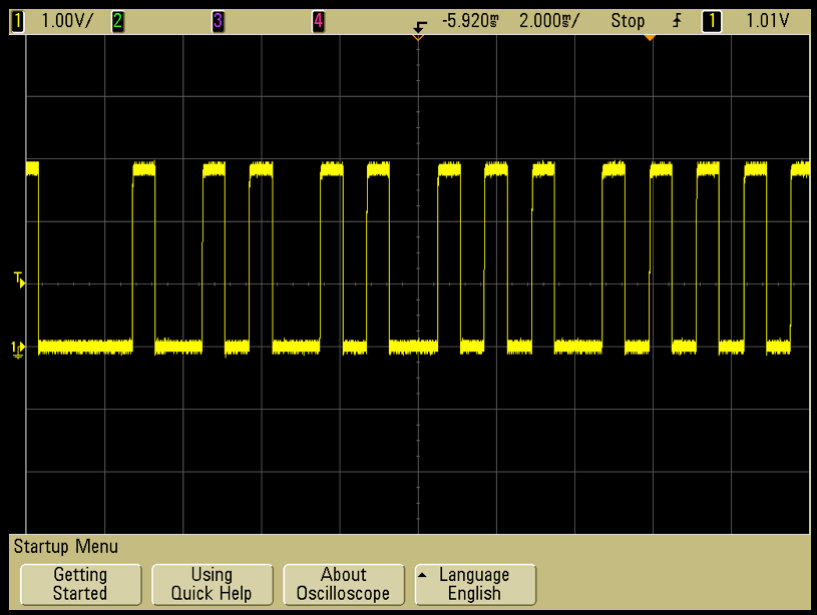
Pulse Width Encoding

The pulse width defines log. '1' or log. '0' respectively, the pulse distance is constant



Sony infrared remote protocol:



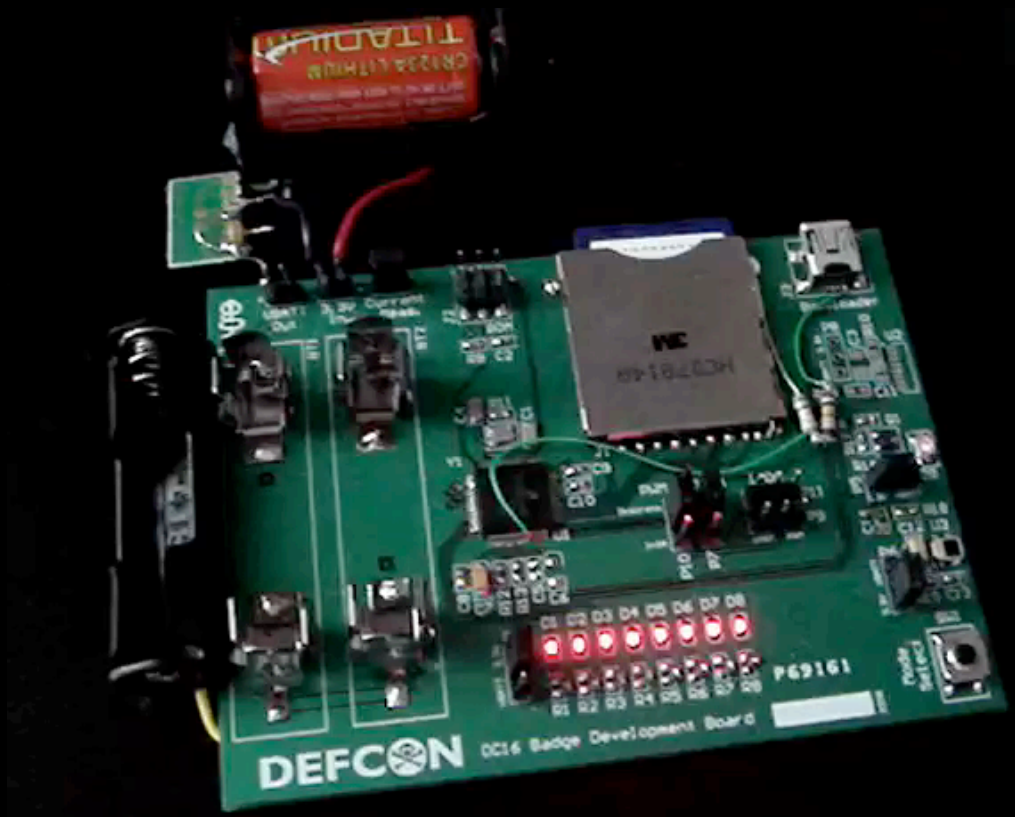


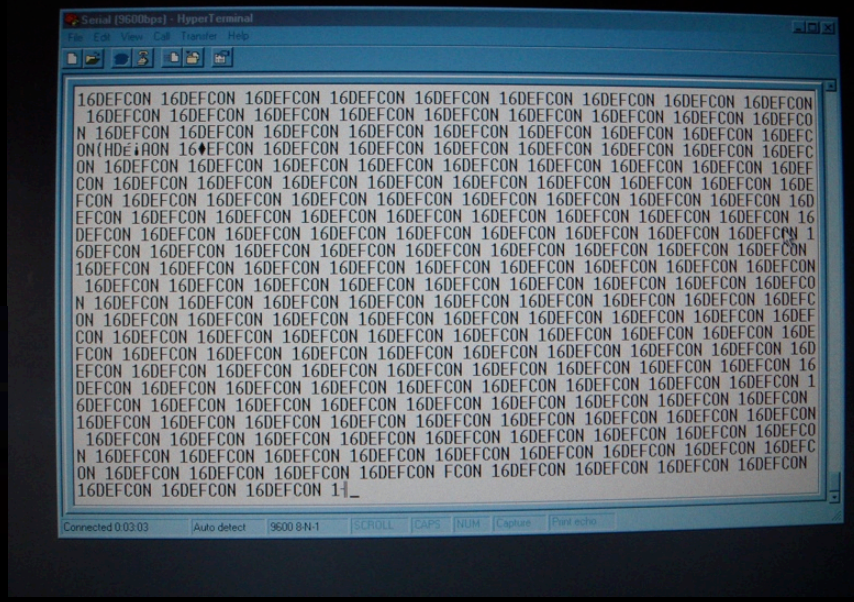
Sony TV power off

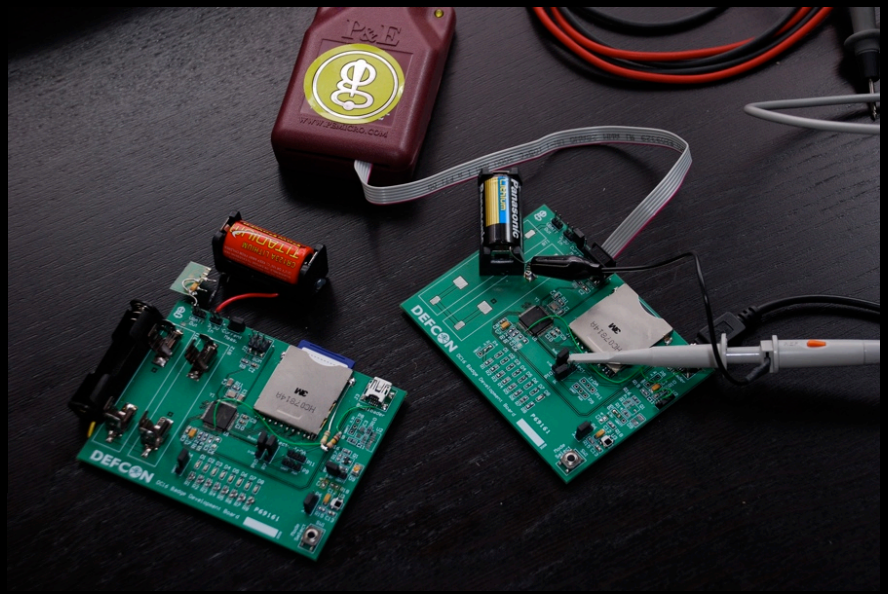
Infrared: TV-B-Gone

- ★ Mitch Altman, Cornfield Electronics, `www.tvbgone.com`
- ★ Also an open-source kit: `www.adafruit.com/index.php?main_page= index&cPath=20`
- ★ Simple device that cycles through all known TV power off codes (N. America/Asia)
- ★ All codes ported to DC16 Badge
- ★ TV-B-Gone mode enabled in TX Mode when no SD card is inserted in badge

Infrared: Data Transfer



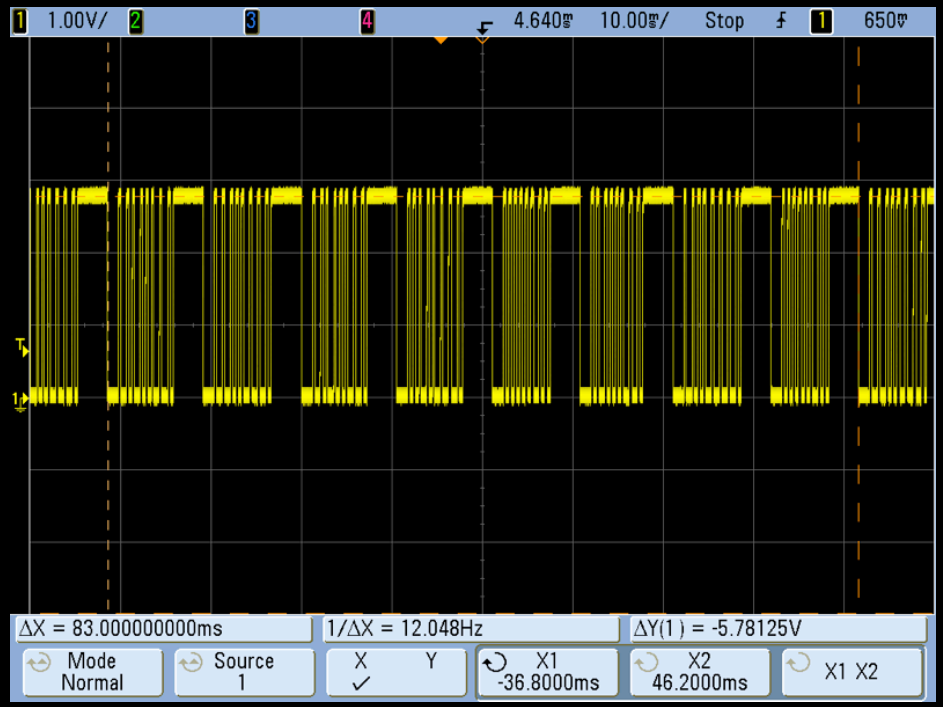




SecureDigital & FAT16

- ★ Based on *DEMOFLEXISJMSD_DataLogger* sample code
- ★ Card must be > 32MB (otherwise defaults to FAT12, which will not work properly)
- ★ Incrementing filenames to prevent duplicates

Infrared: File Transfer



IR file transfer, 8 bytes

8 bytes / 83 ms = 771 bits/sec.

- ★ Desired file to send must *only* have *read-only* flag set
- ★ CRC-16 sent every 512 bytes
- ★ Intentional 128KB file transfer size limit

USB Bootloader/Debug & Freescale BDM

- ★ USB Debug = *DC16Badge.inf* driver (USB HID CDC class)
- ★ USB Bootloader = Driver loaded on GUI install (*JM60 Bootloader GUI Installer 1.1*)
- ★ Freescale BDM (Background Debug Mode) = P&E Multilink or SPYDER08 (maybe?)
- ★ Automatic bus clock adjustment via USB_DETECT line
  - ◉ Normal system clock @ 12MHz
  - ◉ When USB enabled, clock @ 48MHz

USB connectors available at the Hardware Hacking Village

KINGPIN

Parts procurement

- ★ Tough to find 8500 quantity of anything
- ★ Decided to use Digi-Key for as many parts as possible
  - ◉ Huge amount of available stock
  - ◉ Can ship same day
  - ◉ Prices comparable or better than other distributors
  - ◉ Wanted to get as many parts in hand ASAP
- ★ Delays in China customs due to the Olympics was a big hurdle (some of our packages held for over 5 weeks!)
- ★ No matter how much you plan, there will always be a problem...

KINGPIN

Parts procurement 2

★ Lamer of the Year Award #1: 3M

- Before order, quoted 6 week leadtime for SD card sockets
- After order (May 20), leadtime upped to 8-10 weeks
- After promised ship date of July 16 passed, delivery date extended to August 8 (uhhhhh...)
- Spent a week on the phone laying down the law!
- Global Product Manager stepped in to clean up the mess
- All parts finally received 10 days before DEFCON

Parts procurement 3

★ Lamer of the Year Award #2: Source Electronics

- Selected for microprocessor programming via Future Electronics
- Missed 5-day turnaround due to yield problems ("bad" parts)
- Decided to not ship the 6,000+ good parts until fixing the other ones, thus holding up our production
- Balance of "fixed" parts sent to the wrong address
- All parts (short 45 pieces) finally received 10 days before DEFCON

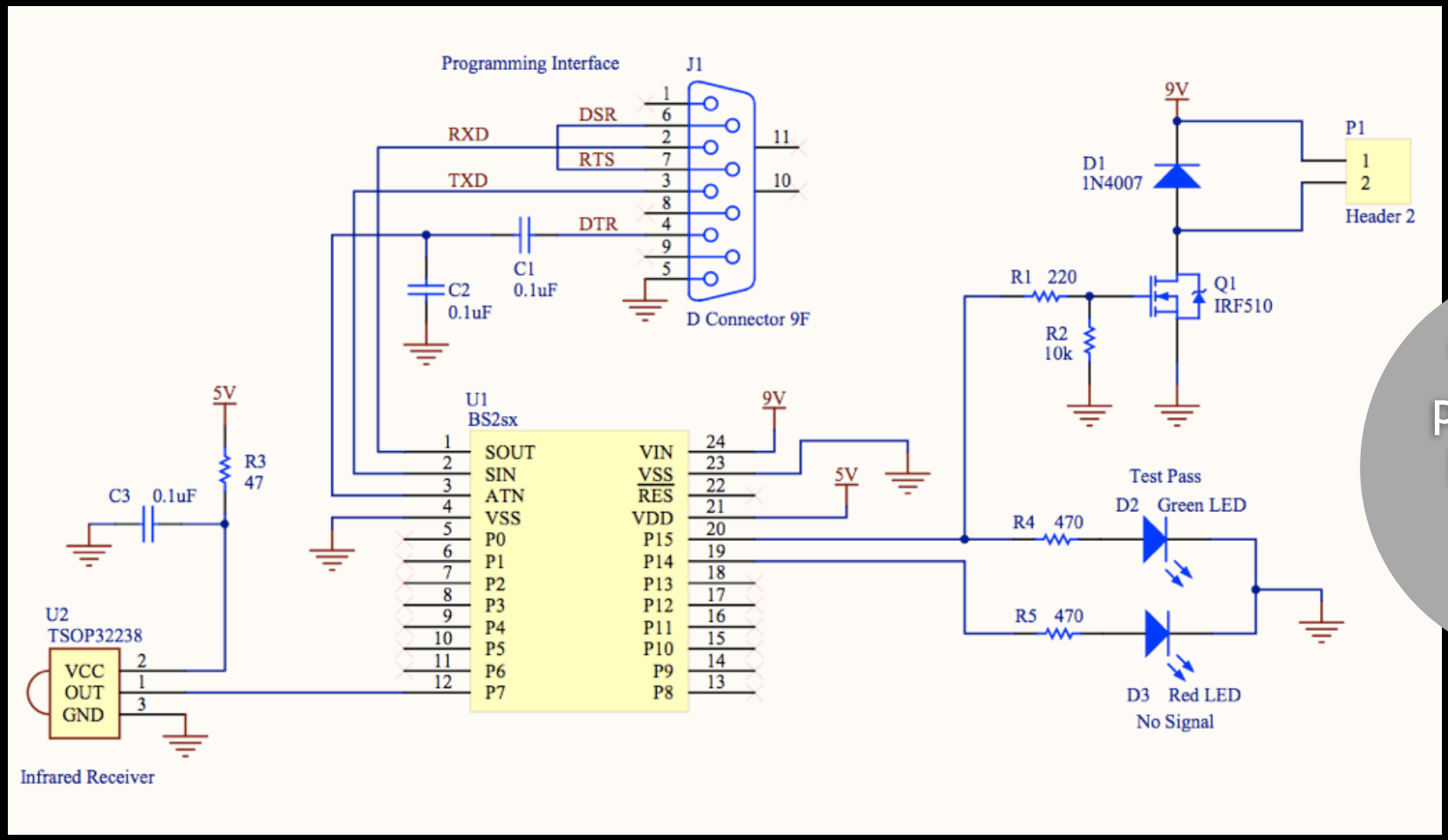
Parts procurement 4

★ Lamer of the Year Award #3: Chinese Customs

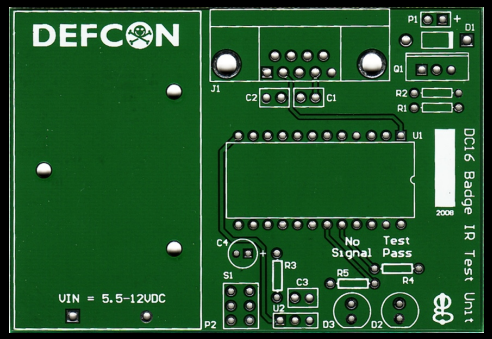
- Extremely tight inspection on import/export due to the Olympics
- One box in custody (2500pc. U2 & 4500pc. D9) since June 30
- On July 29 (10 days before DEFCON), tried to send another set of parts directly from Digi-Key. Held hostage for ~$1000 tax and 5-day delay. Still sitting there.
- On July 31, final attempt to get parts through customs. It worked! Last batch of parts delivered to e-Teknet on August 4 (Four days before DEFCON)
- In the meantime, scrambling around trying to find suitable parts in China, planning hand-assembly line using BH/DC goons, etc.

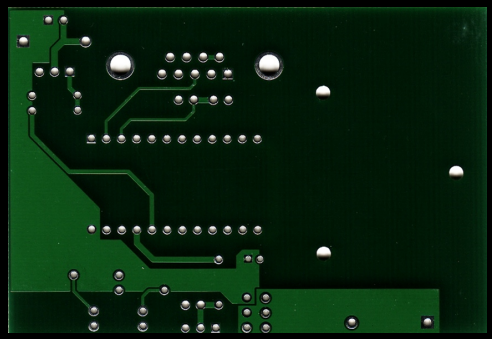
KINGPIN

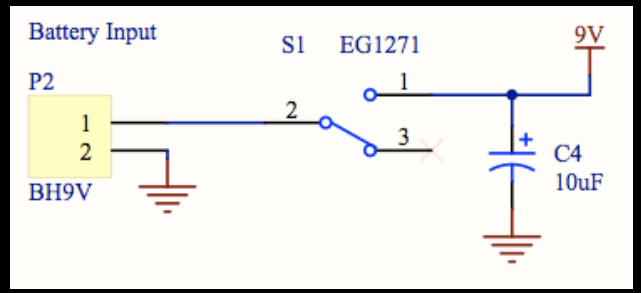
Test unit



Get these parts at the Hardware Hacking Village!

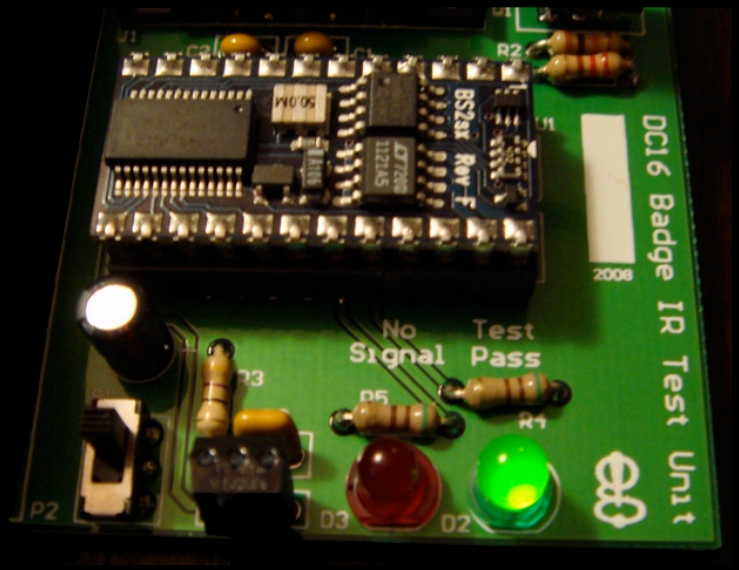


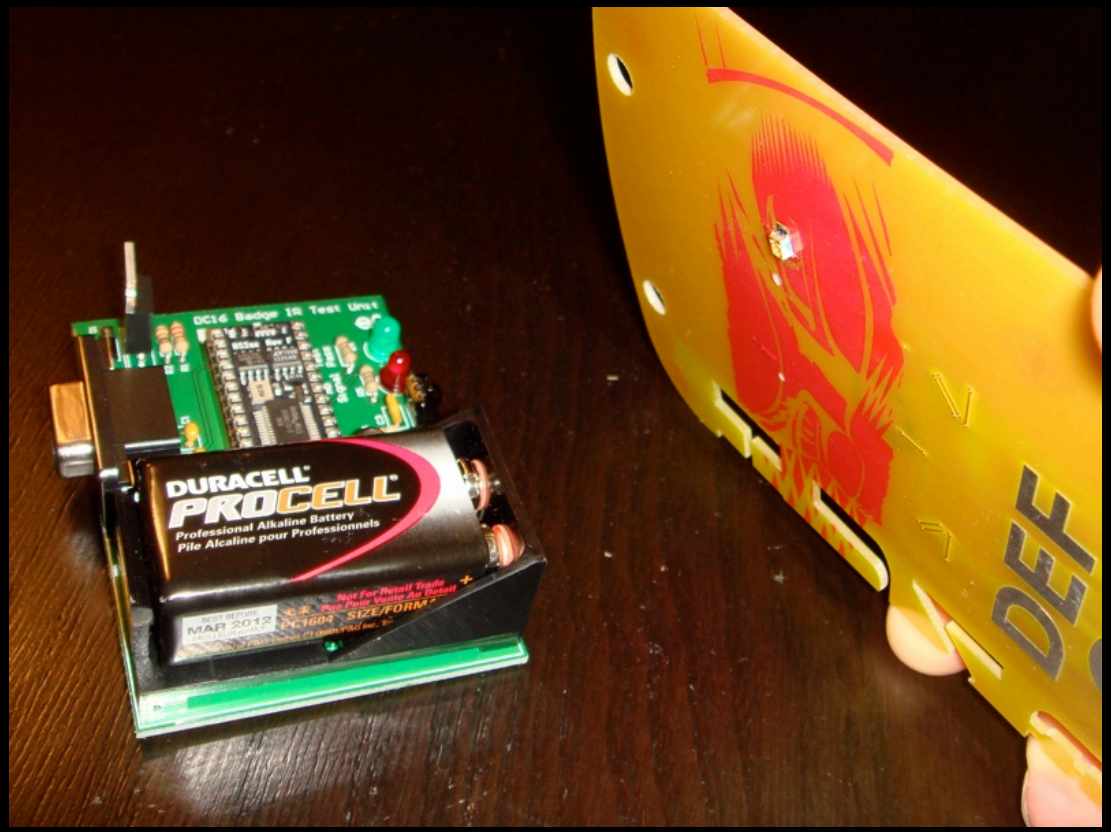




KINGPIN

Test procedure





*** Code on the DEFCON CD

KINGPIN

Total badge types

Have they all arrived yet? Almost!
Remaining badges coming for Friday & Saturday delivery!

```
Press = Green Soldermask / White Silkscreen = 150
Uber = Black Soldermask / Yellow Silkscreen = 100
Goon = Red Soldermask / White Silkscreen = 200
Staff = Red Soldermask / White Silkscreen = 150
Speaker = Blue Soldermask / White Silkscreen = 250
Vendor = Purple Soldermask / White Silkscreen = 100
Contest = Yellow Soldermask  / Red Silkscreen = 50
Human = White Soldermask / Red Silkscreen = 7500

Total: 8500 pieces
```

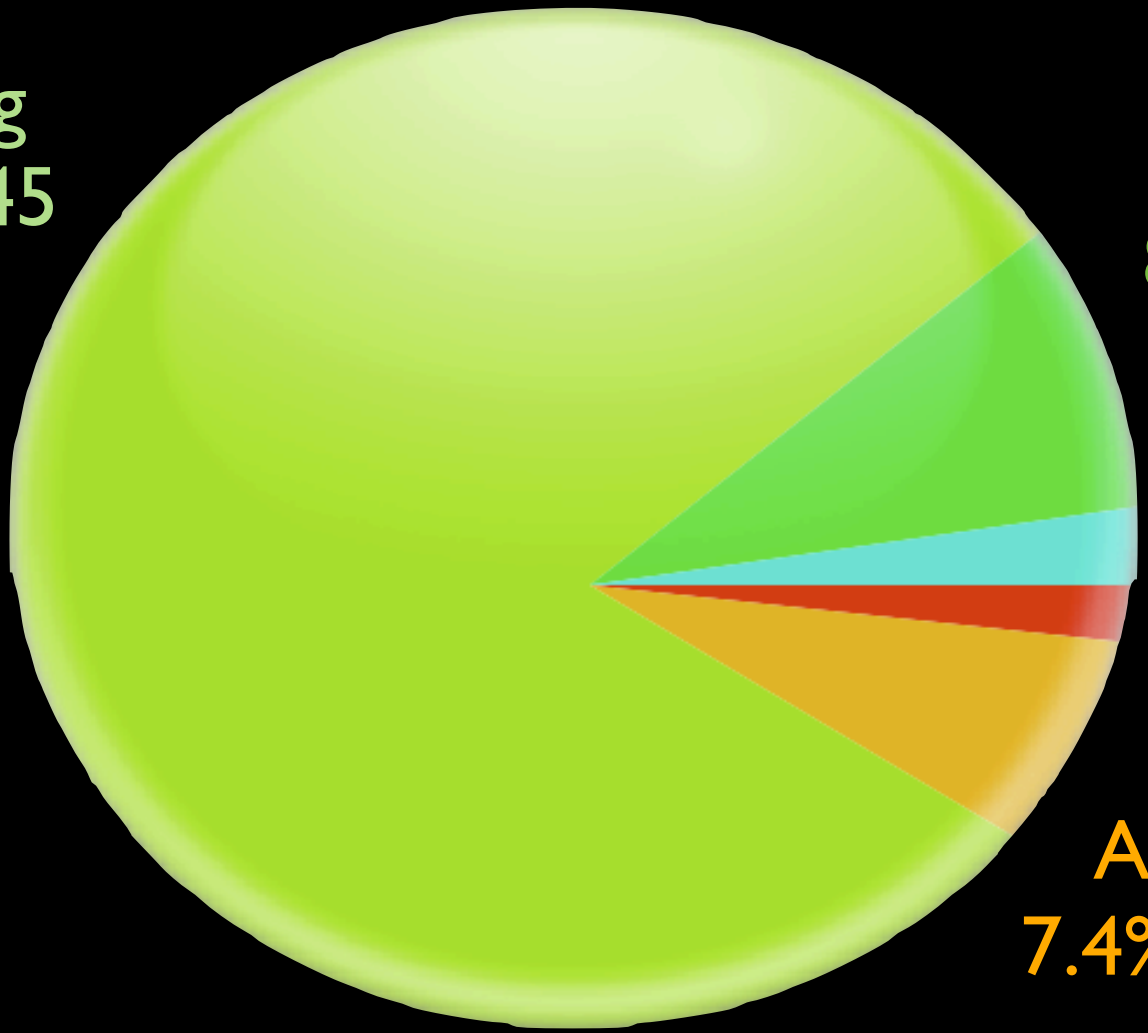
KINGPIN

Beauty shots...

KINGPIN


DEFCON
DEFCON
DEFCON
DEFCON
DEFCON
DEFCON
DEFCON
DEFCON

Time Breakdown



Engineering
79.4% 158:45

Research
8.9% 17:45

Meetings
2.5% 5:00

Writing
1.9% 3:45

Admin
7.4% 14:45

TOTAL: 200 hours (v. 170 hours @ DC15)

(does not include 20+ hours of dealing with logistics/supply chain issues!)

KINGPIN


Submissions due to Kingpin @ HHV by 2pm Sunday
Badge Hacking Contest HQ @ Hardware Hacking Village
Previous results at www.grandideastudio.com/portfolio/defcon-14-badge and /defcon-15-badge
Complete source code, schematics, etc. on DEFCON CD
badge hacking contest!

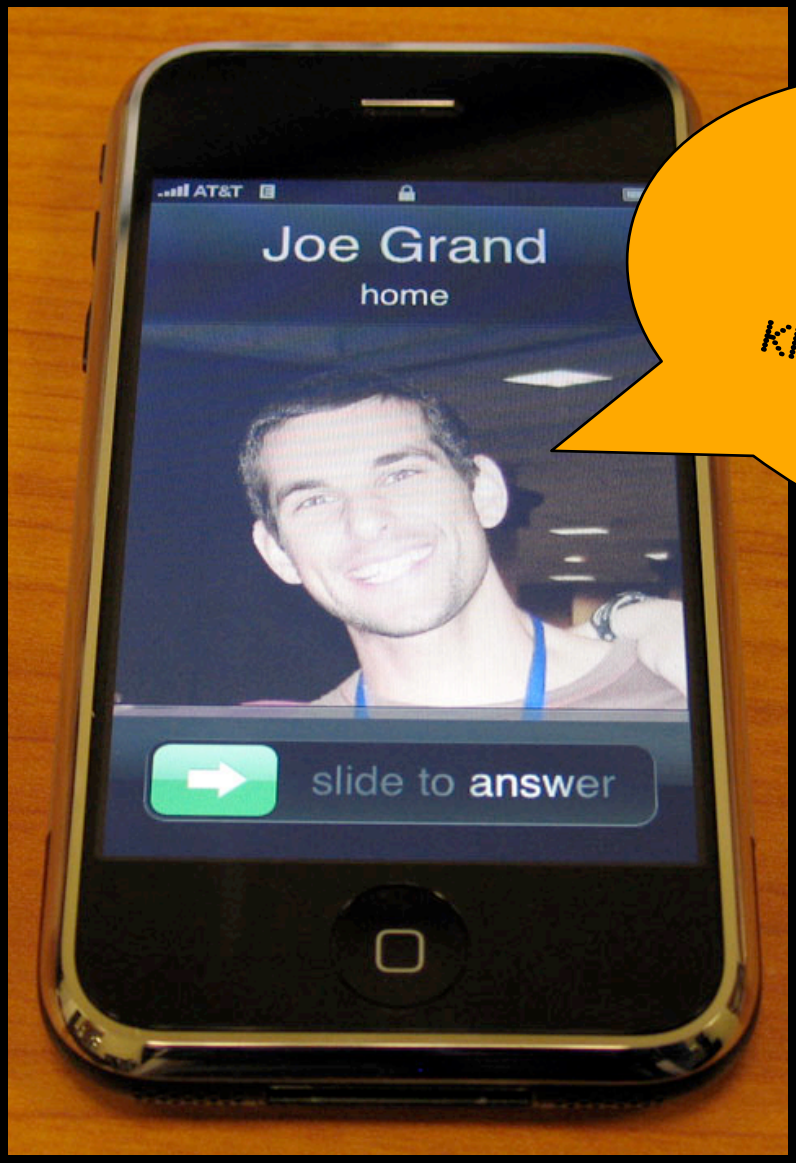
This project did not happen in a vacuum.

Freescale (esp. Dennis Hicks, Angel Galarza, Luis Puebla, Jose Ruiz, Erin Greene, David Niewolny)

e-Teknet - PCB manufacturing & assembly, completed & shipped 8500 badges in under a week

Keely, co-creator of Kingpin back-up unit due to be released September 25, 2008

The Dark Tangent, Ping, KS, V3rtigo, LosT, and other BH/DC staff



THANKS!

KP@KINGPINEMPIRE.COM