BEHIND THE SCENES OF THE DEFCON 27 BADGE

JOE GRAND AKA KINGPIN
BADGE HISTORY
GOALS

- CREATE A GAME TO ENCOMPASS THE DEFCON EXPERIENCE
- USE TECHNOLOGY TO BRING COMMUNITY TOGETHER
- ACCESSIBLE TO ALL DEFCON ATTENDEES
GAMEPLAY / BADGE QUEST

- States denoted by LED patterns
- Advance to the next state by completing tasks
- Some require discovery of magic tokens
- All require interaction with other people
- When all tasks are complete, celebrate
**MCU**

- **NXP KL27**
- **ARM-CORTEX M0+**
- **64KB FLASH, 16KB SRAM**
- **DC27: GPIO, I2C, LPTMR, TPM, UART (2)**
Near Field Magnetic Induction

- Low power, non-propagating field between devices
- Designed for short range data and/or audio transfer (< 1m)
- Hearing aids, wireless ear buds, body area network / tactical
- NXP MIGLO
- NXH2261 = NFMI + ARM
- INTERNAL EEPROM (FIRMWARE) PROGRAMMED VIA I2C ON POWER-UP
- UART TO / FROM KL27
- GPIO FOR STATUS / INTERRUPT
- 10.58MHZ CARRIER, 596KBPS
- CUSTOM MULTI-BADGE DATA TRANSFER CODE BY NXP FOR DC27
- LPBROADCAST_NXH_DC27.EEP.H
• DATA PACKET AKA "PACKET OF INFAMY"
• BROADCAST TO ANY DEVICE WITHIN RANGE
LED DRIVER

• TEXAS INSTRUMENTS LP5569
• 1.5X CHARGE PUMP = HIGH VF LEDS @ LOW VIN
• AUTOMATIC POWER SAVE MODE (10UA)
• EACH LED INDIVIDUALLY ADDRESSABLE, DIMMABLE (12-BIT PWM @ 20KHZ)
• CURRENT OUTPUT VARIATES PER COLOR, SET ON POWER-UP (8-BIT, 100UA STEP)
MOUNTING OPTIONS

- LANYARD
- LANYARD CLIP
- WATCH STRAP
- HEADBAND
- BROOCH / AMULET
- ???
EARLY CONCEPTS
PROTOTYPING / DEVELOPMENT
HUNTING FOR TREASURE

• ADVENTURES AT THE TUCSON GEM SHOW
• 48 SHOWS OVER TWO WEEKS, ~50K PEOPLE
• 36 HOURS TO FIND SUPPLIER
• RETAIL VENDORS / HOTEL ROOMS -> WHOLESALE -> MINE OWNER -> FACTORY
HUNTING FOR TREASURE
GEMSTONE FABRICATION

• HAND CUT QUARTZ CRYSTAL
• RAW MATERIAL FROM BRAZIL
• NATURALLY FRACTURED, STRENGTH VARIES
• DYED COLORS FOR NON-HUMAN BADGES
• CRAFTED BY YEE ON GEMS & JEWELLERY
GEMSTONE FABRICATION
GEMSTONE FABRICATION
GEMSTONE FABRICATION
FIRMWARE

- 85% of Flash (56KB), 33% of RAM (5.3KB)
- ~3K Physical Source Lines of Code in dc27_badge.c (Main)
DEVELOPMENT ENVIRONMENT (SW)

- NXP MCUXPRESSO IDE 10.2.1
- FRDM-KL27Z SDK 2.4.1
**DEVELOPMENT ENVIRONMENT (HW)**

- SWD (ARM SERIAL WIRE DEBUG)
- NXP LPC-LINK2
- TAG-CONNECT TC2050-IDC-NL-050-ALL (NORMAL ORIENTATION)
- TRIM ALIGNMENT PINS IF USING W/ MOUNTED GEMSTONE
- VTREF PROVIDES 1.8V I/O LEVEL TO DEBUG PROBE
DEVELOPMENT ENVIRONMENT (HW)

- UART
- 1.8V @ 115200, 8N1
- DEBUG OUTPUT / SYSTEM STATUS
- COMMAND-BASED INTERACTIVE MODE
- WILL ENTER AUTOMATICALLY IF RX LINE IS PULLED HIGH
- MUST EXIT W/ CTRL-X

Mates to Harwin M20-8770442 or compatible
PCB ASSEMBLY
PROGRAMMING / TESTING

• WINDOWS W/ MCUXPRESSO + LPC-LINK2
• CMD SCRIPT TO PROGRAM KL27
• POWER ON SELF TEST
• INSPECTION OF LEDS (VISIBLE) AND PIEZO (AUDIBLE)
• DETECTION / CONFIGURATION OF NXH2261 + LP5569
FINAL ASSEMBLY
NUMBERS

- HUMAN, WHITE: 26,500
- GOON, RED: 550
- SPEAKER, BLUE: 375
- VENDOR, PURPLE: 250
- PRESS, GREEN: 250
- VILLAGE, ORANGE: 250
- CONTEST, YELLOW: 250
- ARTIST, LIGHT BLUE: 100
- CFP REVIEW, GREY: 45
- UBER, BLACK: 20

(BEFORE GEMSTONE ATTACHMENT)
CHALLENGES / INSIGHTS

• TIME FRAME
• COMMUNICATION W/ PCB FAB
• USING UNFAMILIAR TECHNOLOGIES / NON-STANDARD MATERIALS
• BREAK PROJECT INTO SMALL BITES
• ALL PROBLEMS HAVE A ROOT CAUSE
**BATTERY LIFE**

- **CR2032 3V LITHIUM COIN CELL**
- **225MAH TO 2V**
- **POWER UP: 4.2MA**
- **ATTRACT MODE: 2.3 - 4.6MA**
- **SLEEP MODE (NFMI ENABLED)**
  - **0.41 - 2.0MA**
  - **0.61MA AVERAGE**
- **MINIMUM DESIRED LIFE = 4 DAYS (96 HOURS) -> 2.3MAH AVERAGE**
FUTURE USE

• DATA TRANSFER
• COVERT MESSAGE PASSING (NO RF SIGNATURE)
• ROBOTICS (LOCATION TRACKING / SENSING)
• BLINKENLIGHTS
• GENERAL PURPOSE ARM DEV. ENVIRONMENT
• ???
RESOURCES

• DC27 HARDWARE HACKING VILLAGE (HHV)
• EXTRA MATERIALS (GEMSTONES, COMPONENTS, BATTERIES)
• REAL-LIFE ENGINEER FROM NXP
• DESIGN DOCUMENTATION, CODE, ETC.
• www.grandideastudio.com/portfolio/
  defcon-27-badge/
ENJOY THE CON!

@JOEGRAND | WWW.GRANDIDEASTUDIO.COM