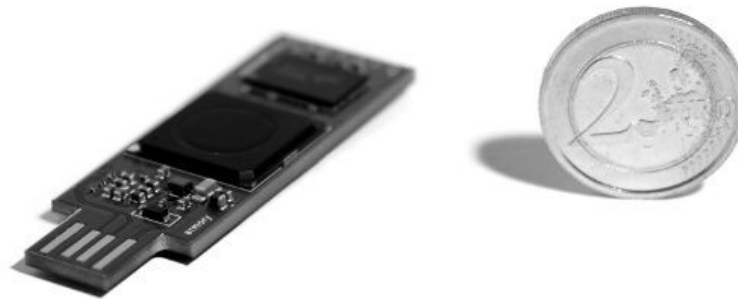


# Forging the USB armory

Andrea Barisani

<andrea@inversepath.com>



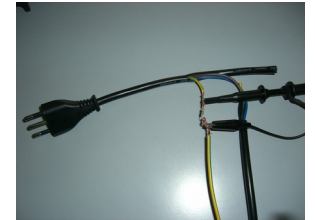
2007: Unusual Car Navigation Tricks

Injecting RDS-TMC Traffic Information Signals



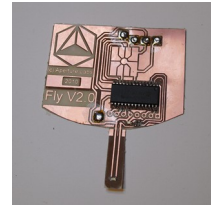
2009: Sniff Keystrokes With Lasers/Voltmeters

Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage



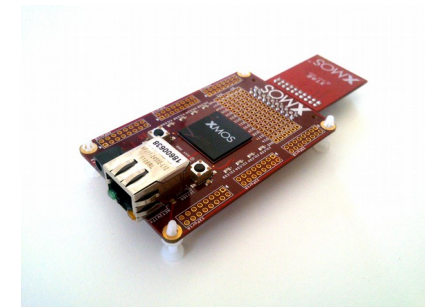
2011: Chip & PIN is definitely broken

Credit card skimming and PIN harvesting in an EMV world



2013: Fully arbitrary 802.3 packet injection

Maximizing the Ethernet attack surface







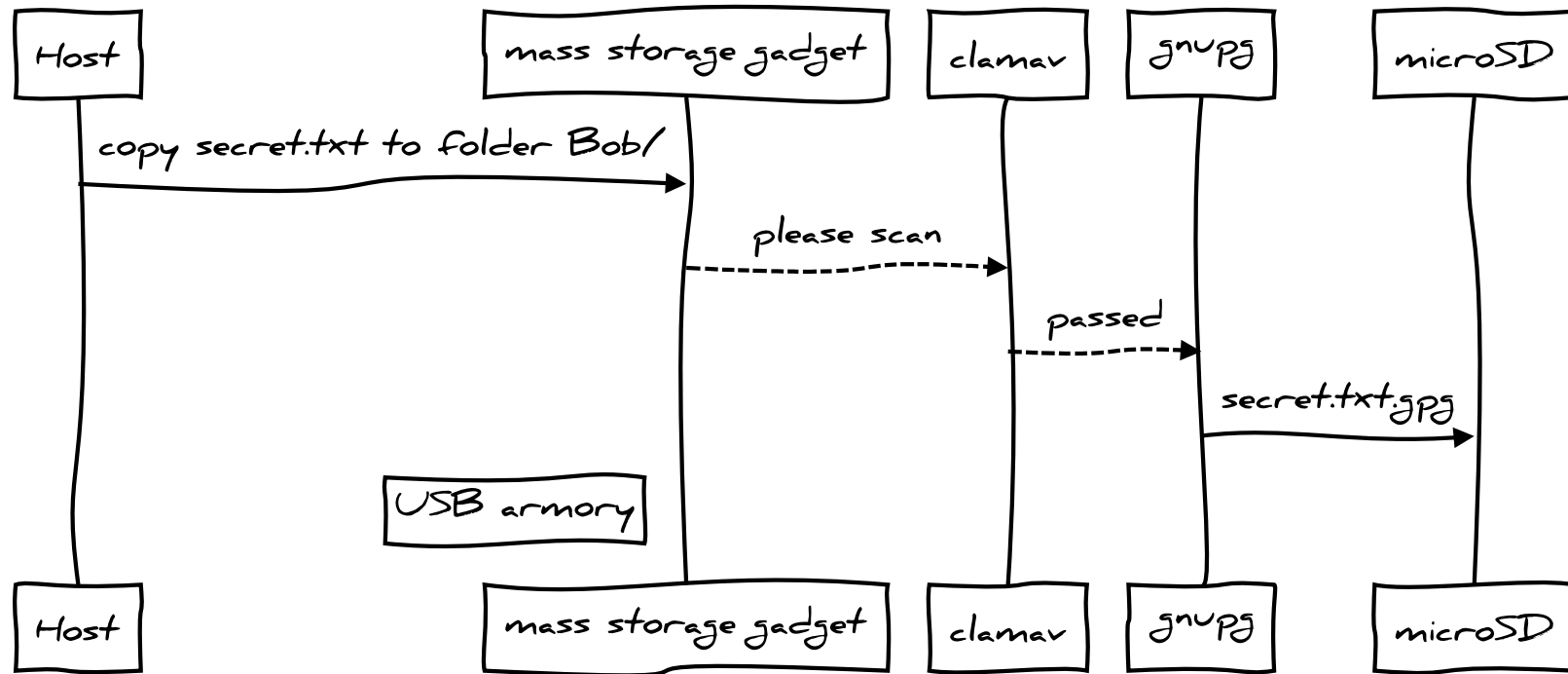
Designed for personal security applications

- mass storage device with advanced features such as automatic encryption, virus scanning, host authentication and data self-destruct
- OpenSSH client and agent for untrusted hosts (kiosk)
- router for end-to-end VPN tunneling, Tor
- password manager with integrated web server
- electronic wallet (e.g. pocket Bitcoin wallet)
- authentication token
- portable penetration testing platform
- low level USB security testing



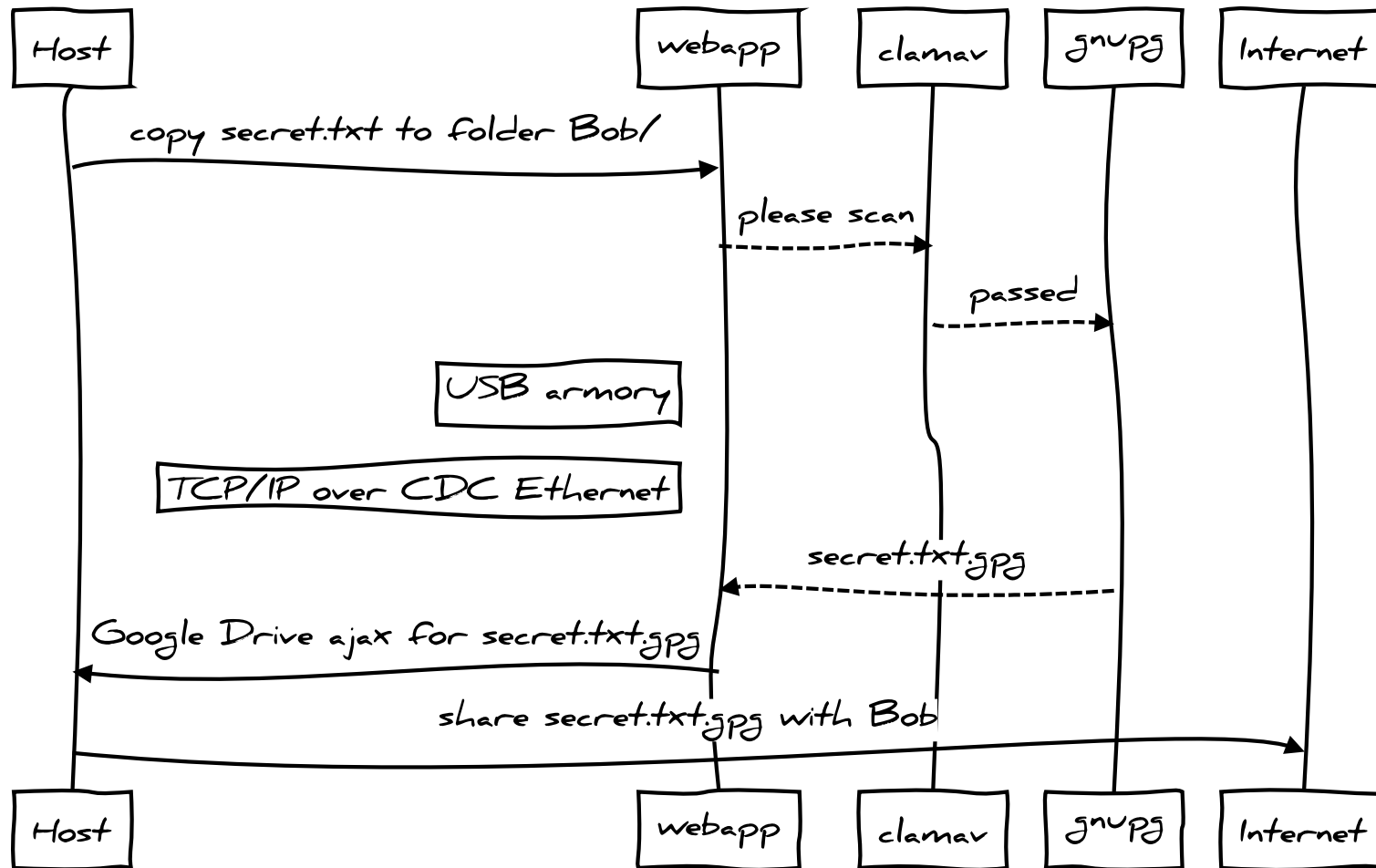


## enhanced mass storage



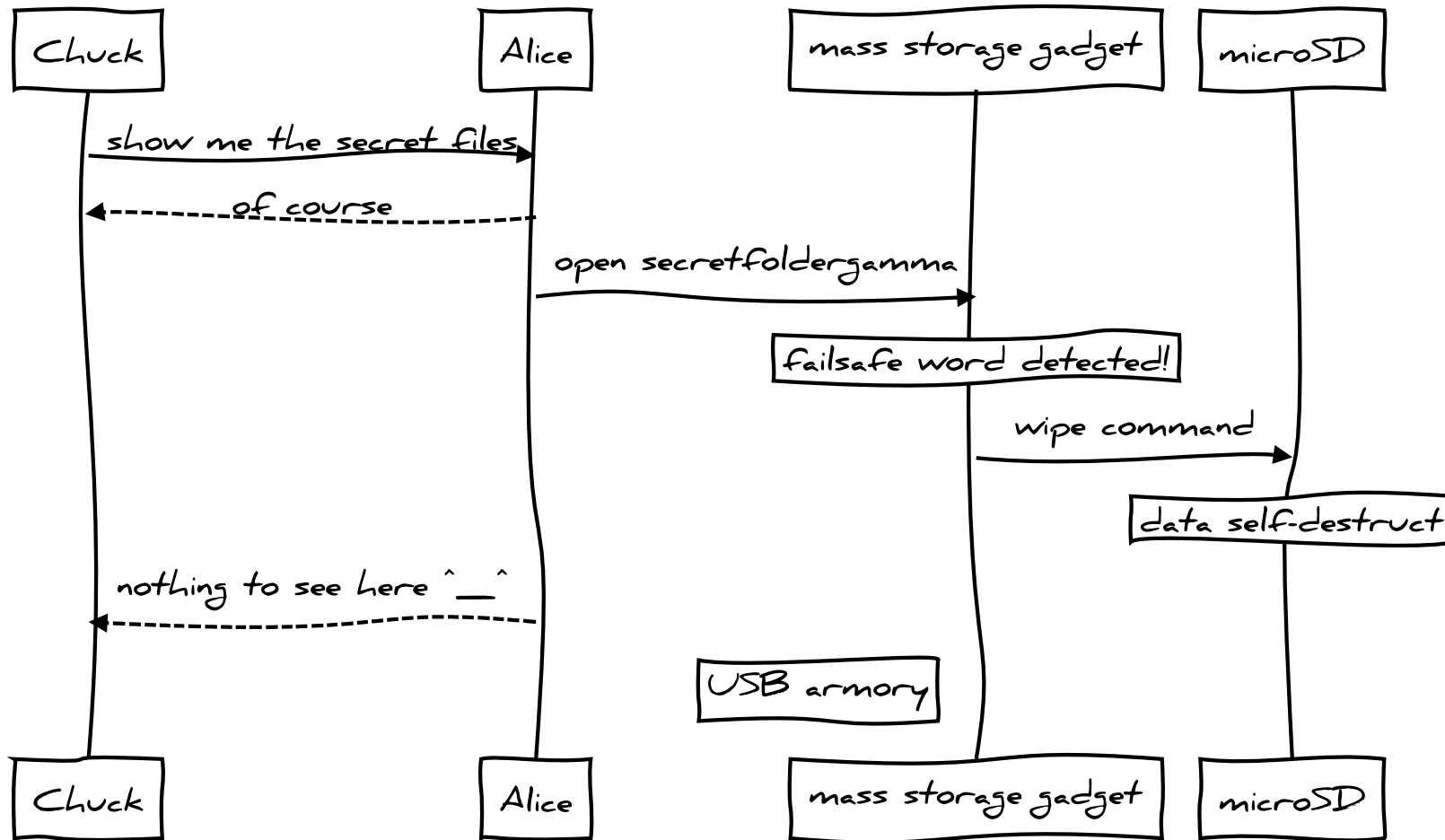


## enhanced mass storage



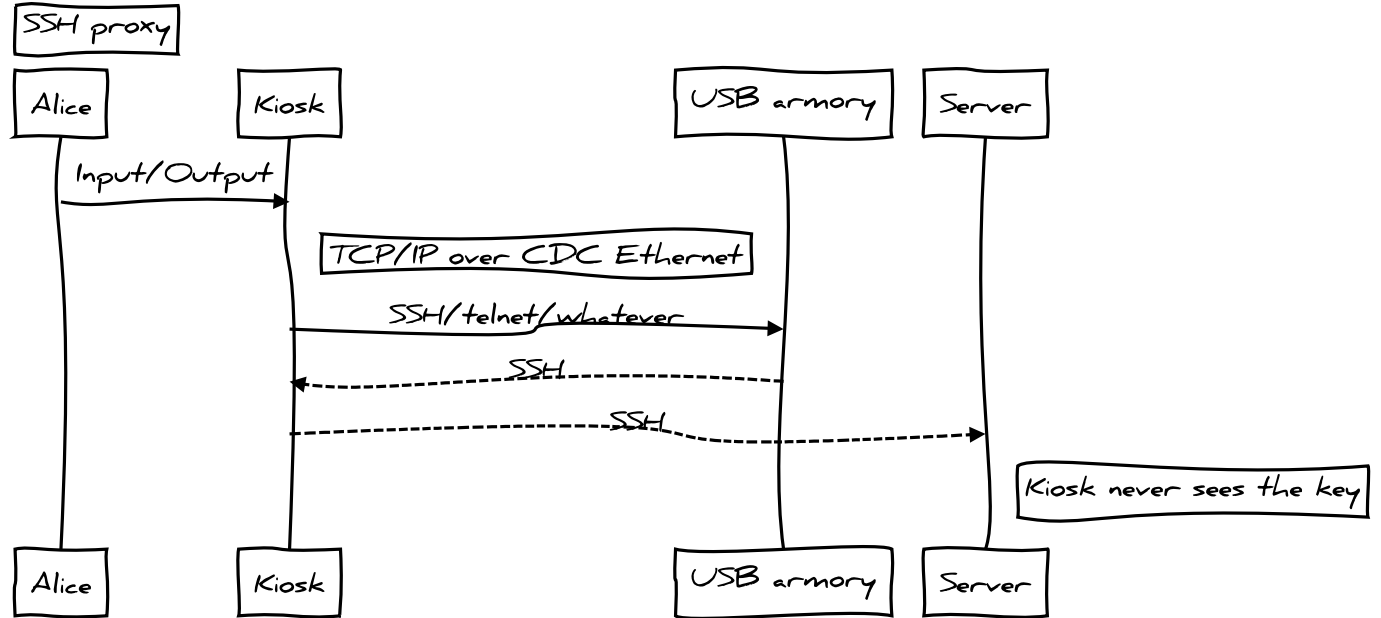
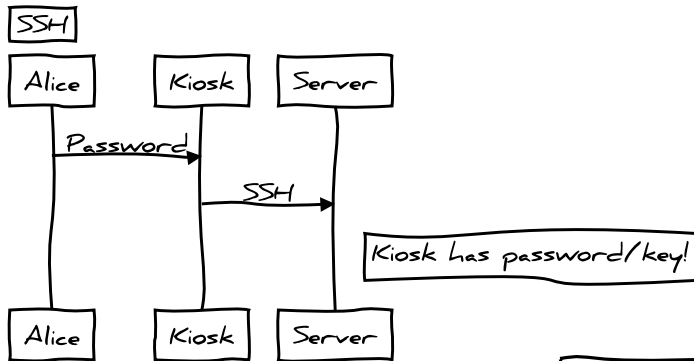


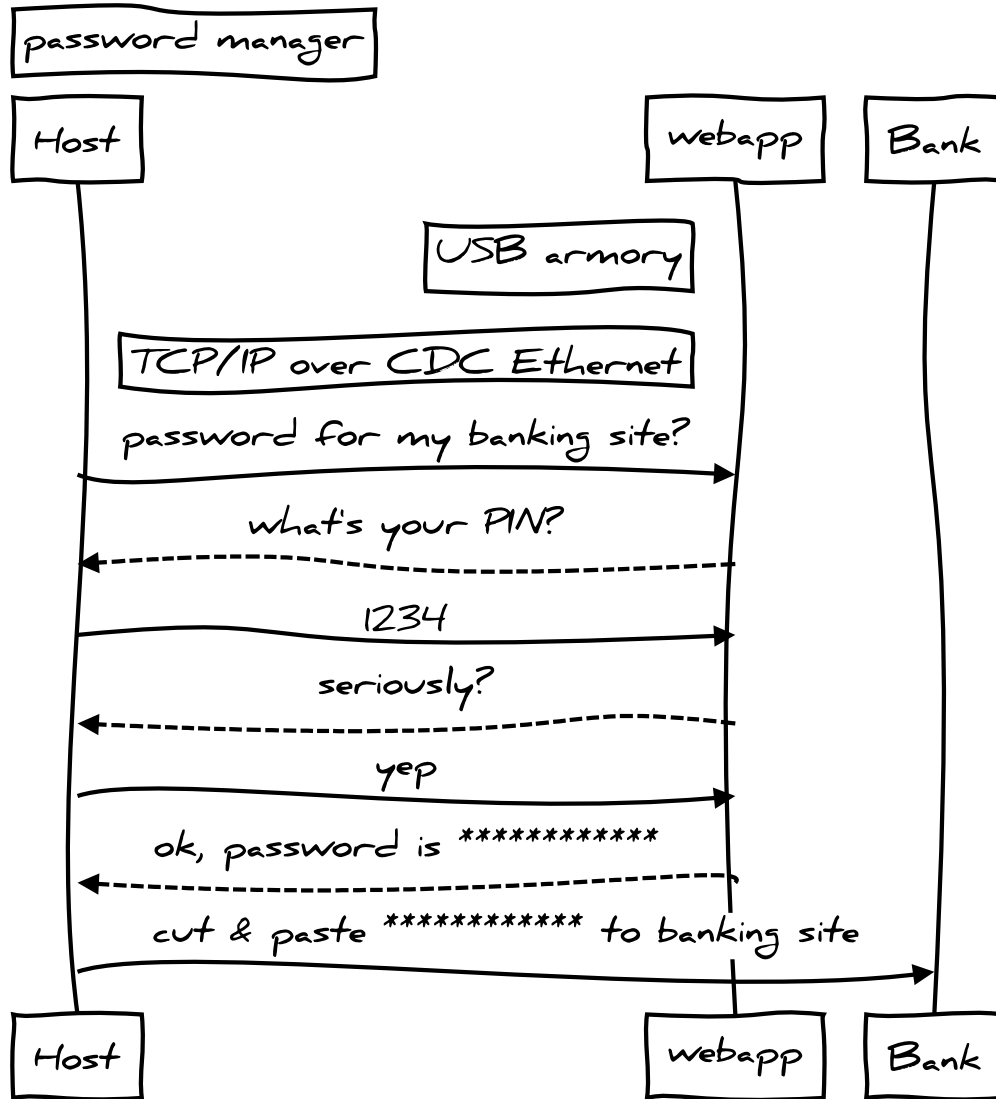
## enhanced mass storage





## SSH proxy



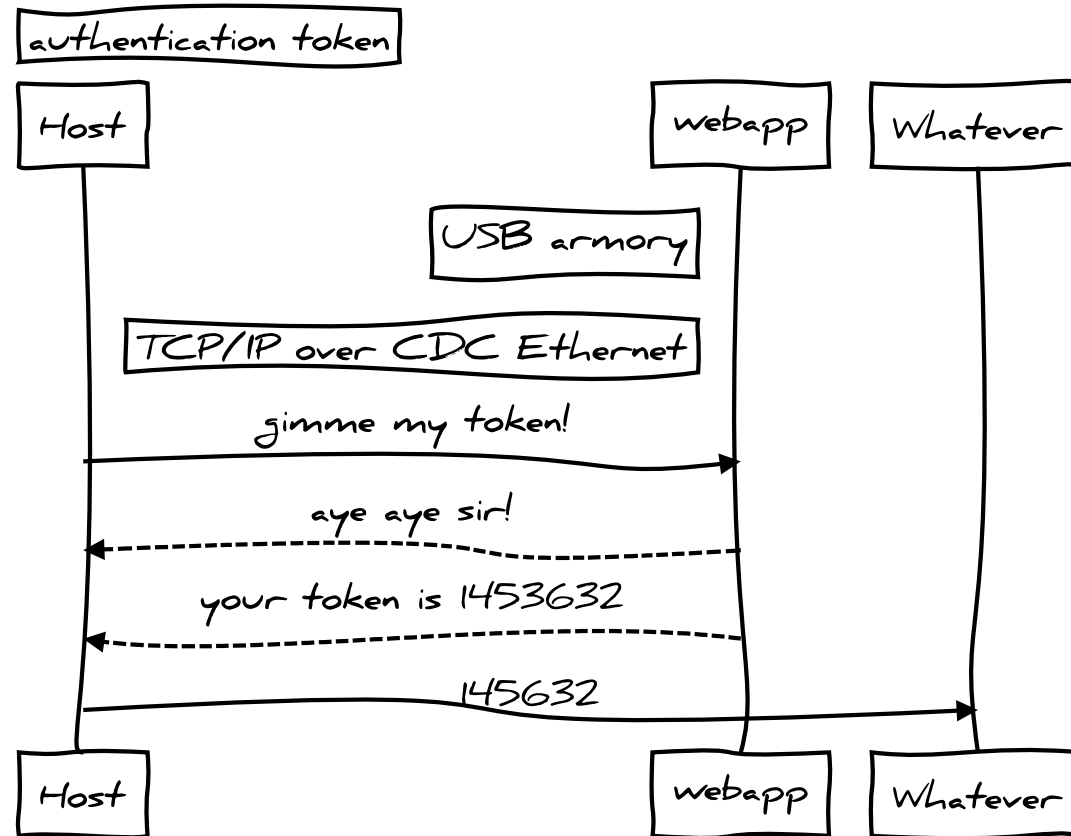


password manager

*\*trivial example, better options planned*

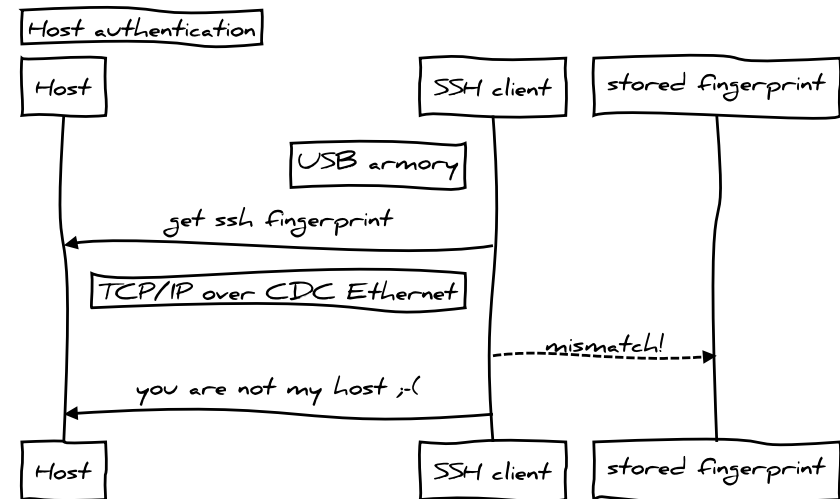
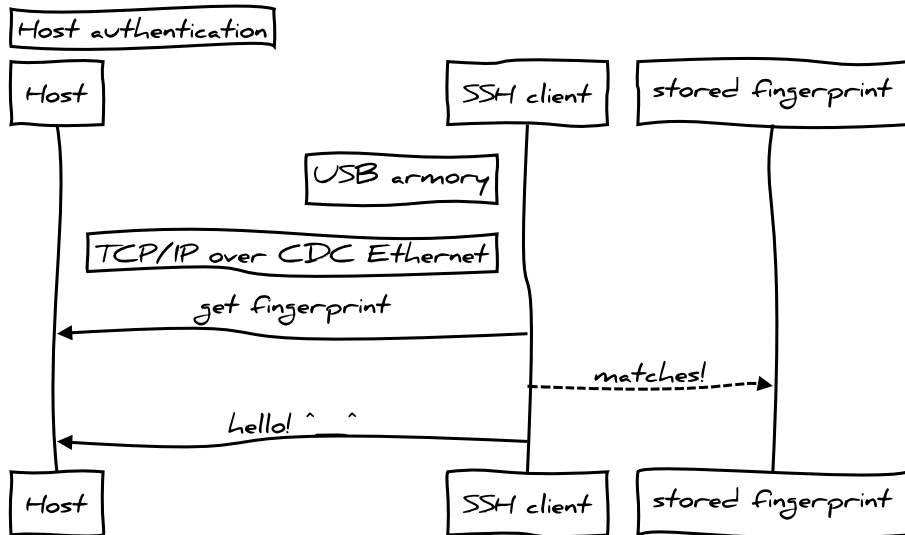


## authentication token





## USB device authenticates host





## Design goals

Compact USB powered device

Fast CPU and generous RAM

Secure boot

Standard connectivity over USB

Familiar developing/execution environment

Open design

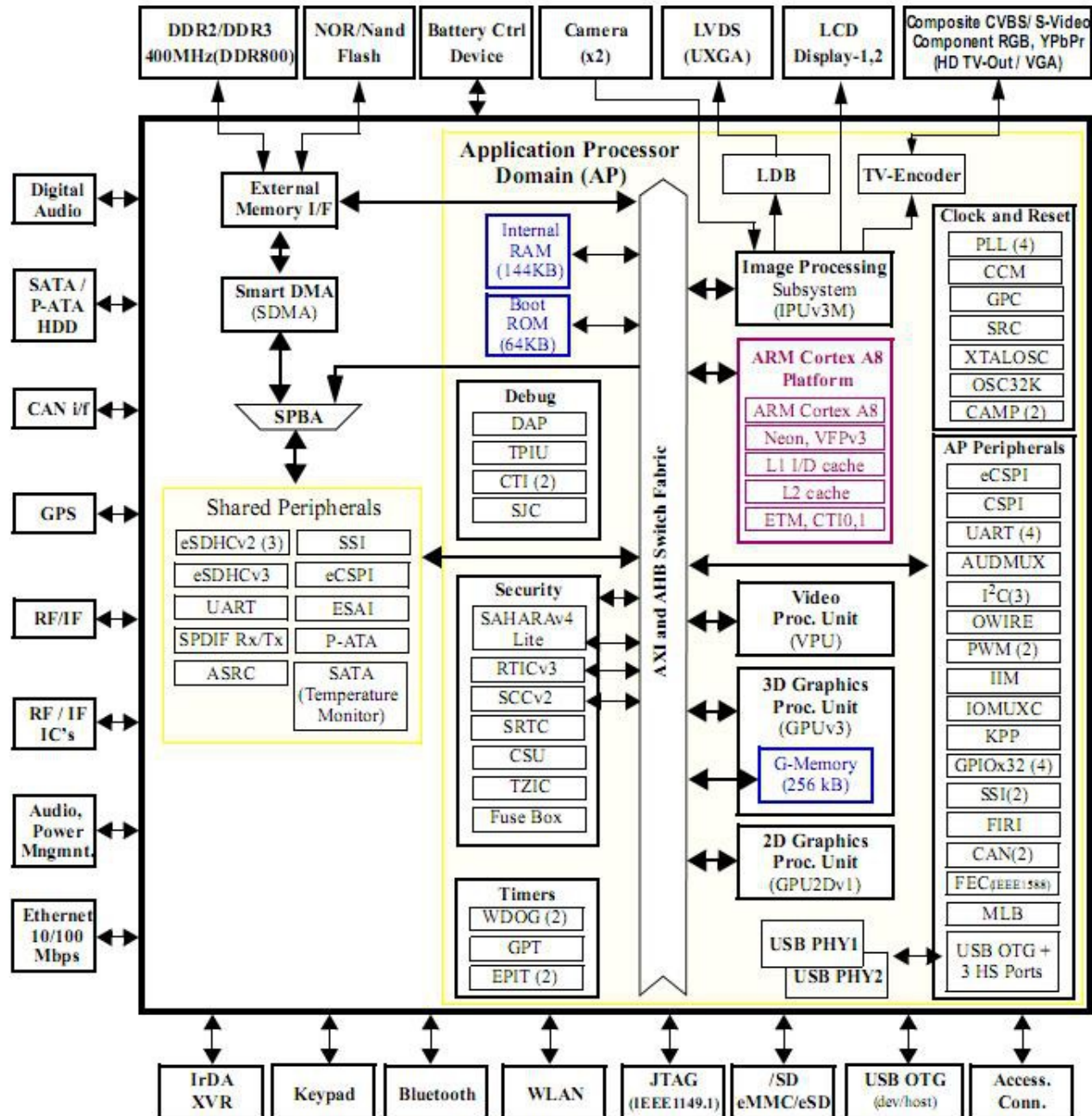




## Selecting the System on Chip (SoC)

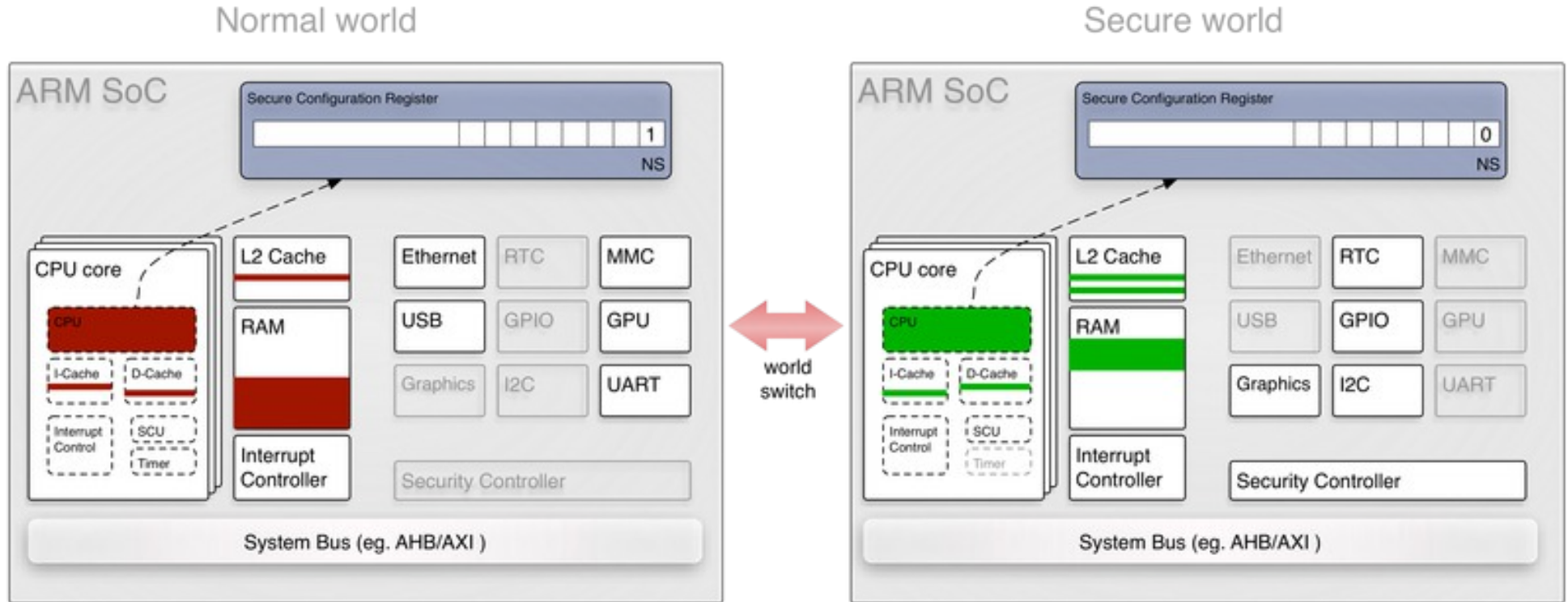
### Freescale i.MX53

- ARM® Cortex™-A8 800-1200 Mhz
- almost all datasheets/manuals are public (no NDA required)
- Freescale datasheets are "ok" (far better than other vendors)
- ARM® TrustZone®, secure boot + storage + RAM
- detailed power consumption guide available
- excellent native support (Android, Debian, Ubuntu, FreeBSD)
- good stock and production support guarantee





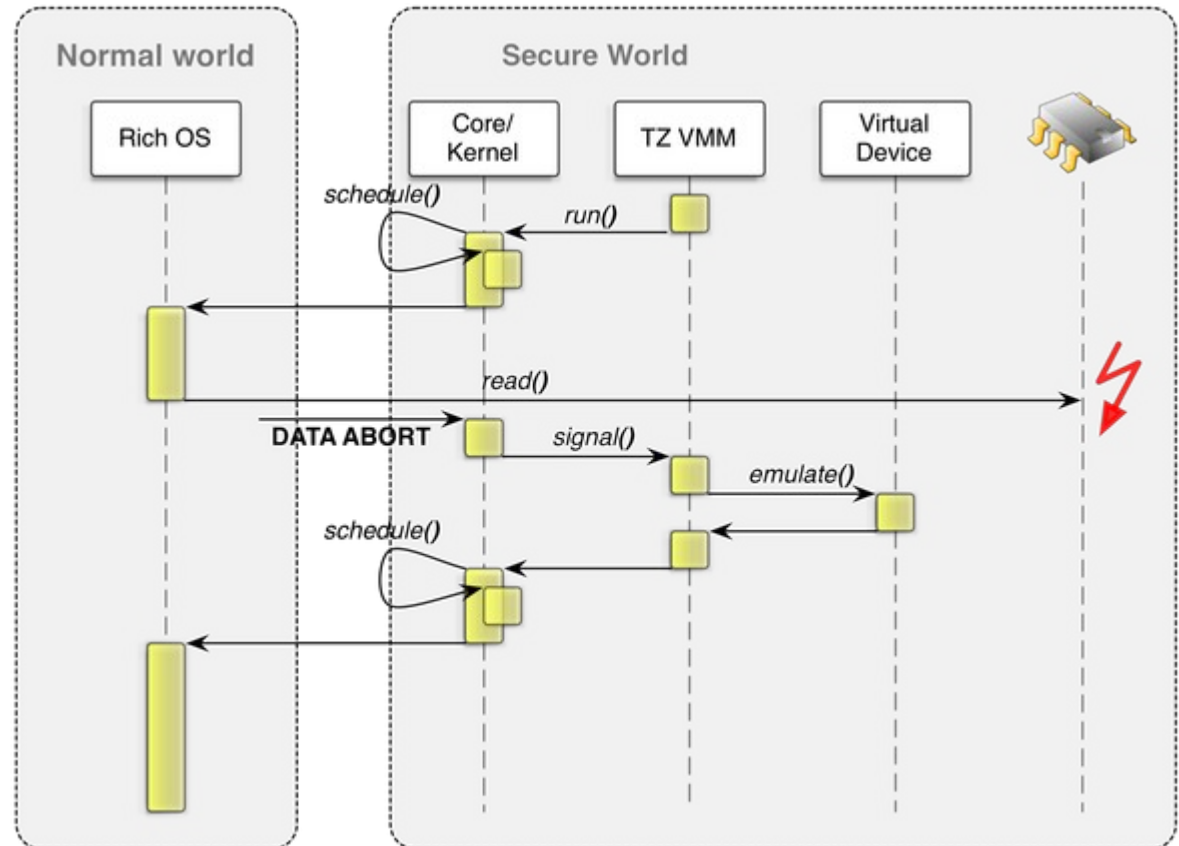
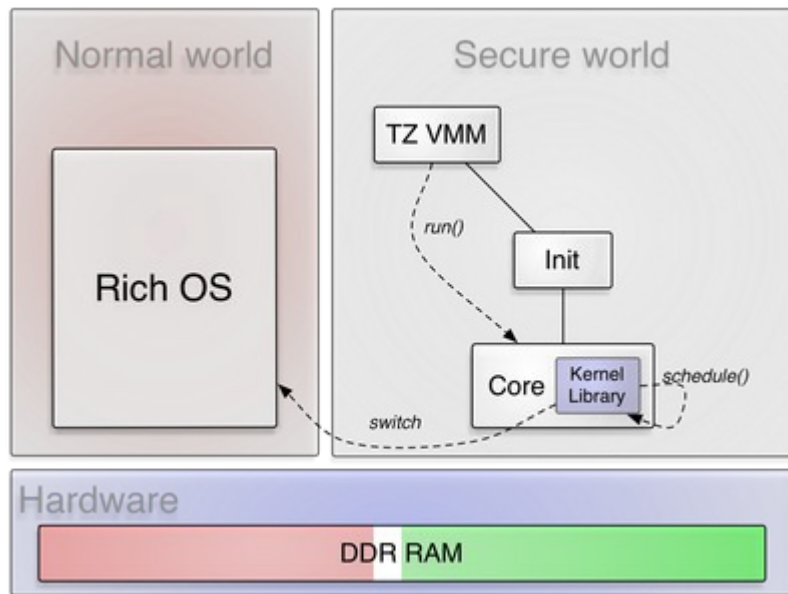
## ARM® TrustZone®



<http://genode.org/documentation/articles/trustzone>



## ARM® TrustZone®



<http://genode.org/documentation/articles/trustzone>

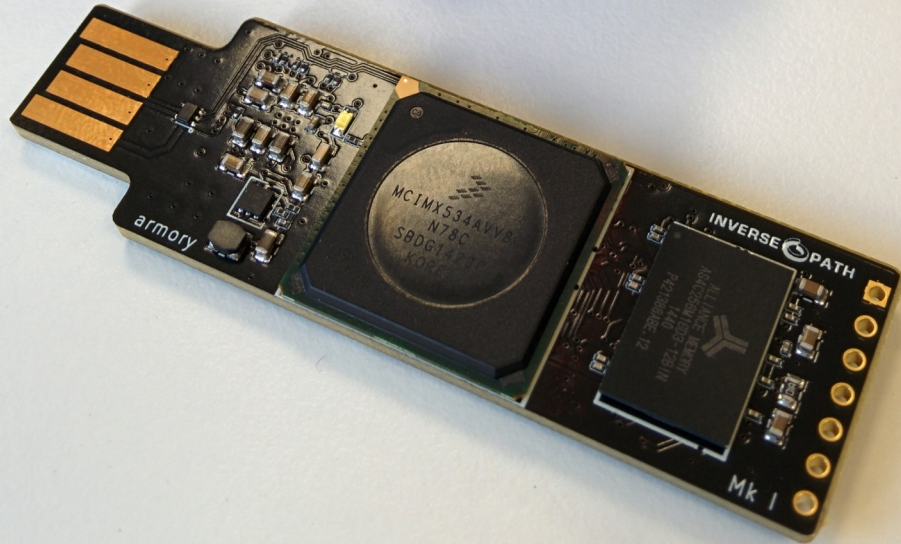


## Development time-line

- 2014/01: first concept idea (based on Atmel SoCs)
- 2014/03: schematics development begins (Freescale chosen)
- 2014/04: PCB layout for breakout/prototyping board
- 2014/08: alpha board order
- 2014/09: USB armory alpha board delivery & evaluation
- 2014/10: project announcement
- 2014/10: order for 7 optimized beta revisions
- 2014/11: beta boards delivery & evaluation
- 2014/11: design finalization, Mk I production candidate order
- 2014/12: Mk I delivery
- 2015/01: first batch production



INVERSE  PATH



open source  
hardware



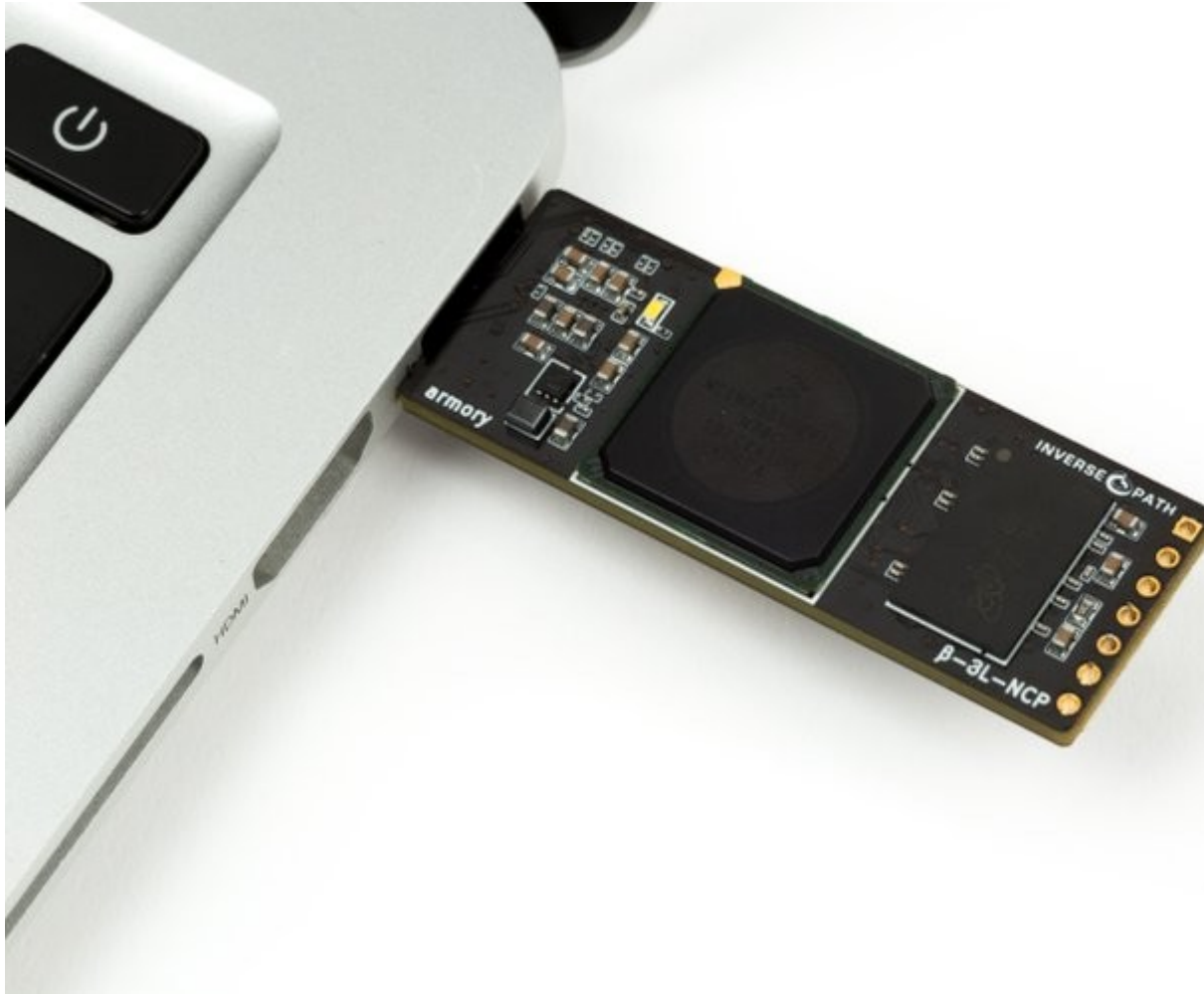
open source

<http://inversepath.com/usbarmory>



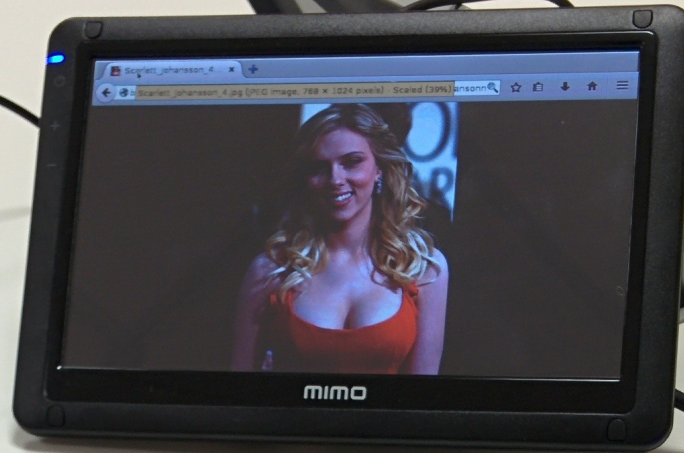
## USB armory - Open source flash-drive-sized computer

- Freescale i.MX53 ARM® Cortex™-A8 800Mhz, 512MB DDR3 RAM
- USB host powered (<500 mA) device with compact form factor (65 x 19 x 6 mm)
- ARM® TrustZone®, secure boot + storage + RAM
- microSD card slot
- 5-pin breakout header with GPIOs and UART
- customizable LED, including secure mode detection
- excellent native support (Android, Debian, Ubuntu, FreeBSD)
- USB device emulation (CDC Ethernet, mass storage, HID, etc.)
- Open Hardware & Software



device mode





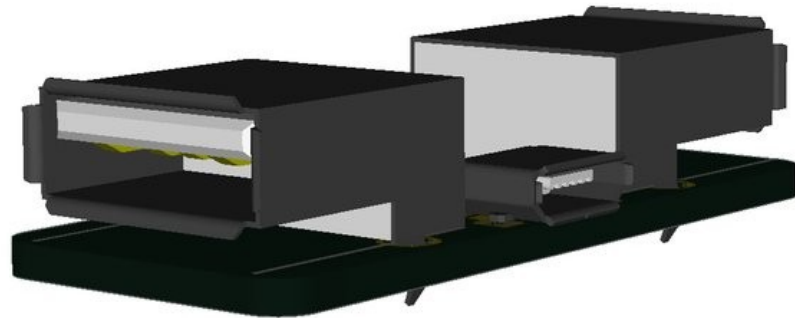
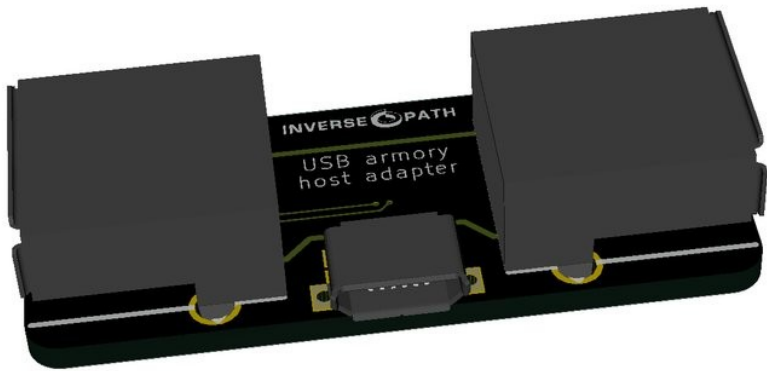
host mode  
(stand-alone)

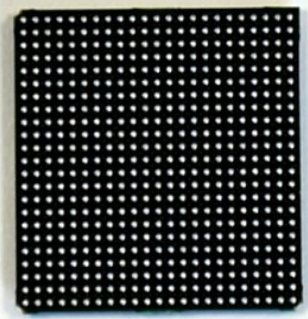
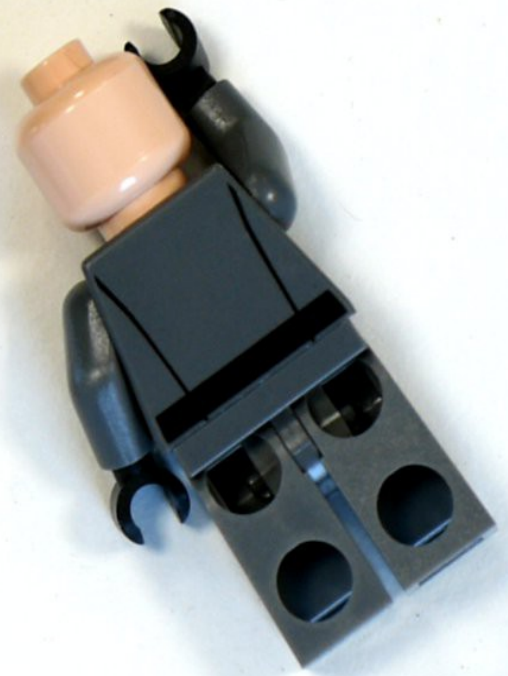




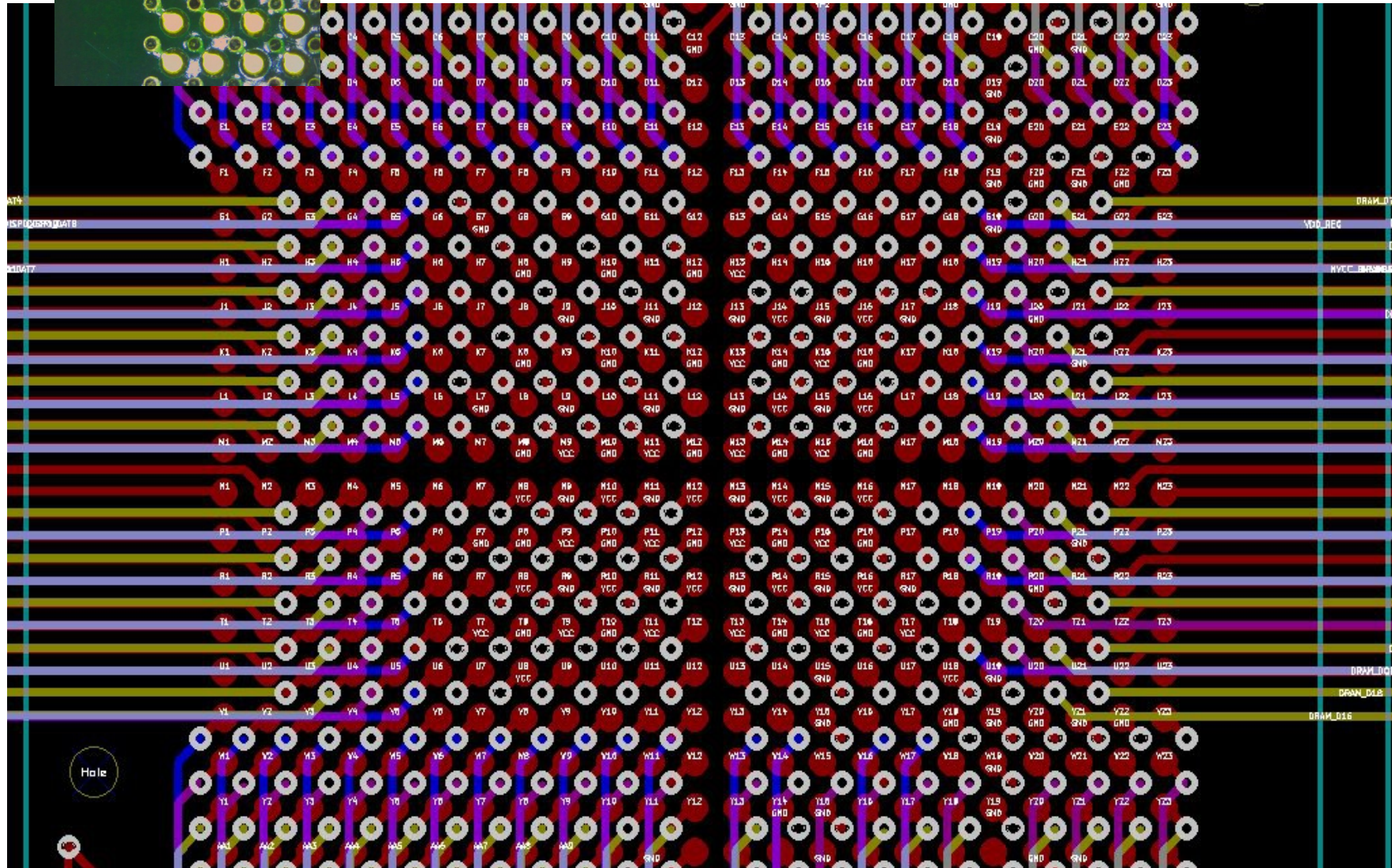
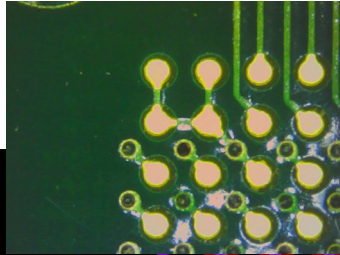


custom host adapter

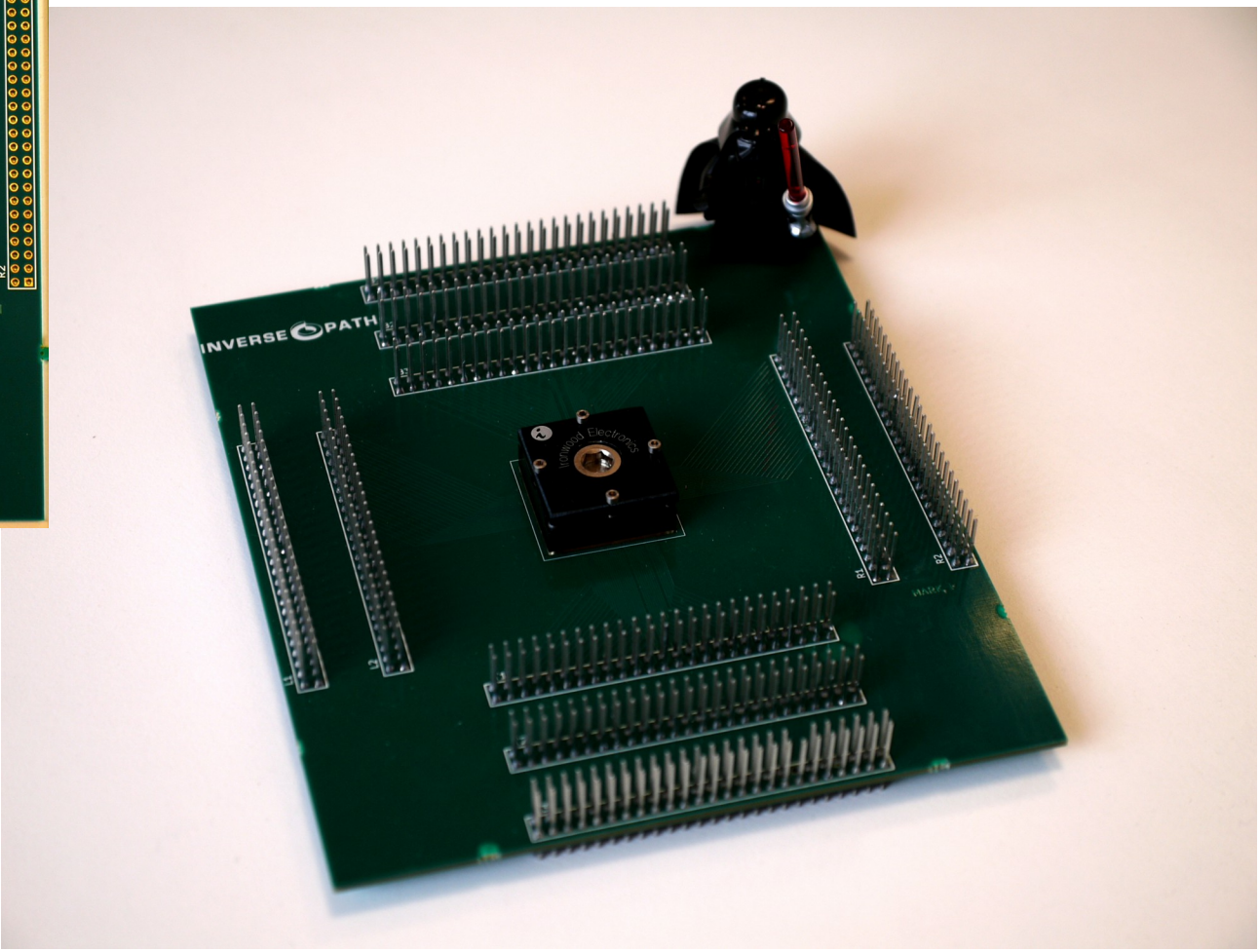
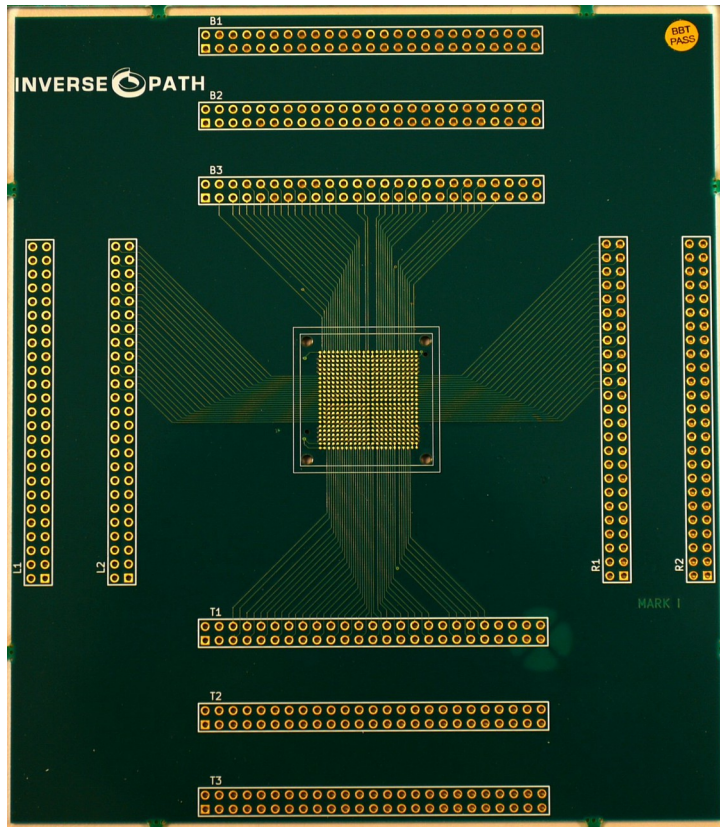




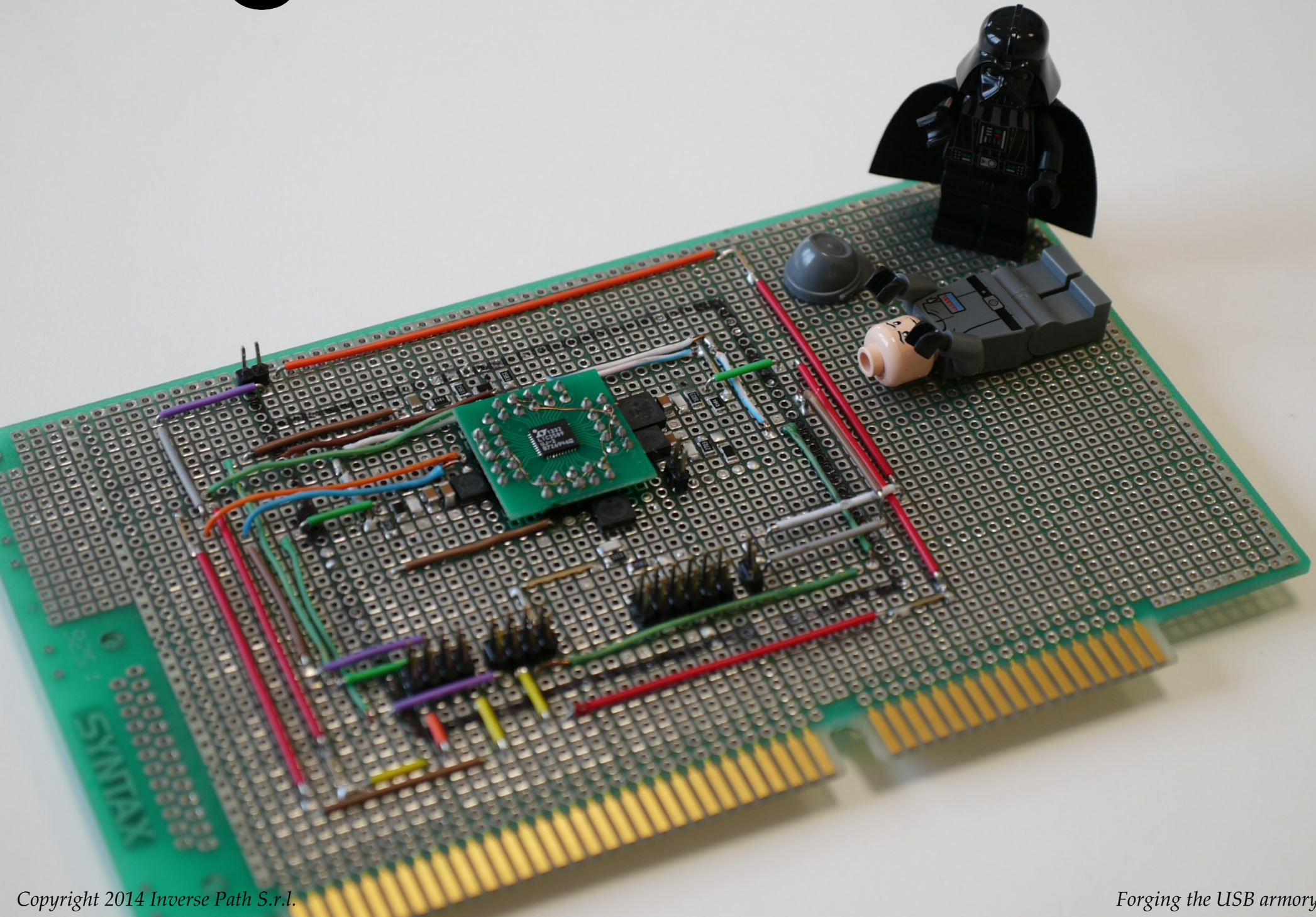




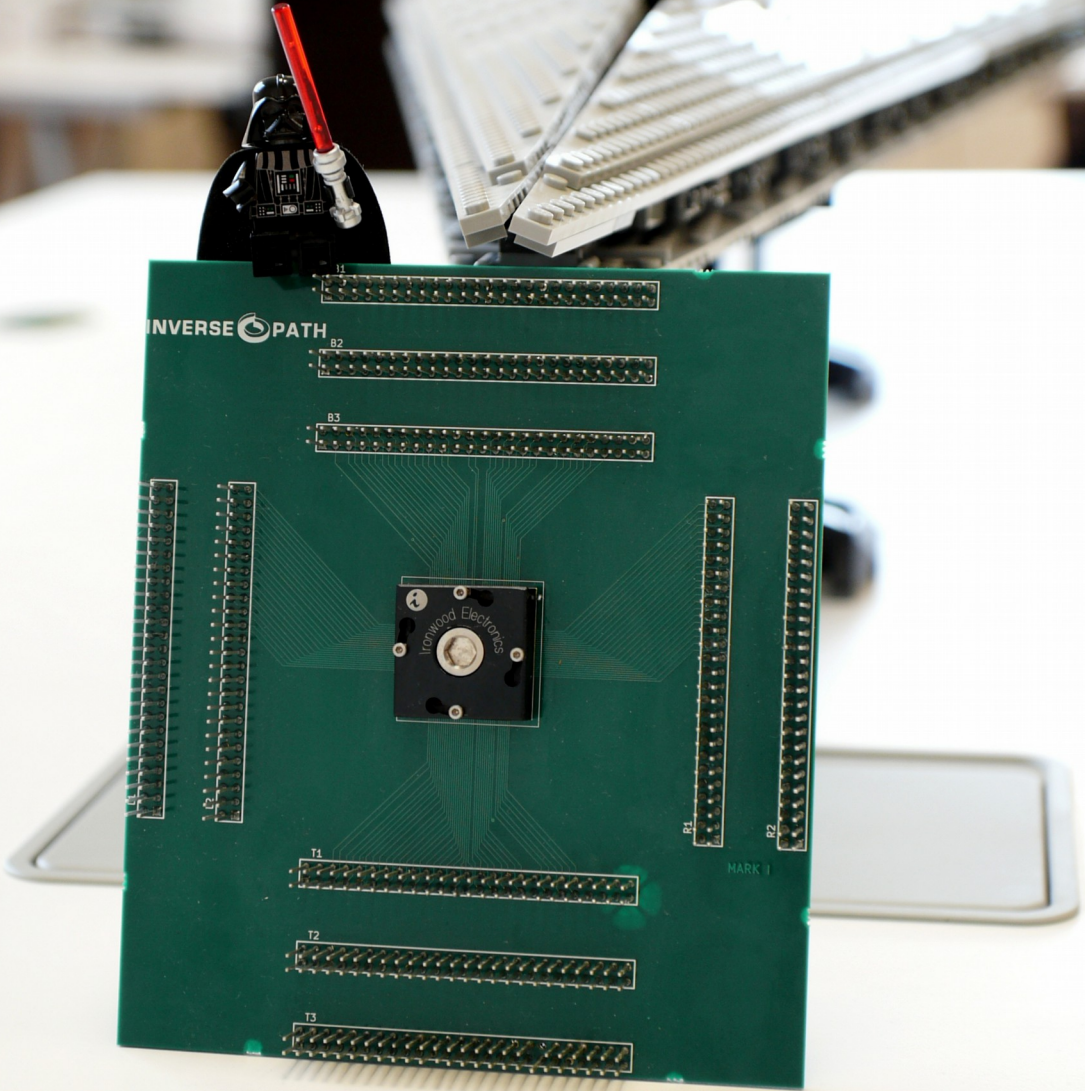




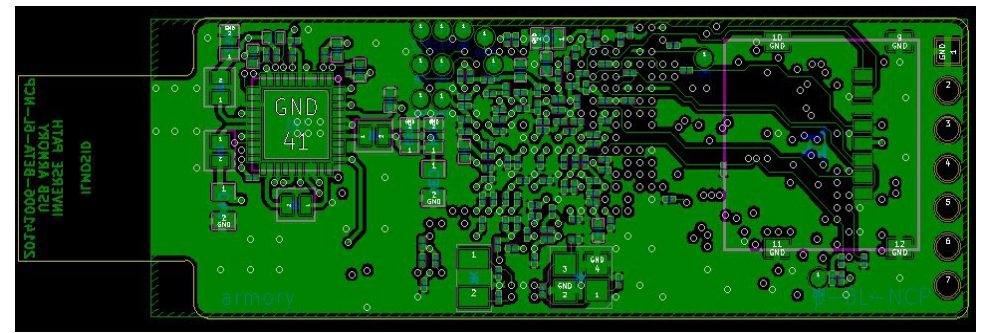
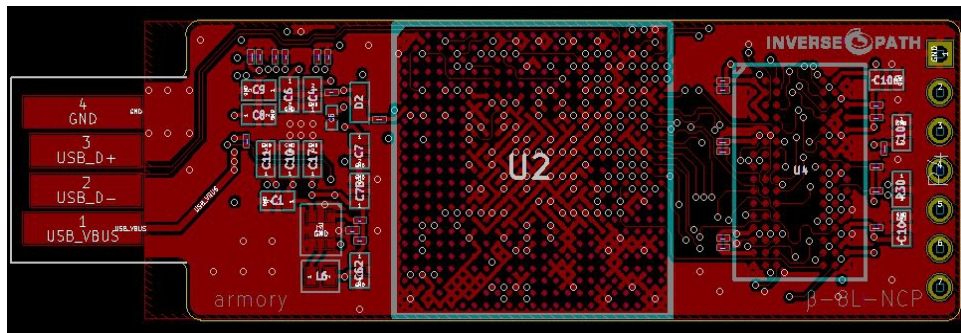
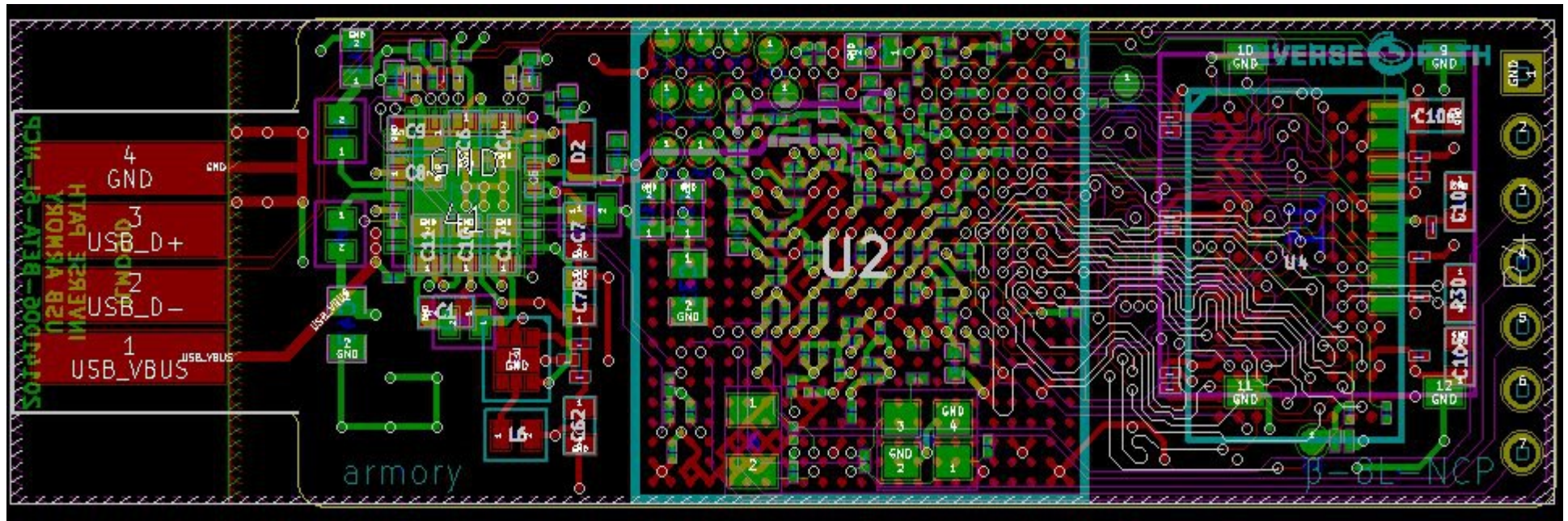




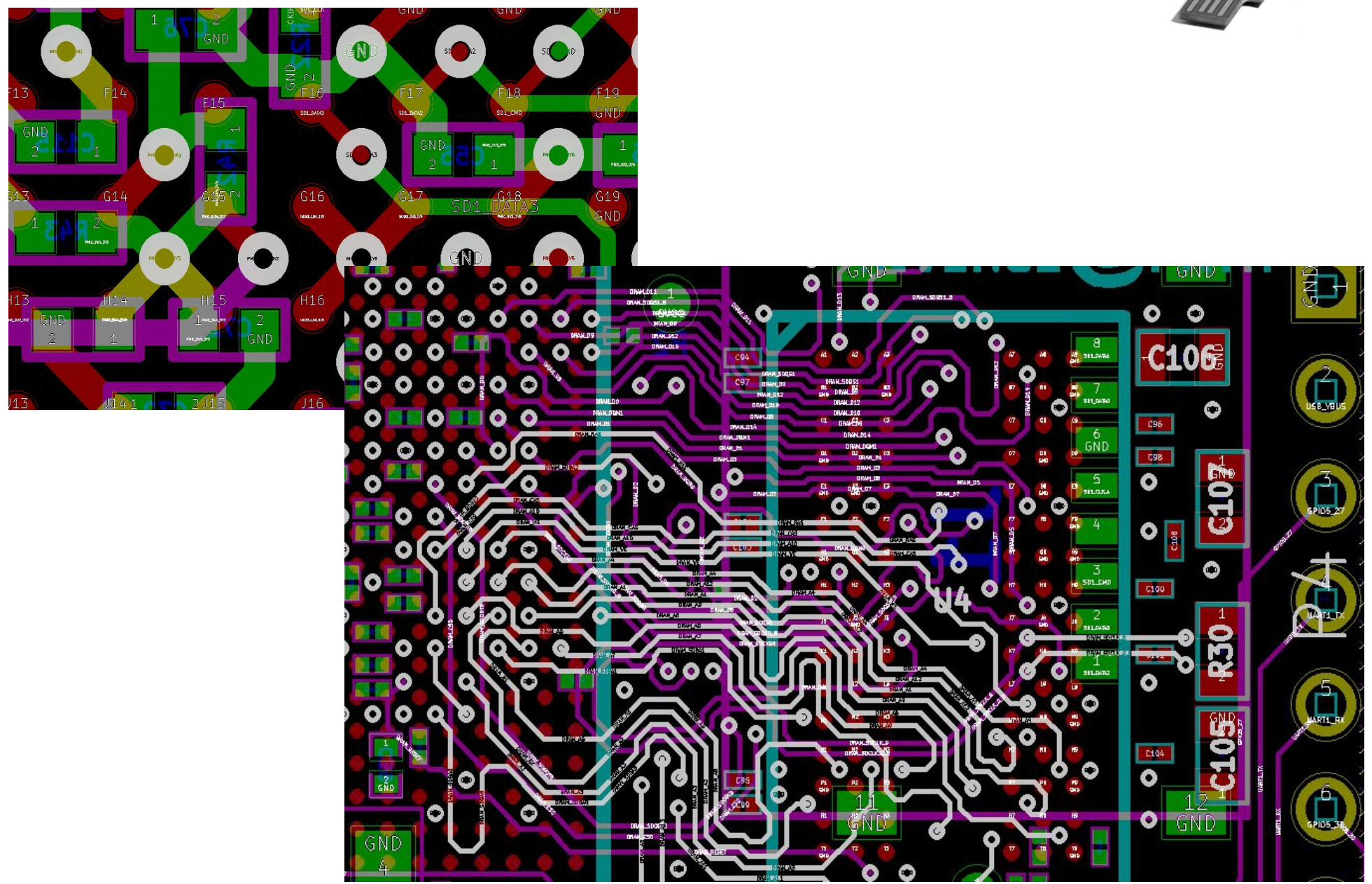


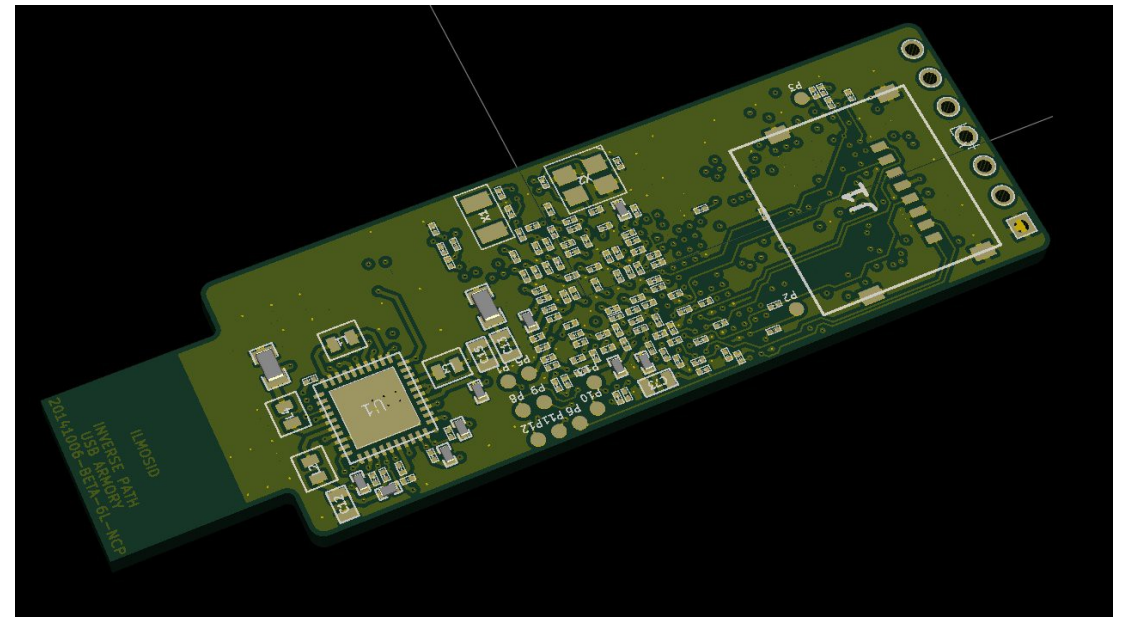
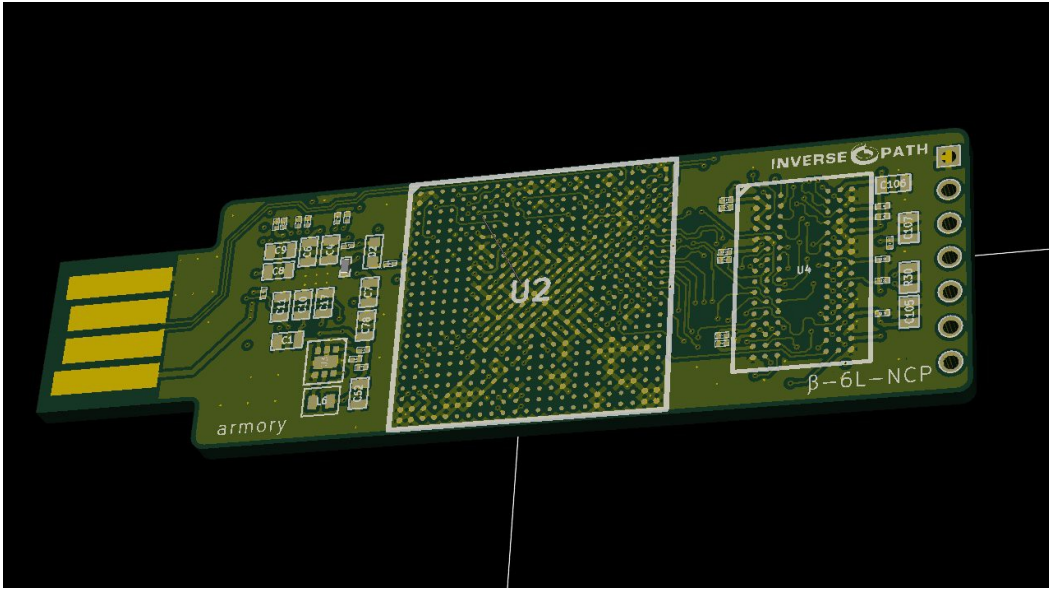




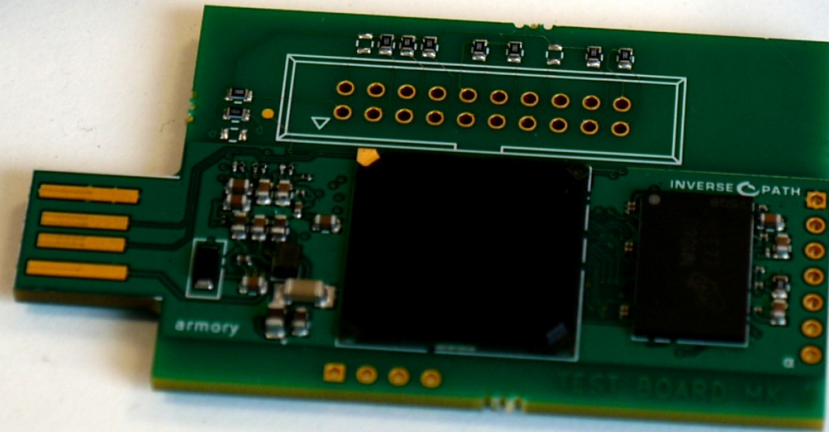




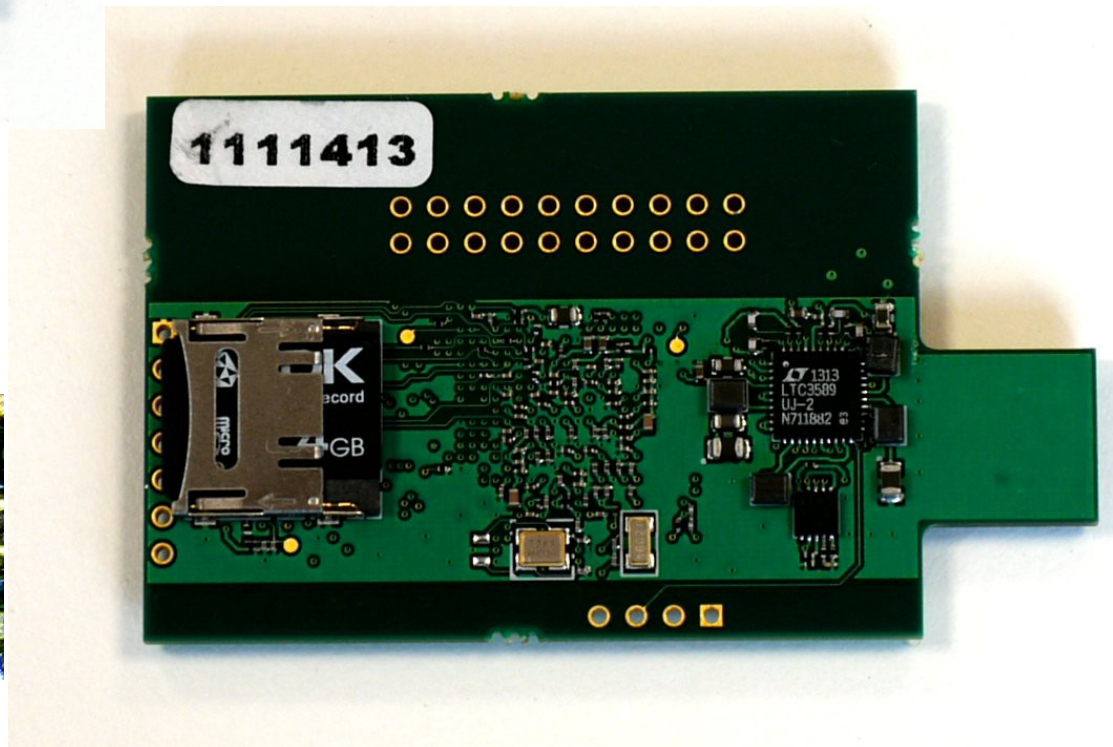
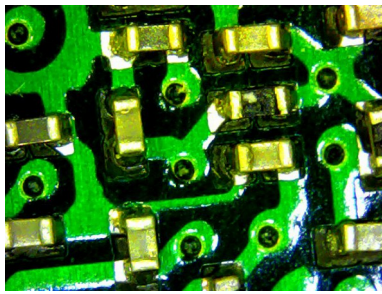
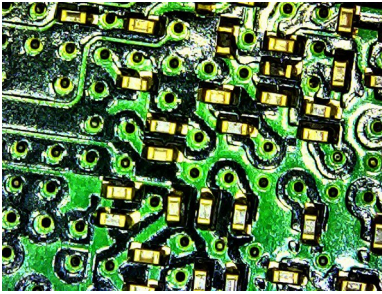
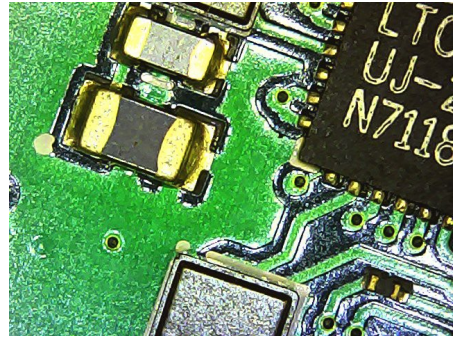
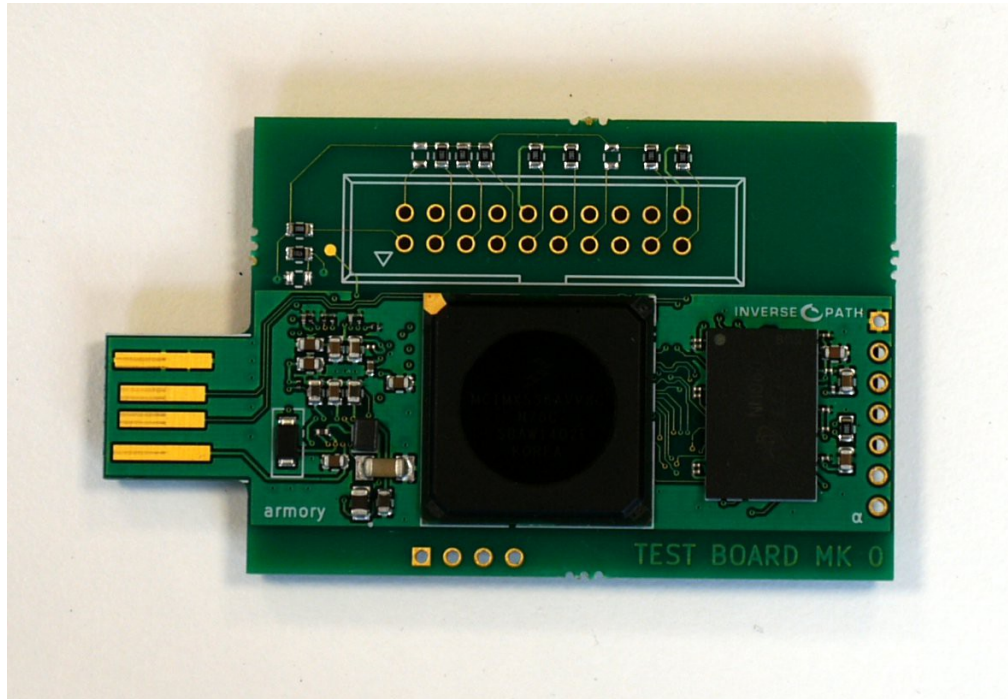




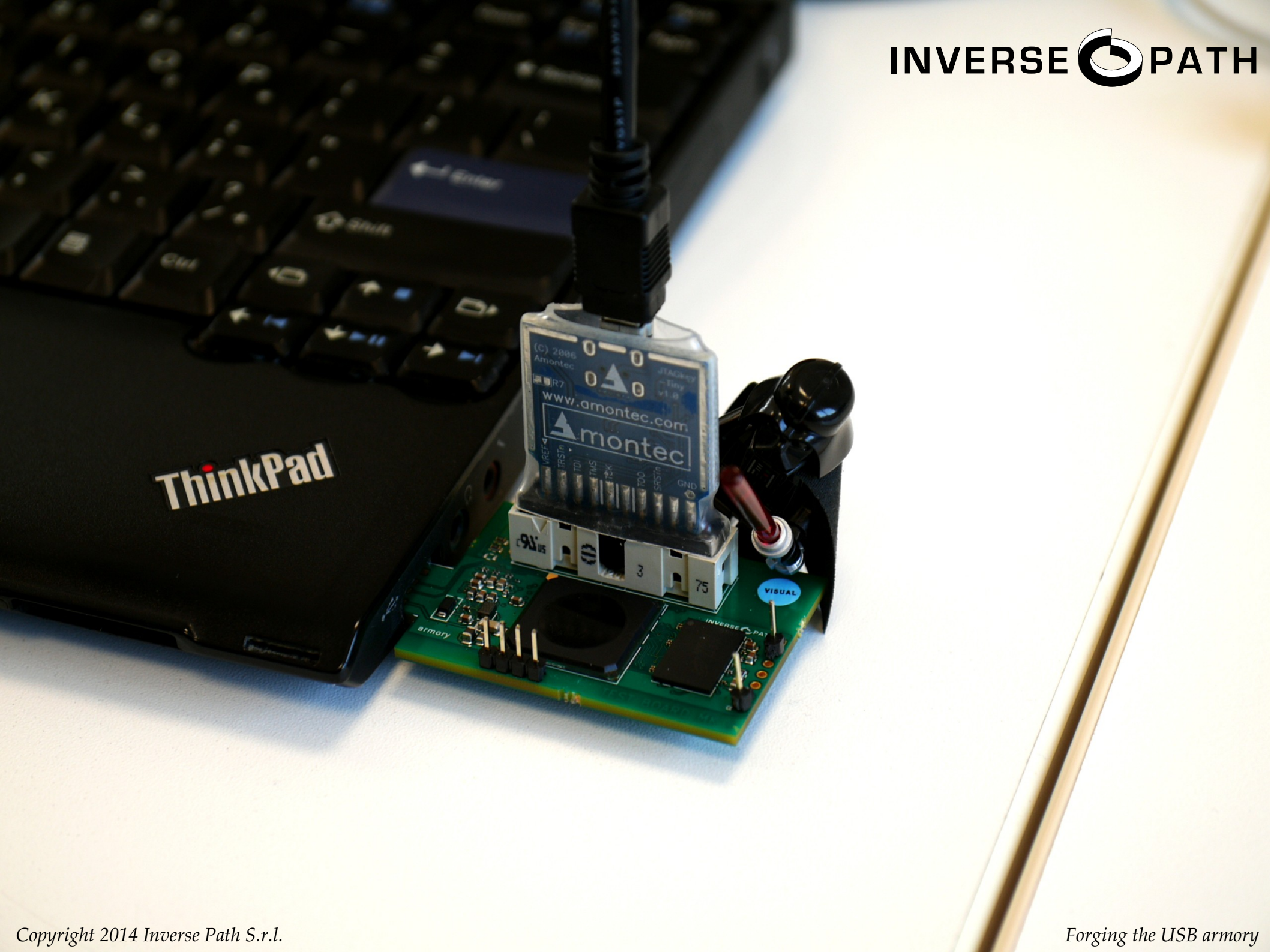












ThinkPad

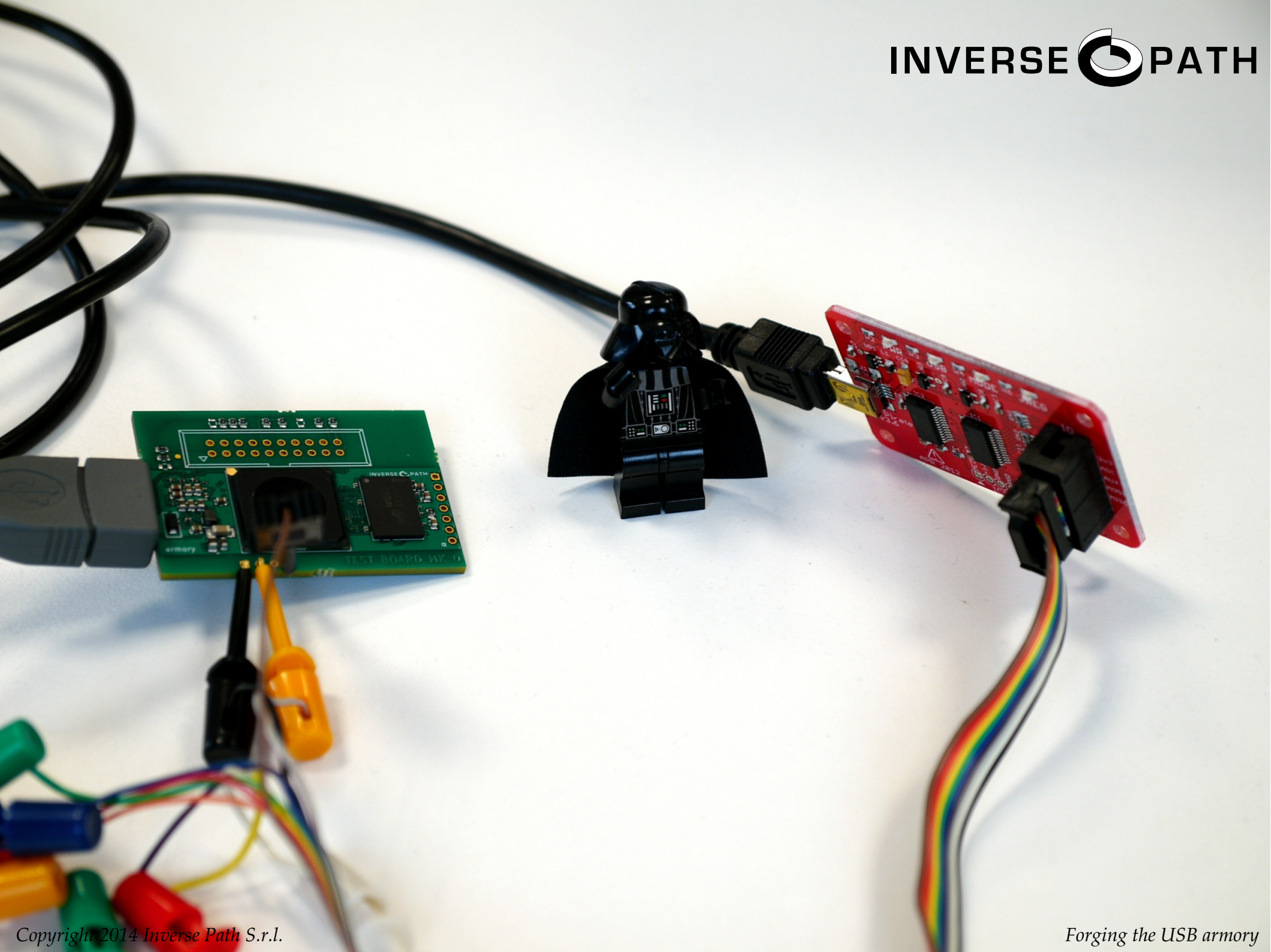
(C) 2006  
Amontec  
www.amontec.com  
montec

VISUAL

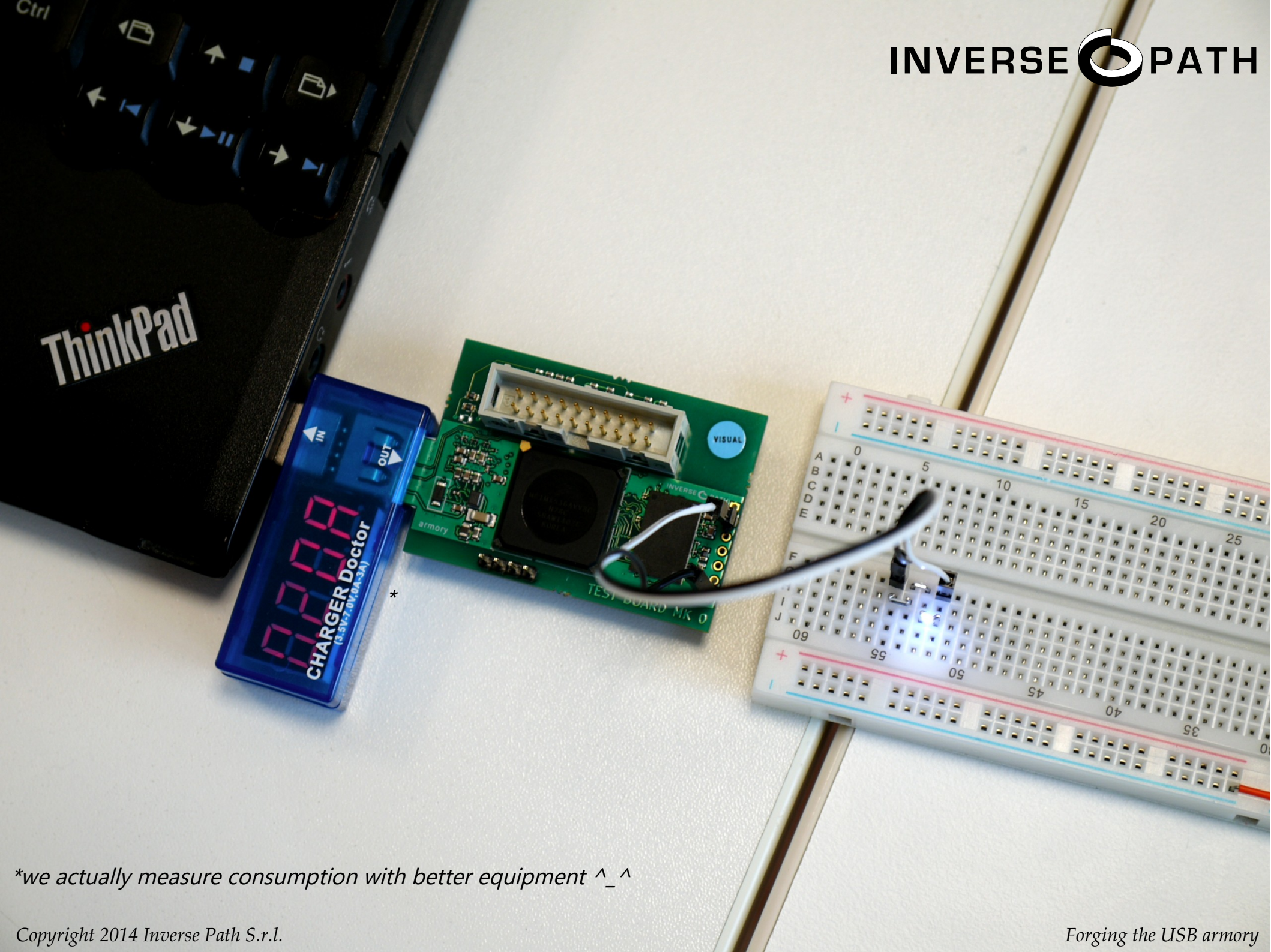
armory

INVERSE PATH










ThinkPad

CHARGER Doctor  
(3.3V, 7.0V, 1A-3A)

armory  
TEST BOARD MK 0  
INVERSE   
VISUAL

0 5 10 15 20 25  
A B C D E  
F  
09  
55  
50  
45  
40  
35  
10

*\*we actually measure consumption with better equipment ^\_^*



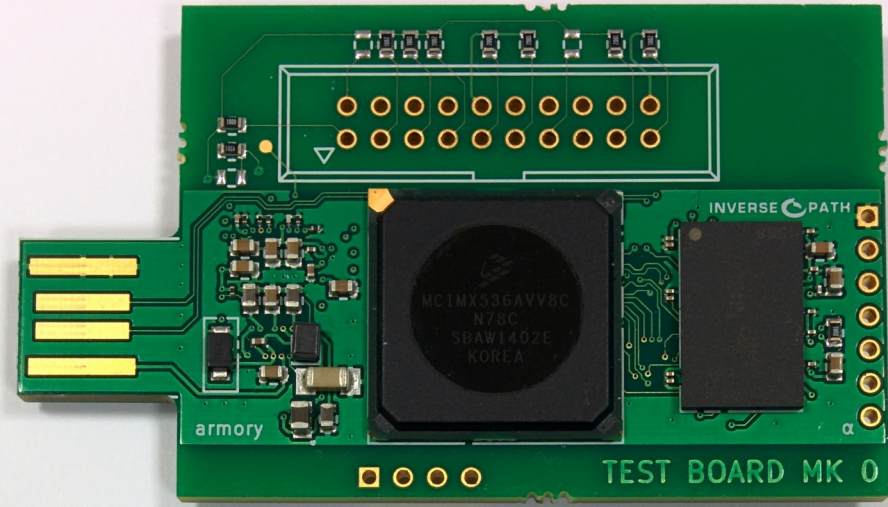






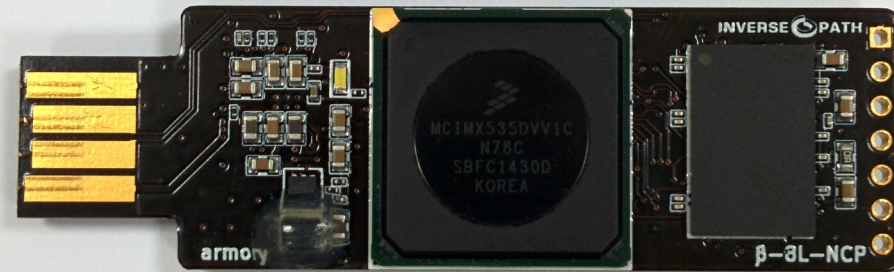


$\alpha$

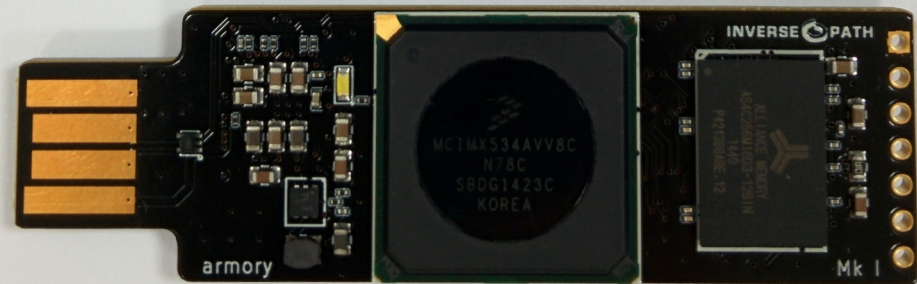


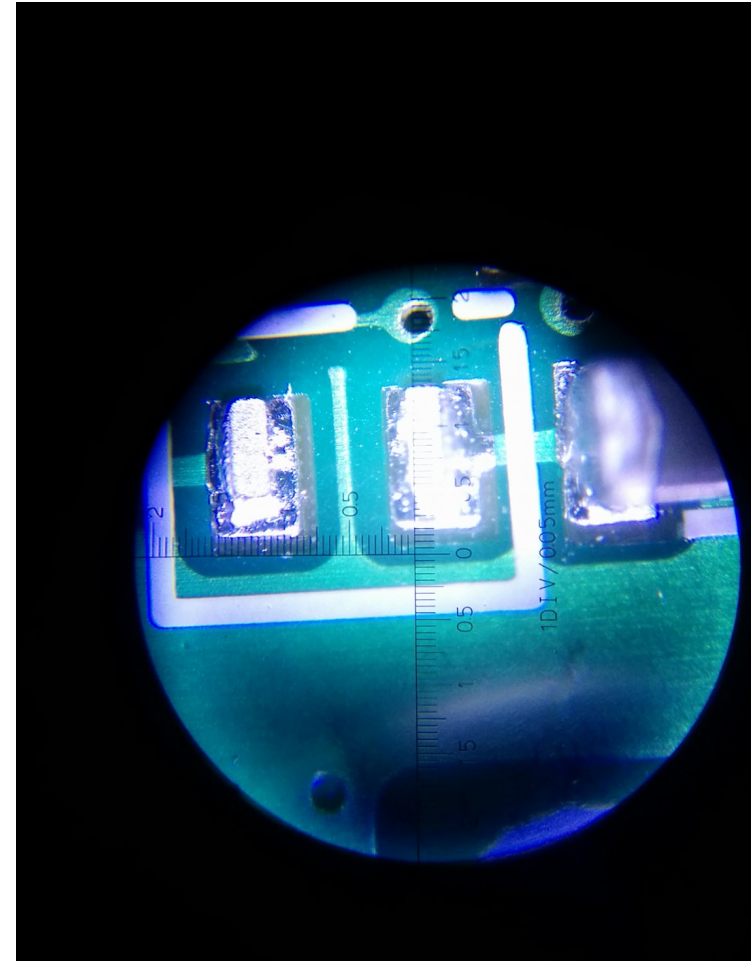
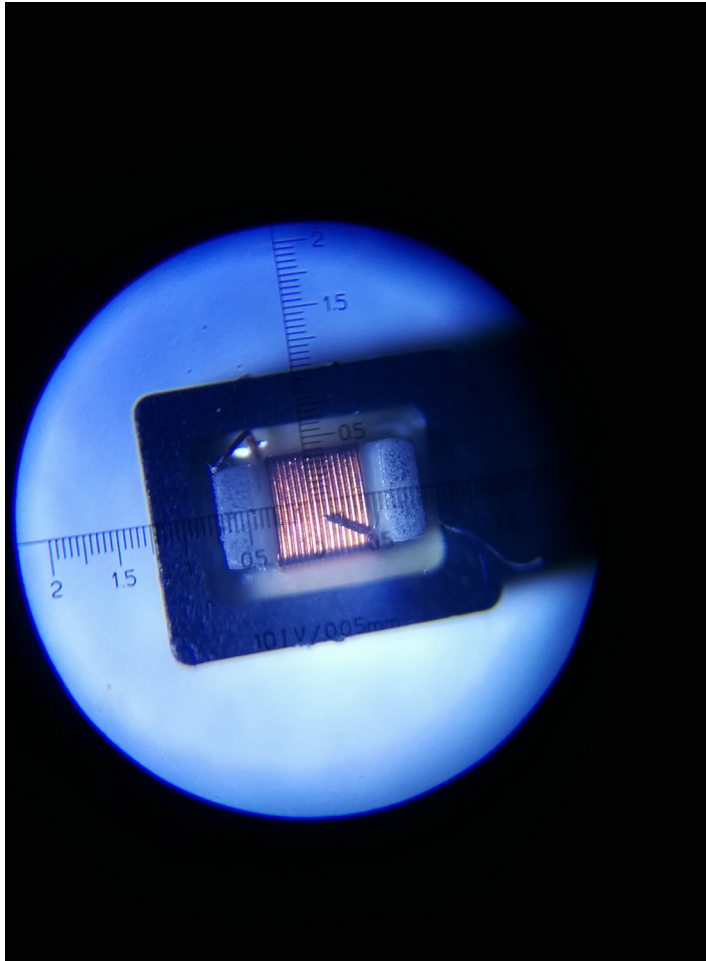
$\beta s$

8L-NOUSBH,8L, 8L-DDR-LDO, 8L-DDR-NCP  
6L, 6L-DDR-LDO, 6L-DDR-NCP



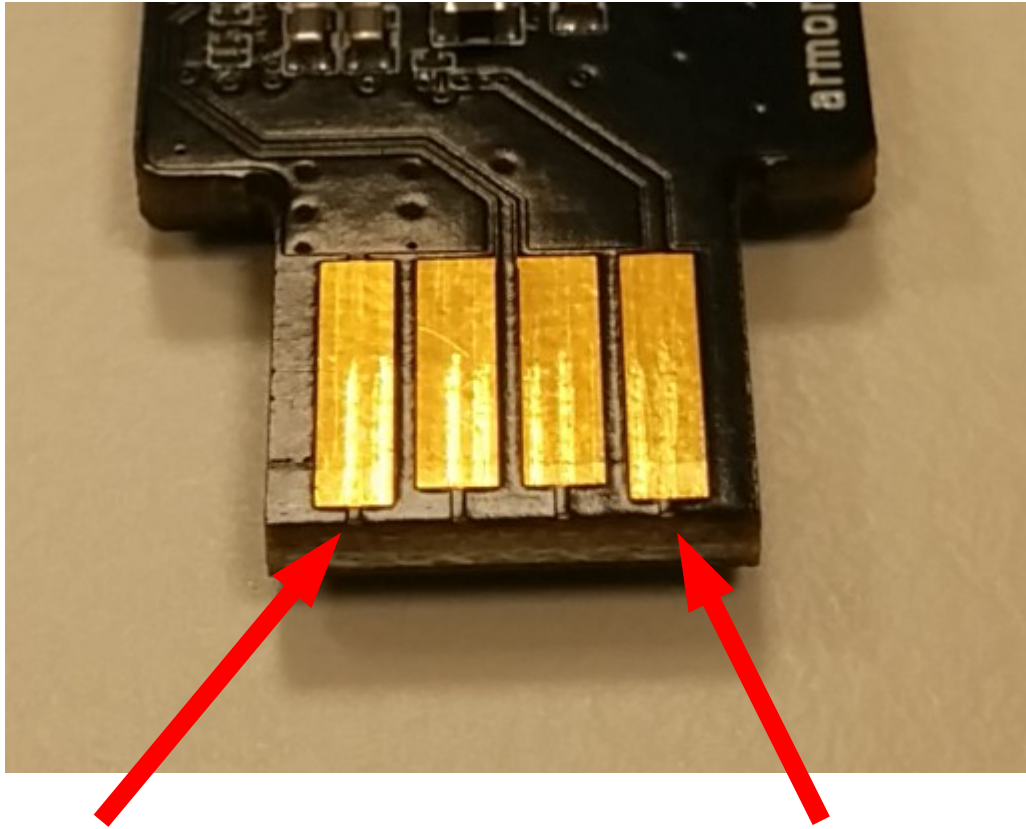
Mk I



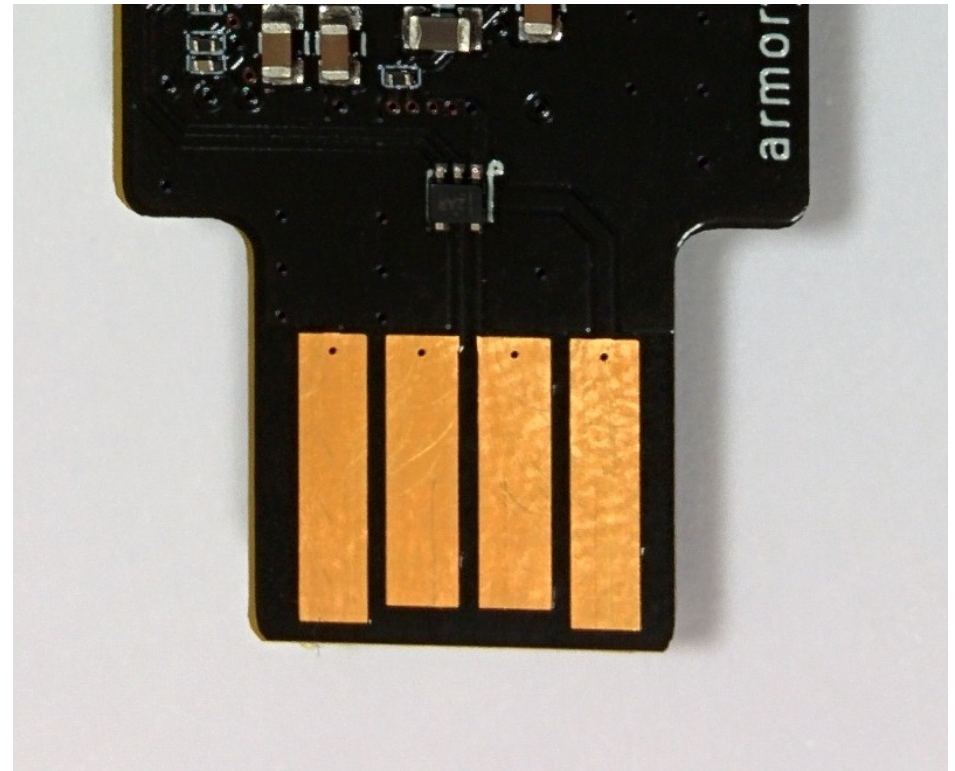


lessons learned #1  
tiny inductors are fragile



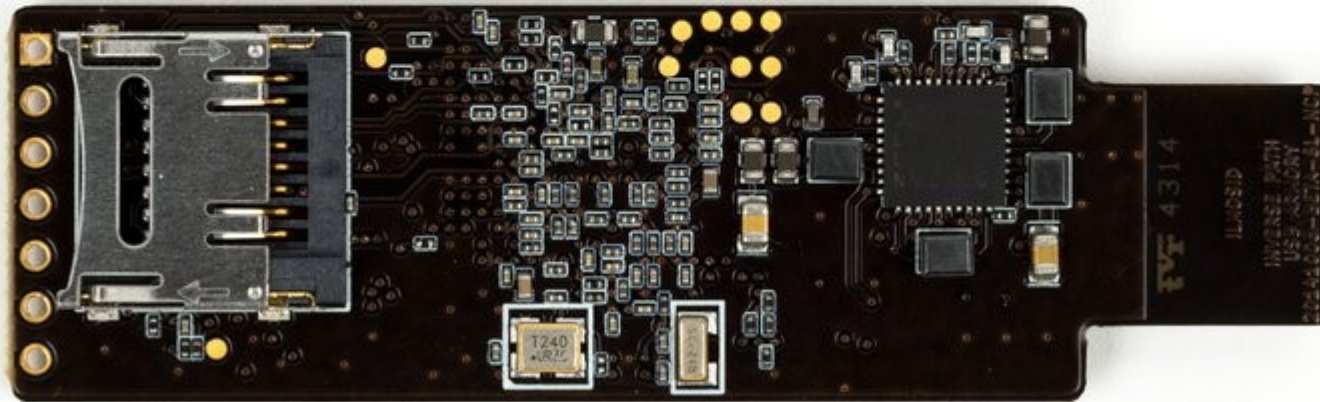


evil



good

lessons learned #2 (the five-second rule)  
gold plating traces cause under-voltage on hot swap



Thank you!

Q & A

Andrea Barisani

<[andrea@inversepath.com](mailto:andrea@inversepath.com)>

