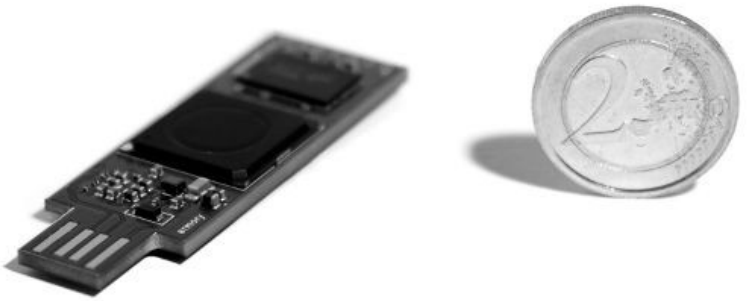
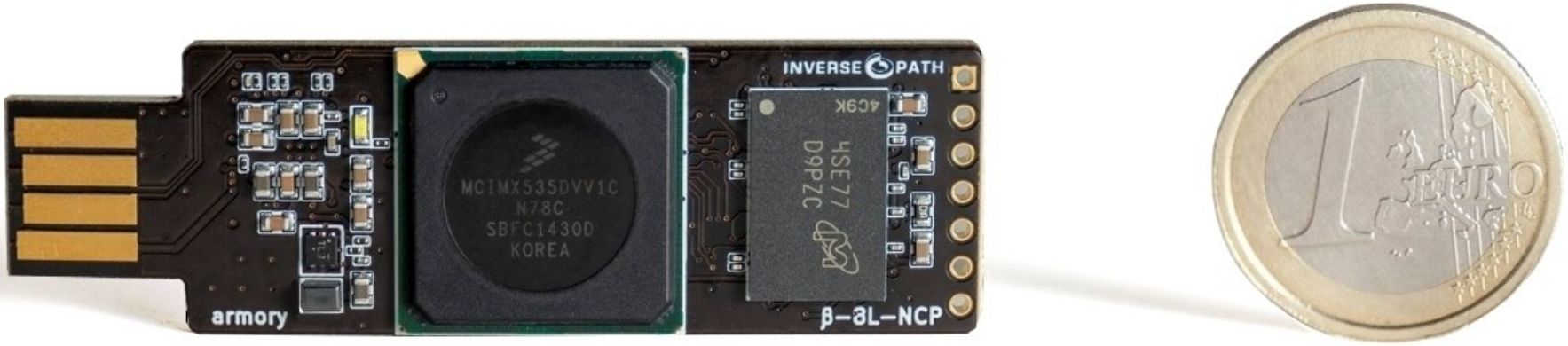
INVERSE PATH

Forging the USB armory

Andrea Barisani
<andrea@inversepath.com>



INVERSE PATH



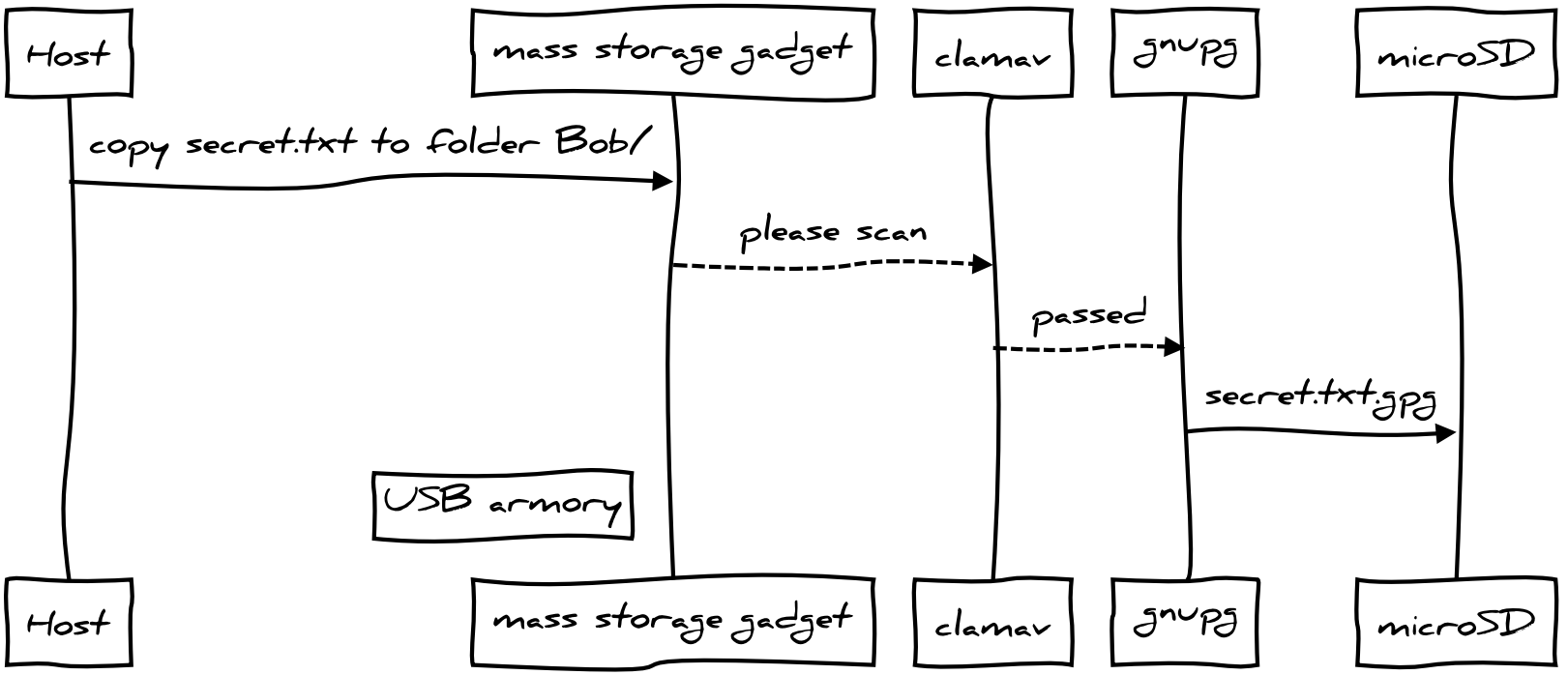
INVERSE PATH

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

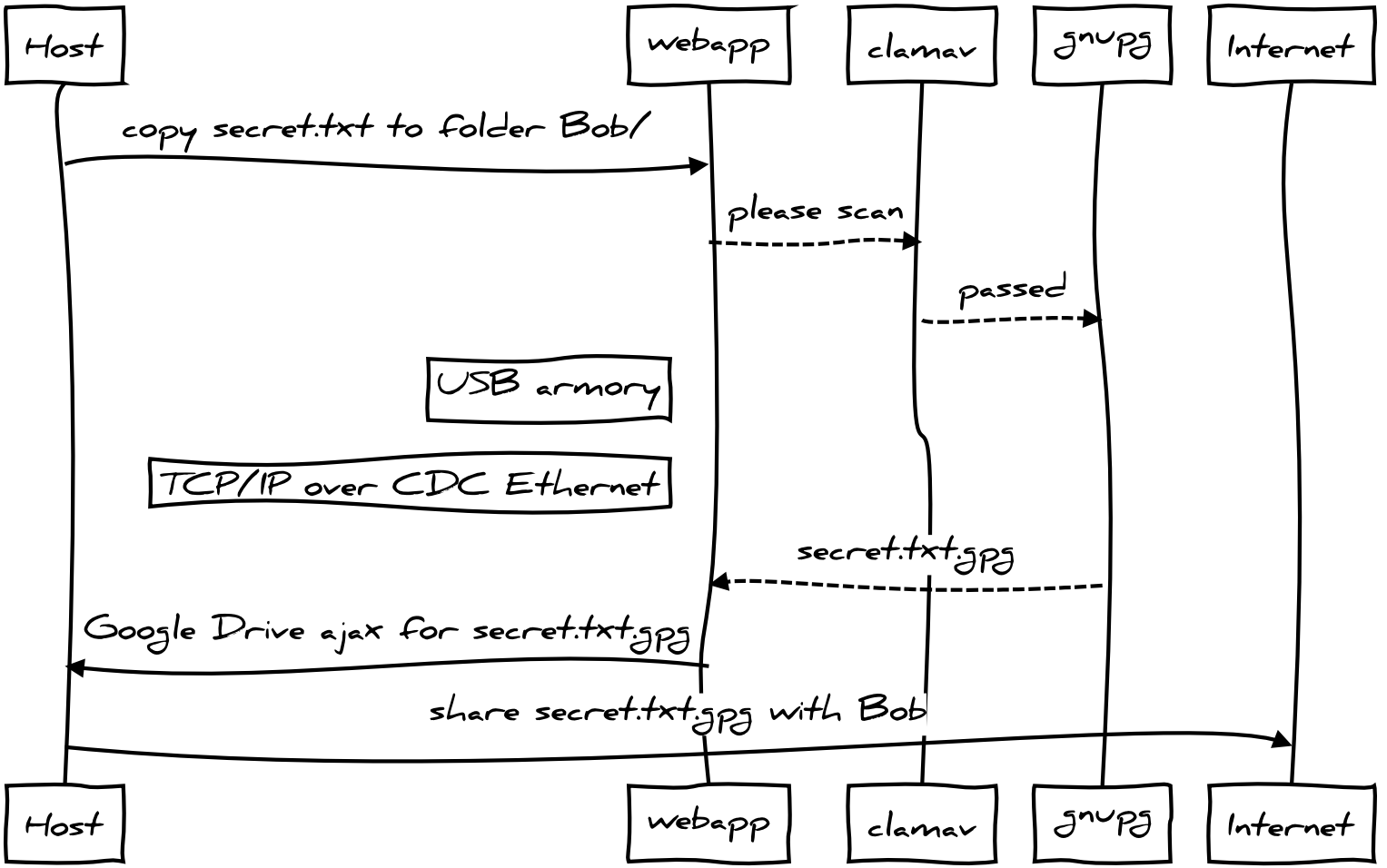
INVERSE PATH

enhanced mass storage



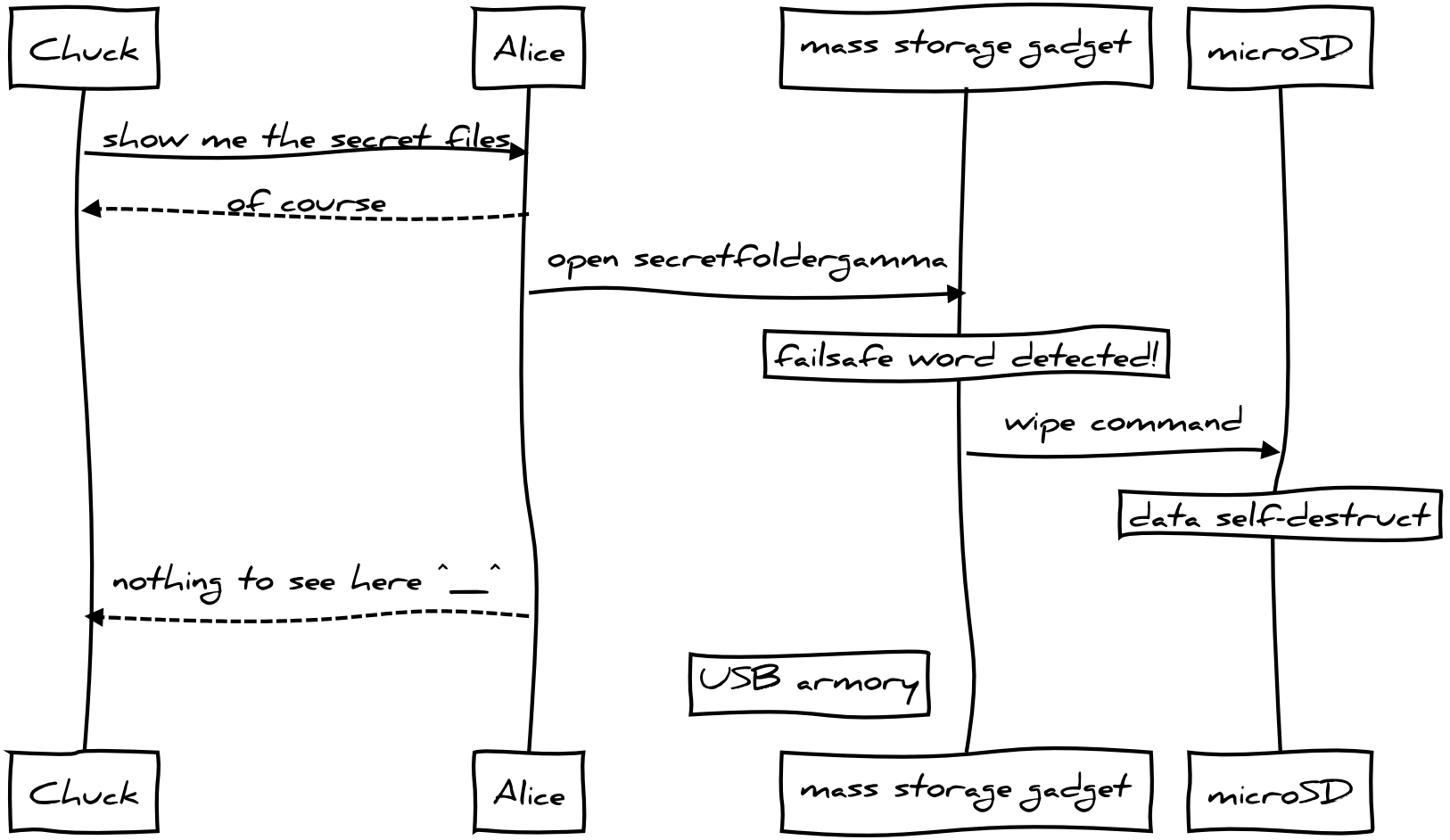
INVERSE PATH

enhanced mass storage



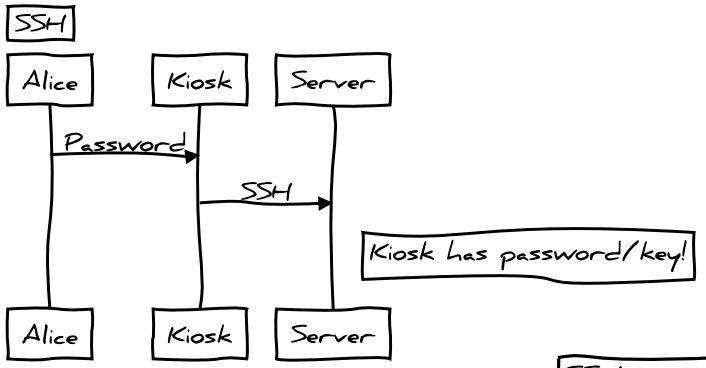
INVERSE PATH

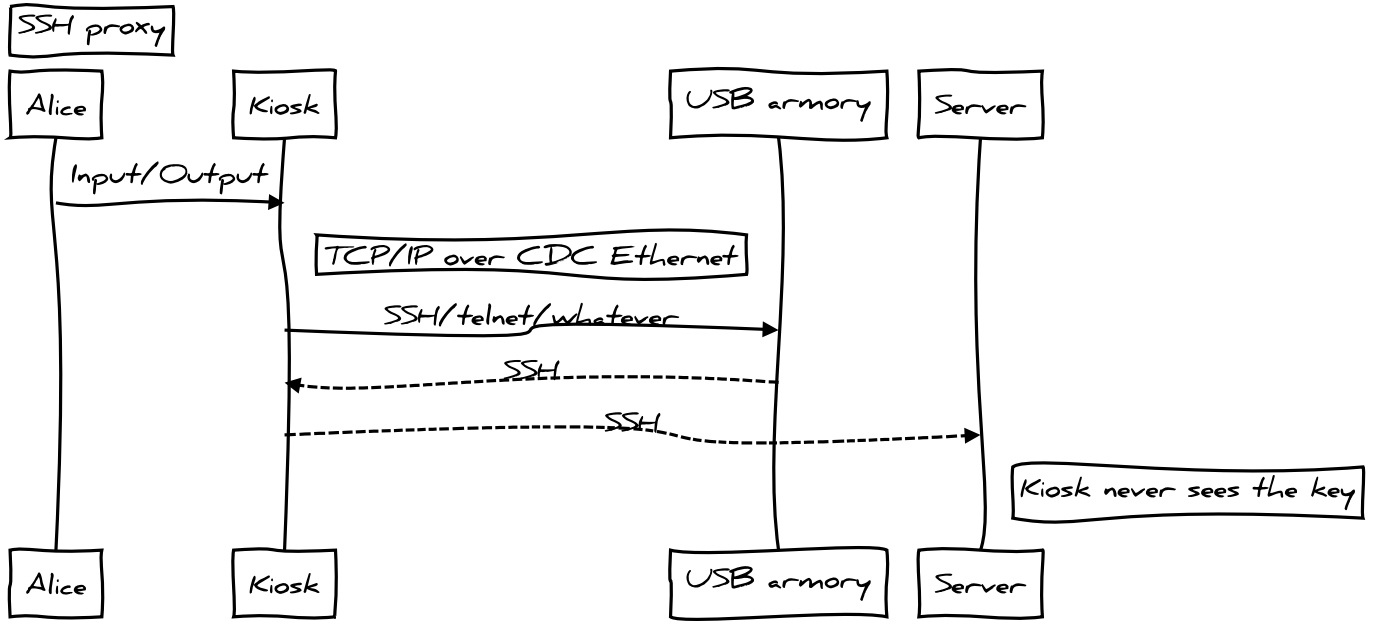
enhanced mass storage

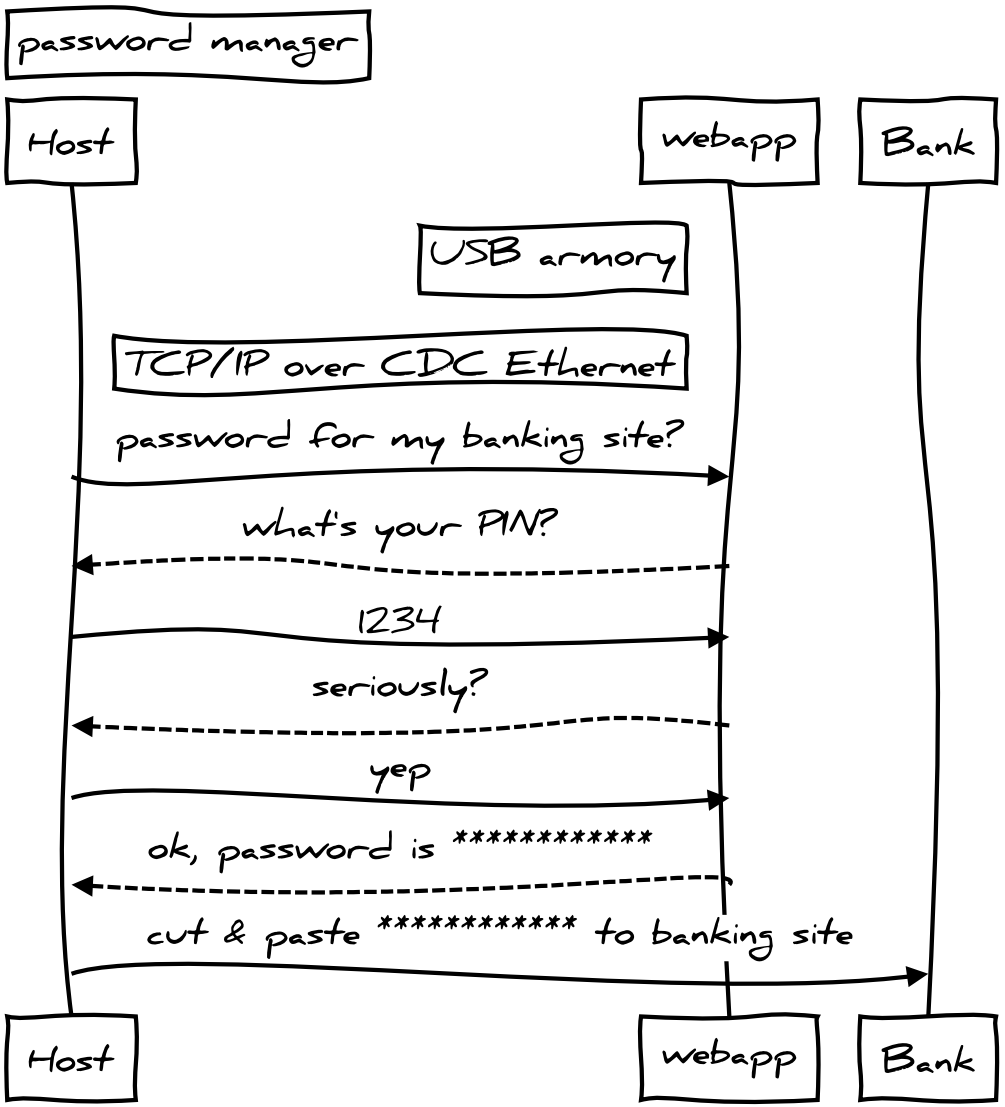


INVERSE PATH

SSH proxy





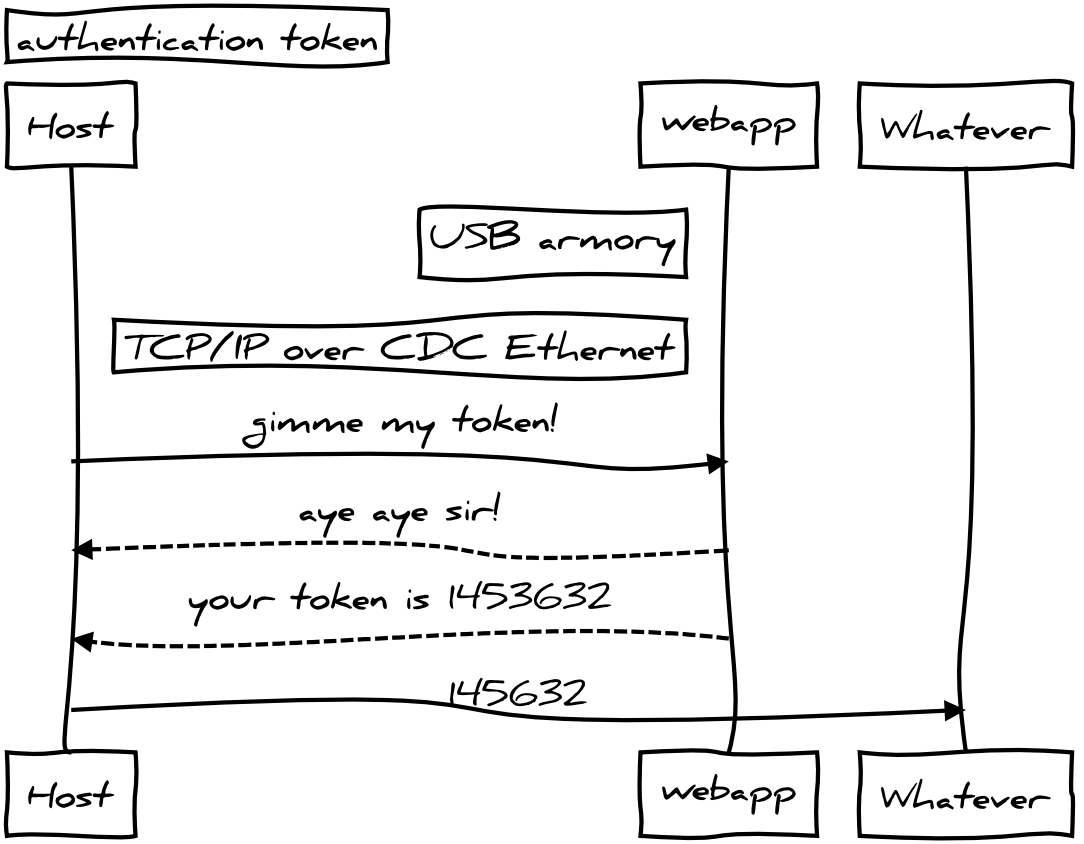


password manager

**trivial example, better options planned*

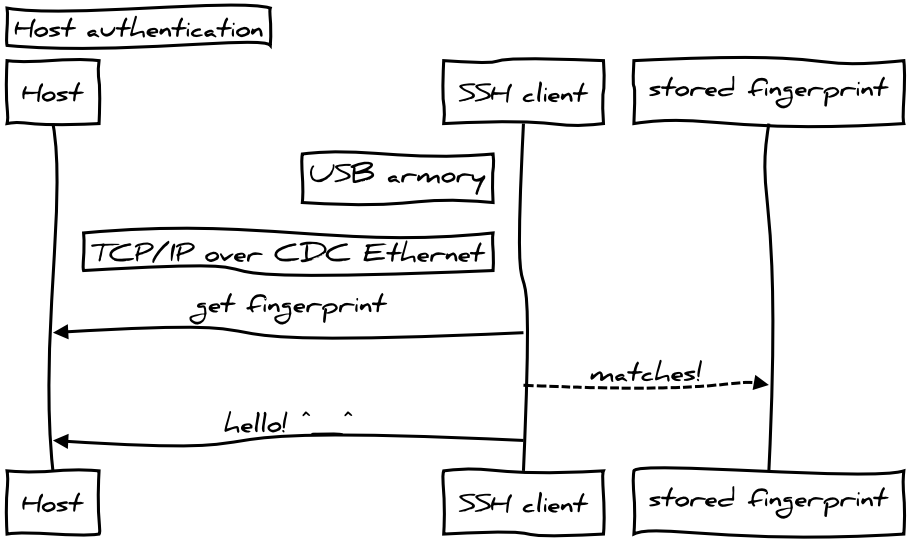
INVERSE PATH

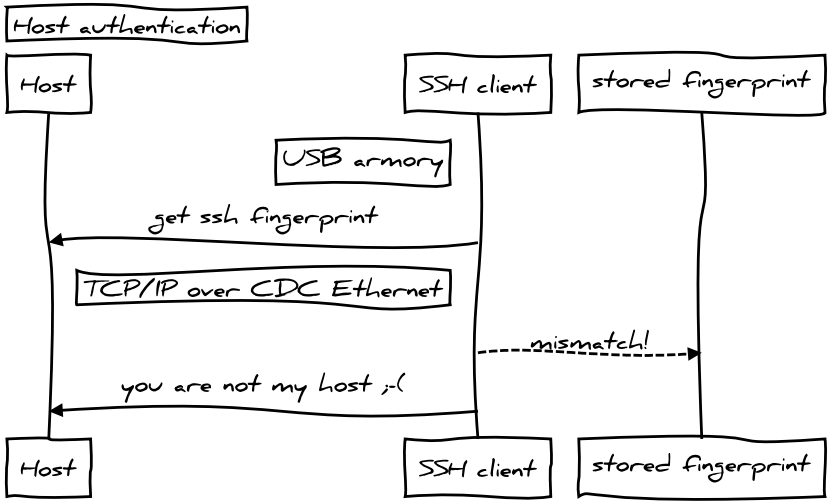
authentication token



INVERSE PATH

USB device authenticates host





INVERSE PATH

Design goals

Compact USB powered device

Fast CPU and generous RAM

Secure boot

Standard connectivity over USB

Familiar developing/execution environment

Open design

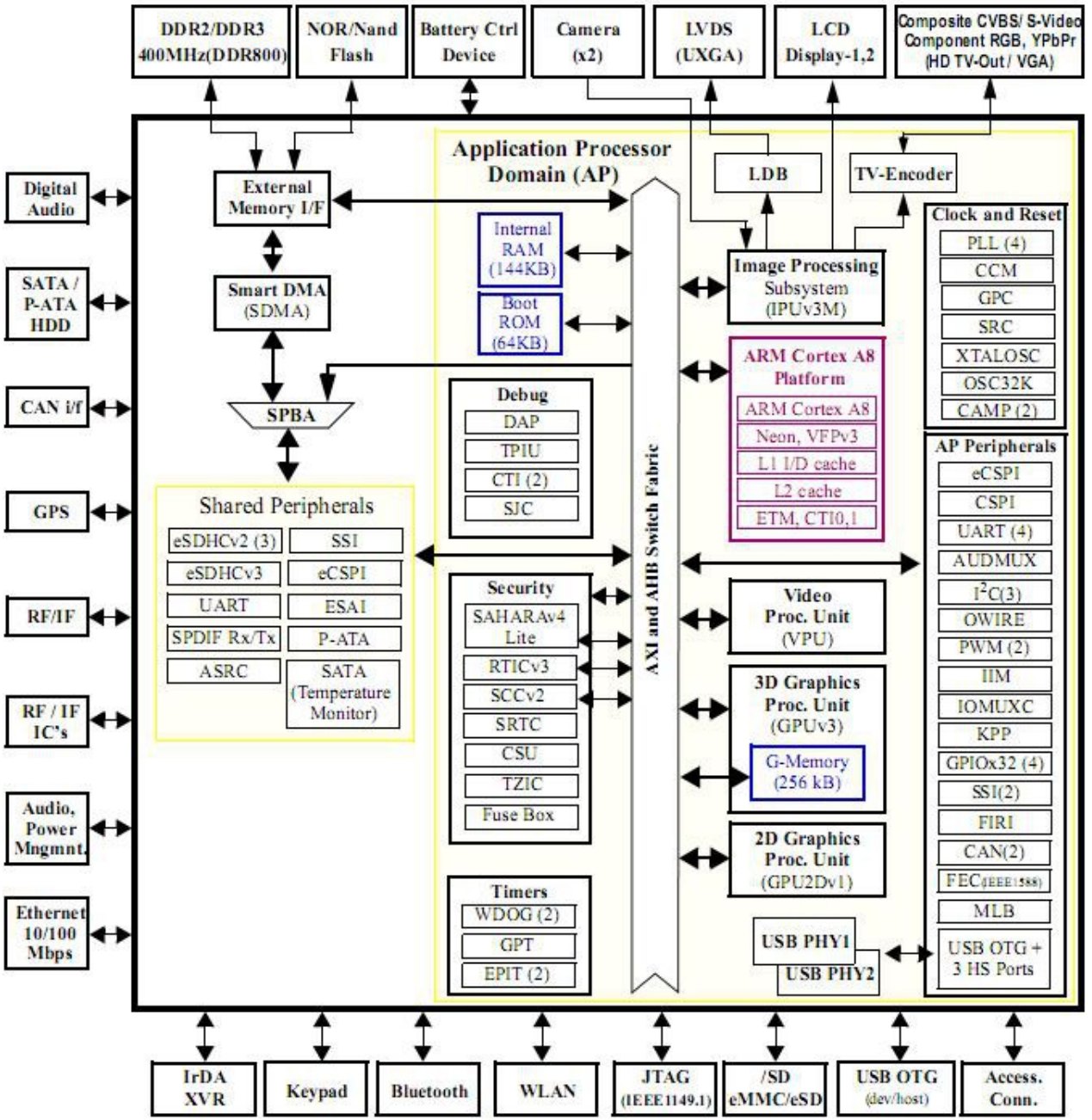
INVERSE PATH

Selecting the System on Chip (SoC)

Freescale i.MX53

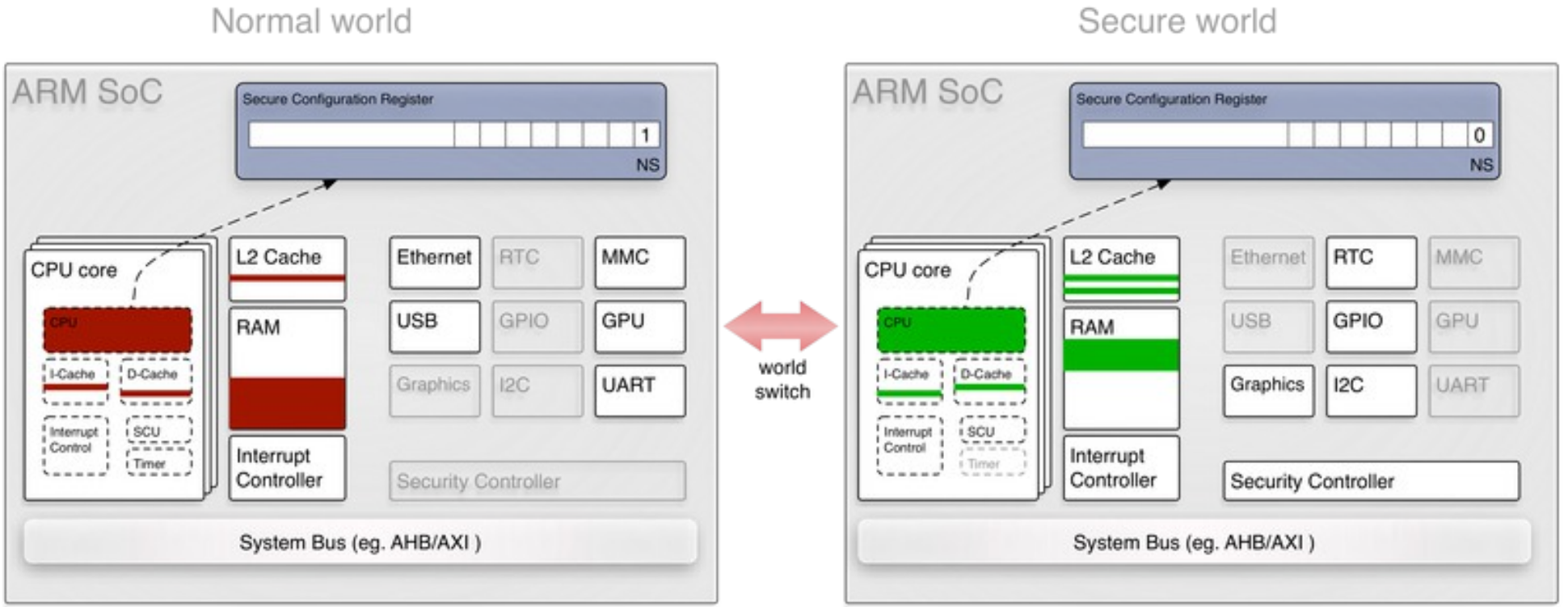
- ARM® Cortex™-A8 800-1200 Mhz
- almost all datasheets/manuals are public (no NDA required)
- Freescale datasheets are “ok” (far better than other vendors)
- ARM® TrustZone®, secure boot + storage + RAM
- detailed power consumption guide available
- excellent native support (Android, Debian, Ubuntu,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

INVERSE PATH



INVERSE PATH

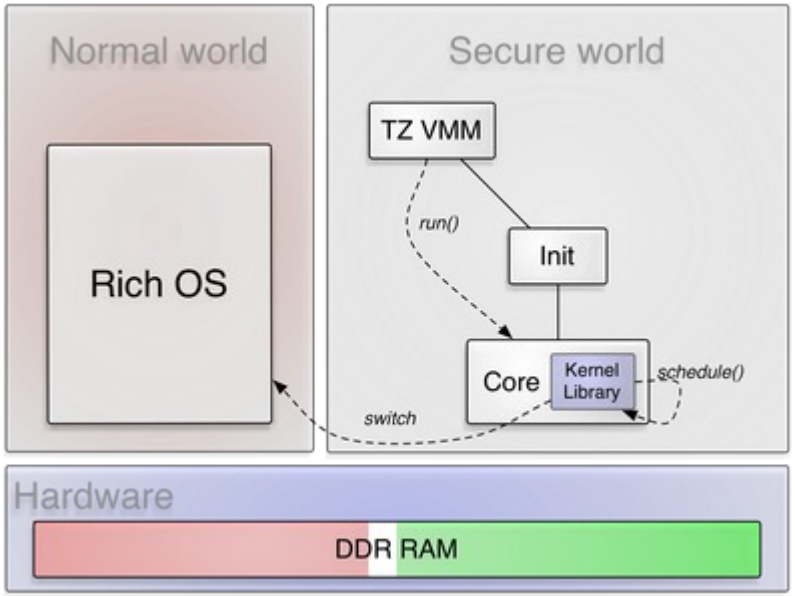
ARM® TrustZone®

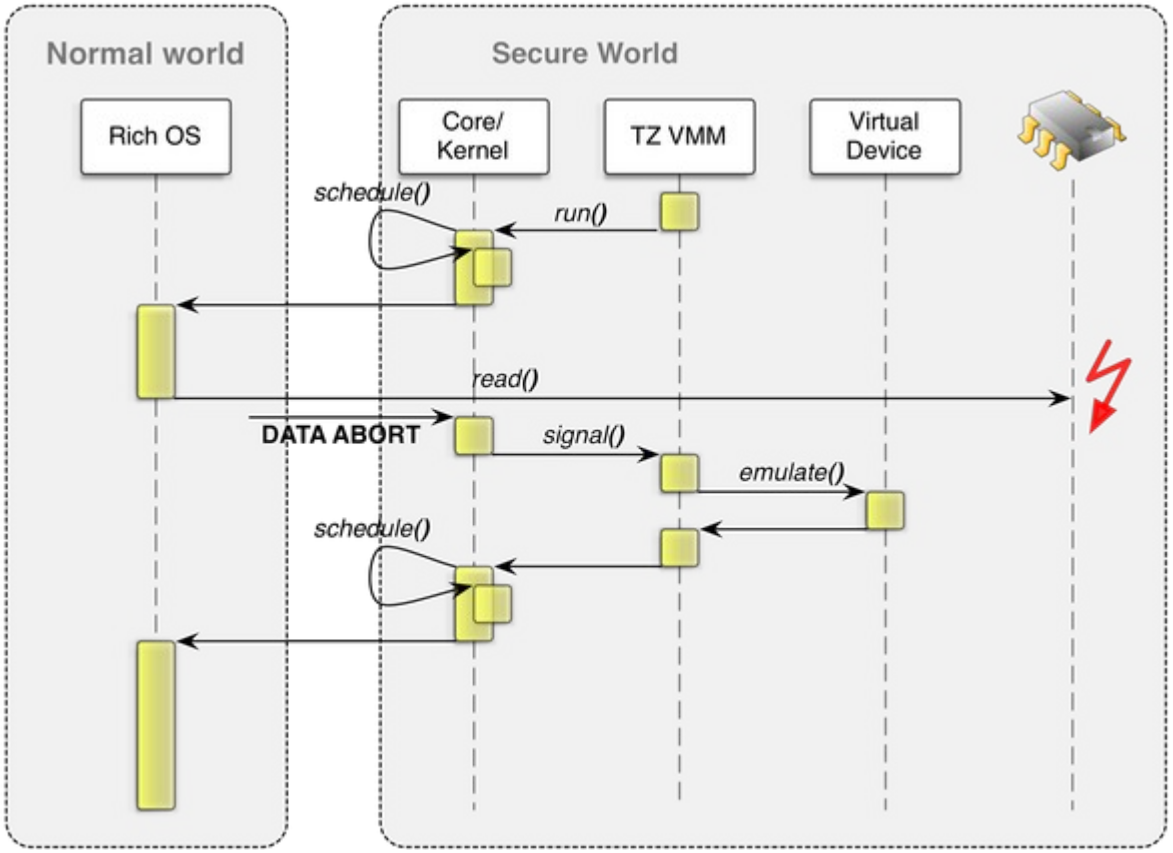


http://genode.org/documentation/articles/trustzone

INVERSE PATH

ARM® TrustZone®





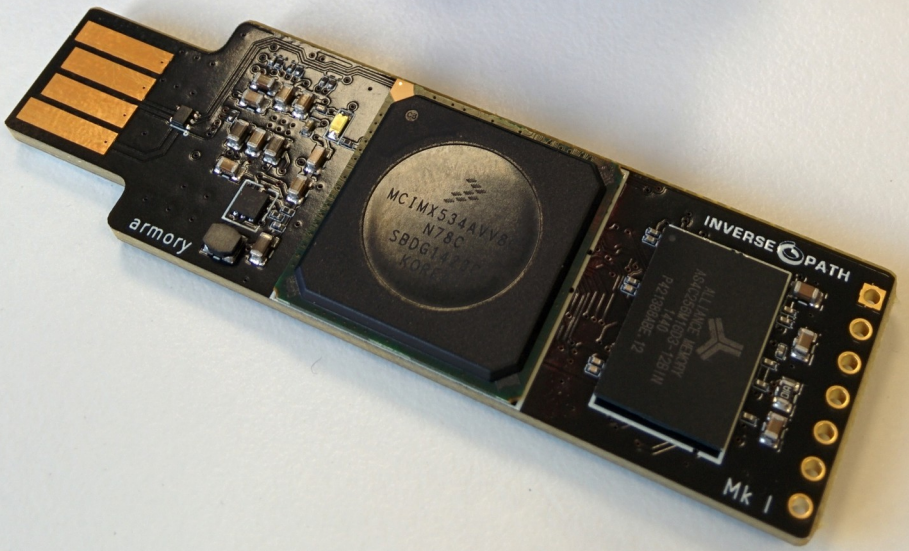
http://genode.org/documentation/articles/trustzone

INVERSE PATH

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

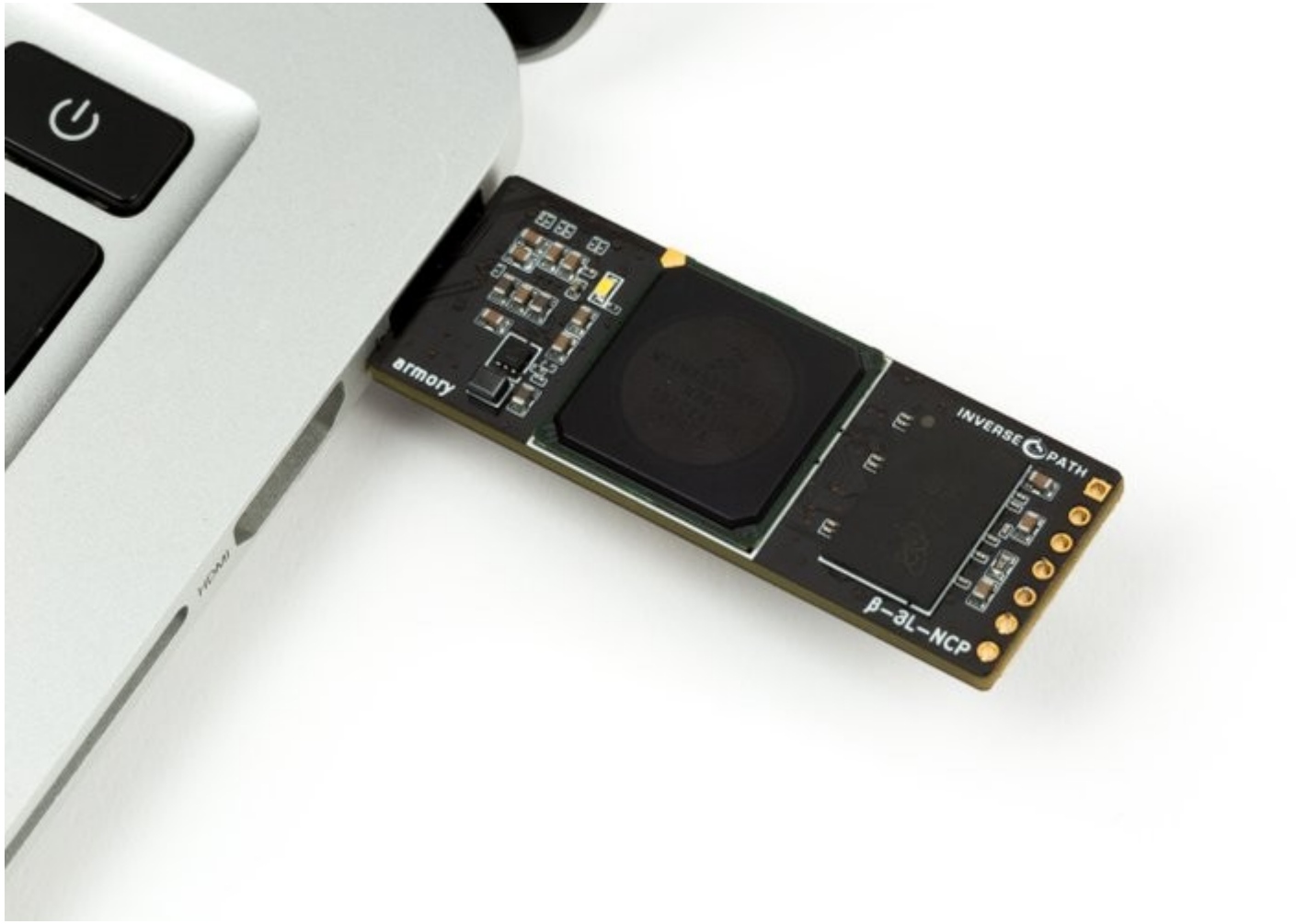
http://inversepath.com/usbarmory

Forging the USB armory

INVERSE PATH

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

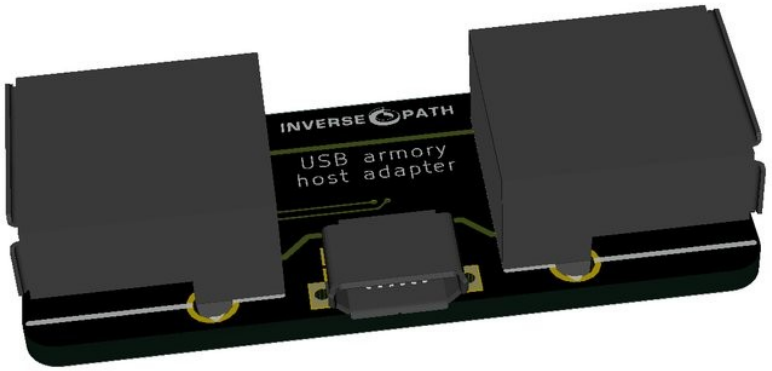


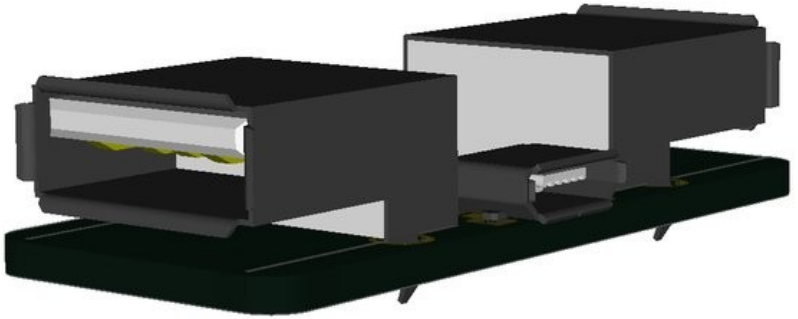
device mode

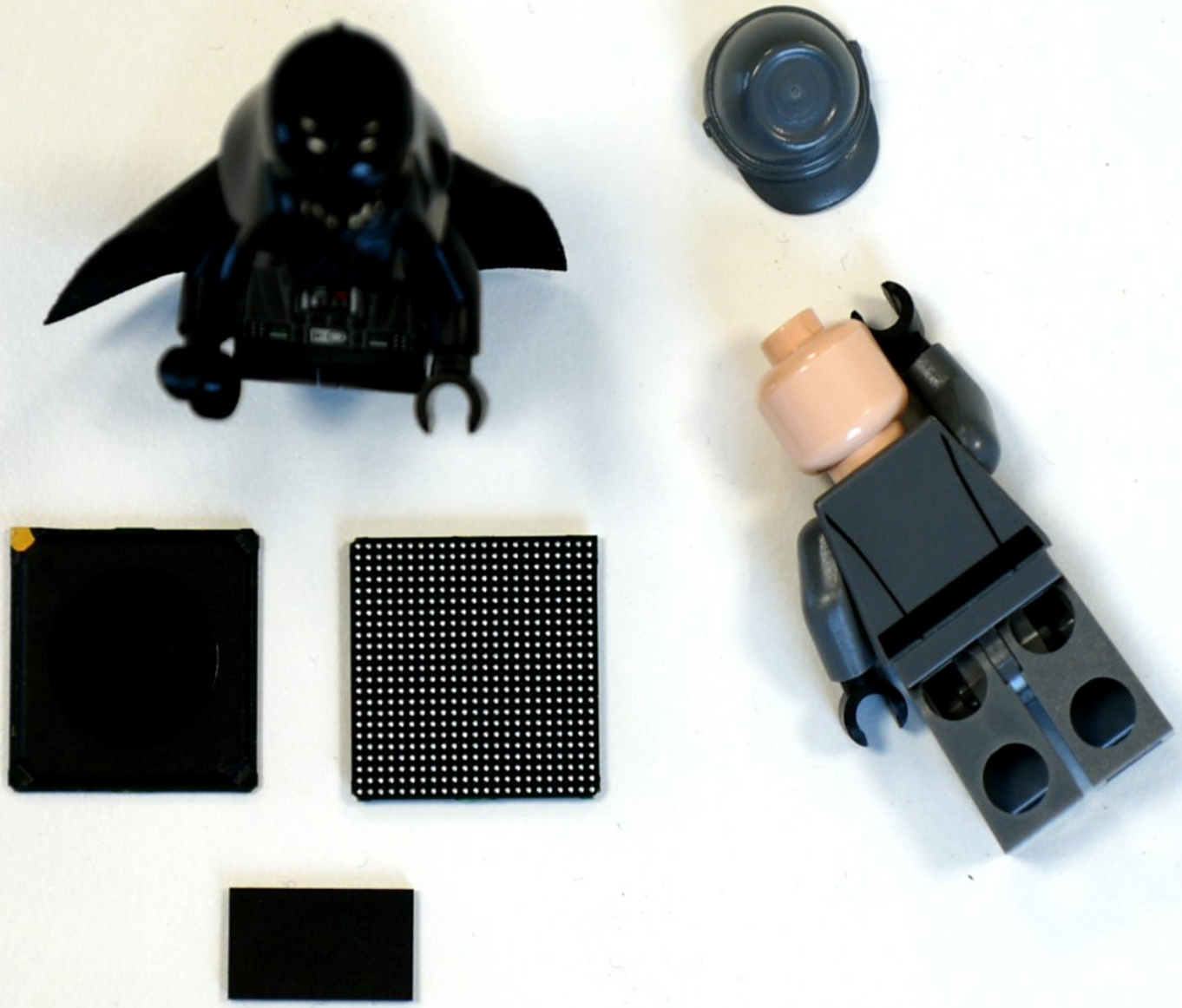
INVERSE PATH

INVERSE PATH

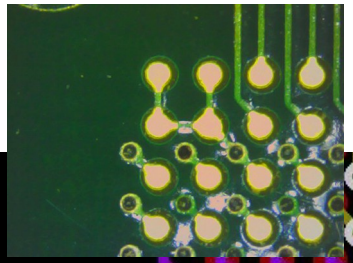
custom host adapter

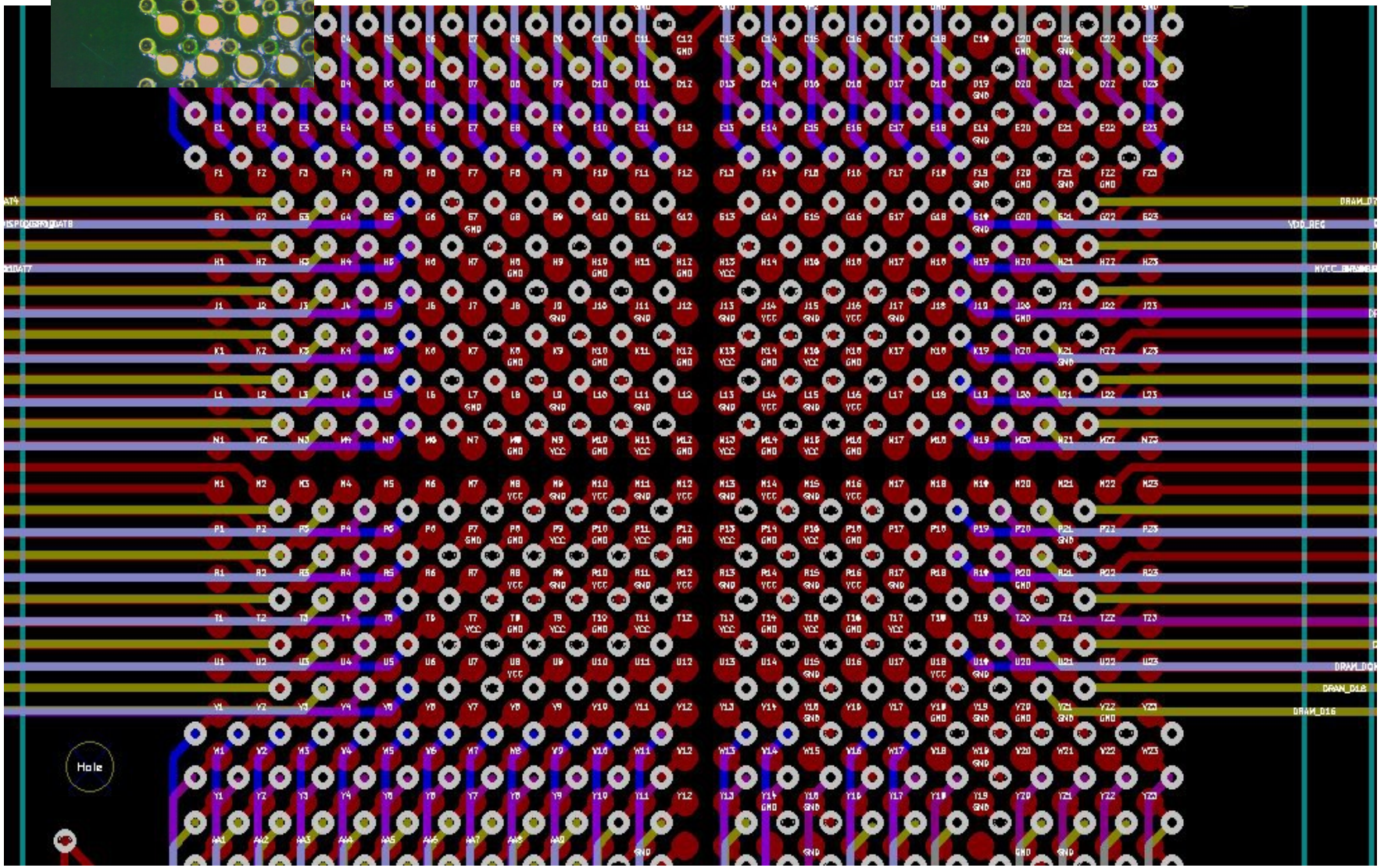




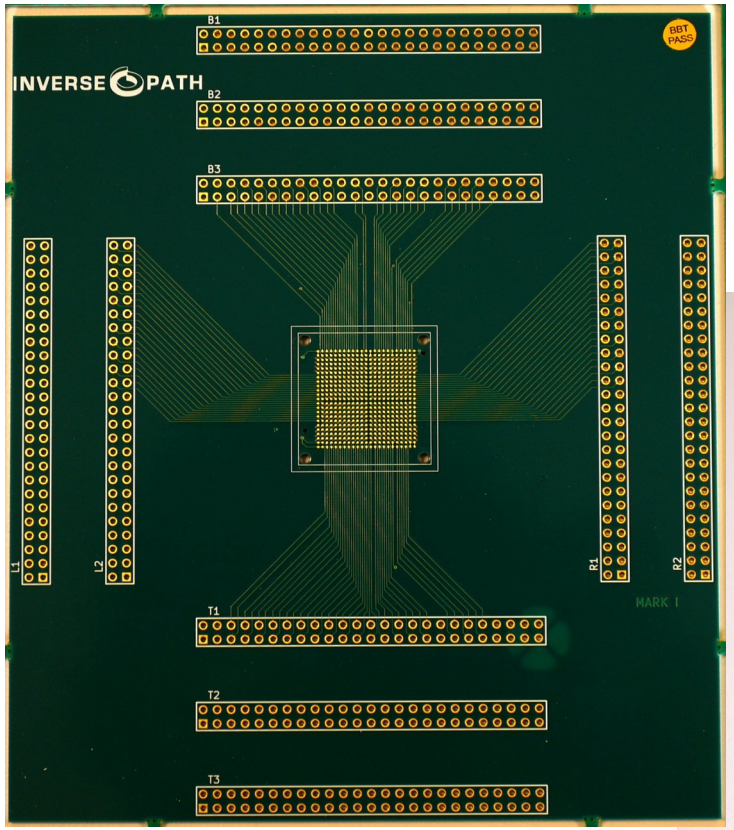


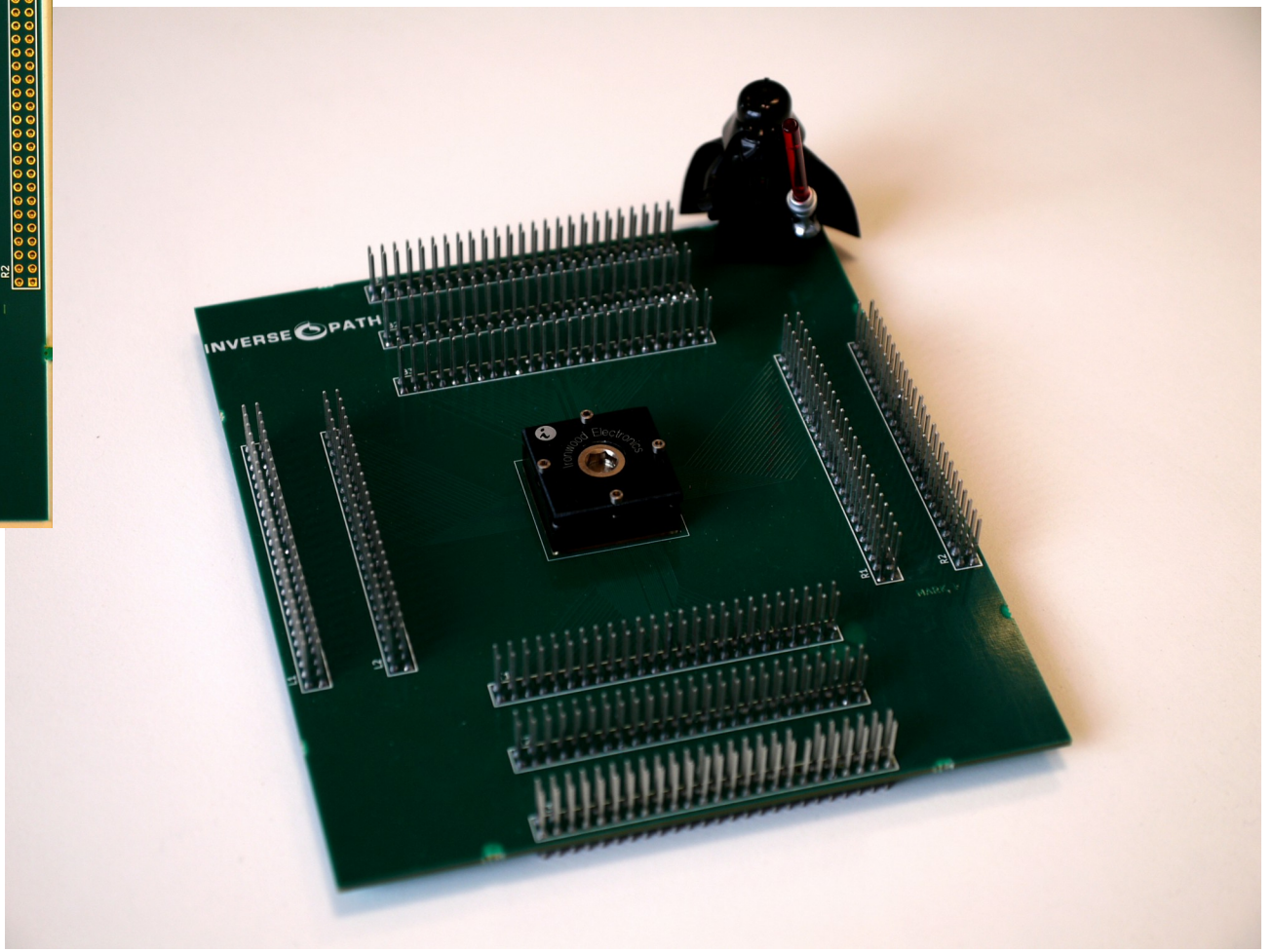
INVERSE PATH



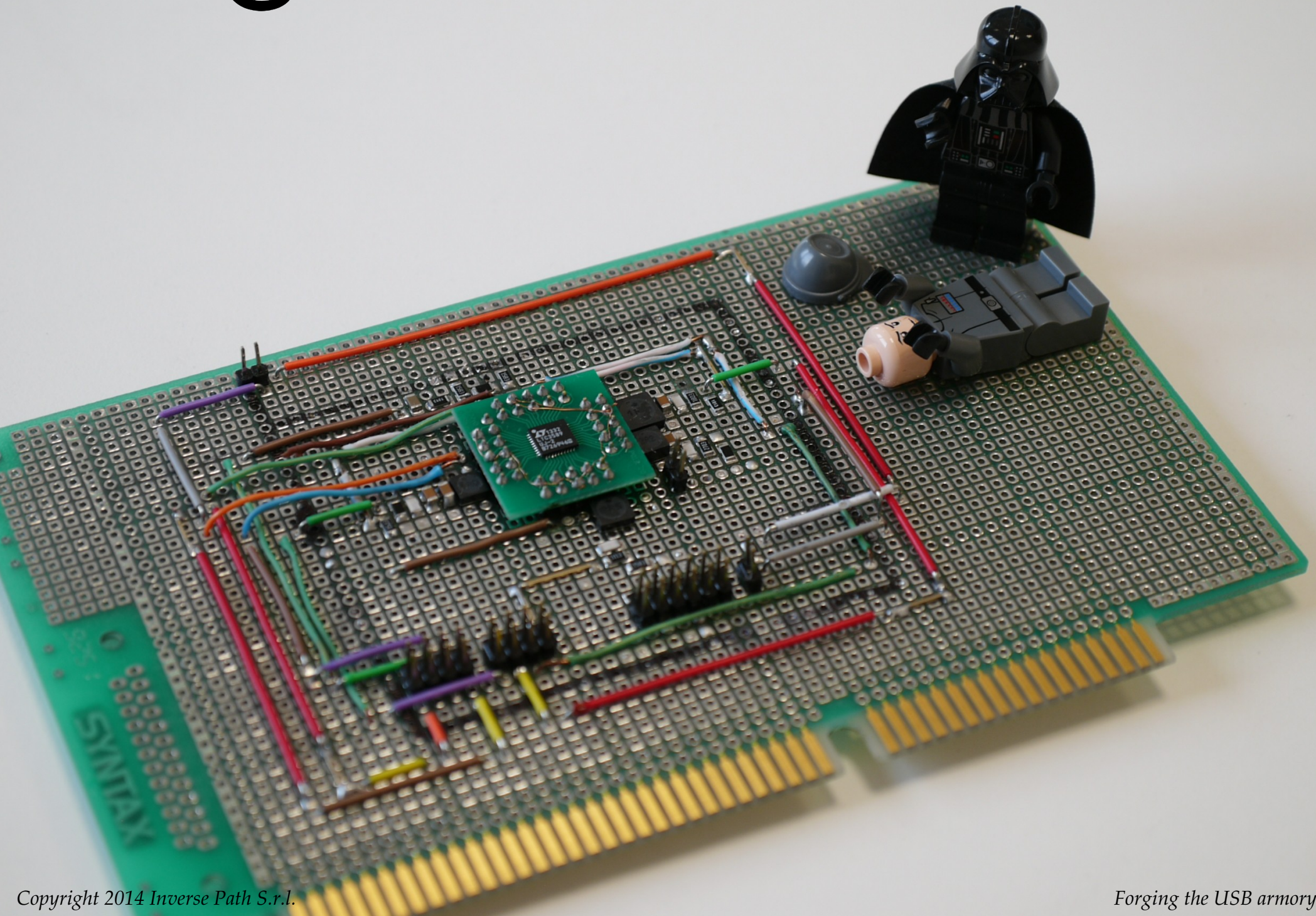


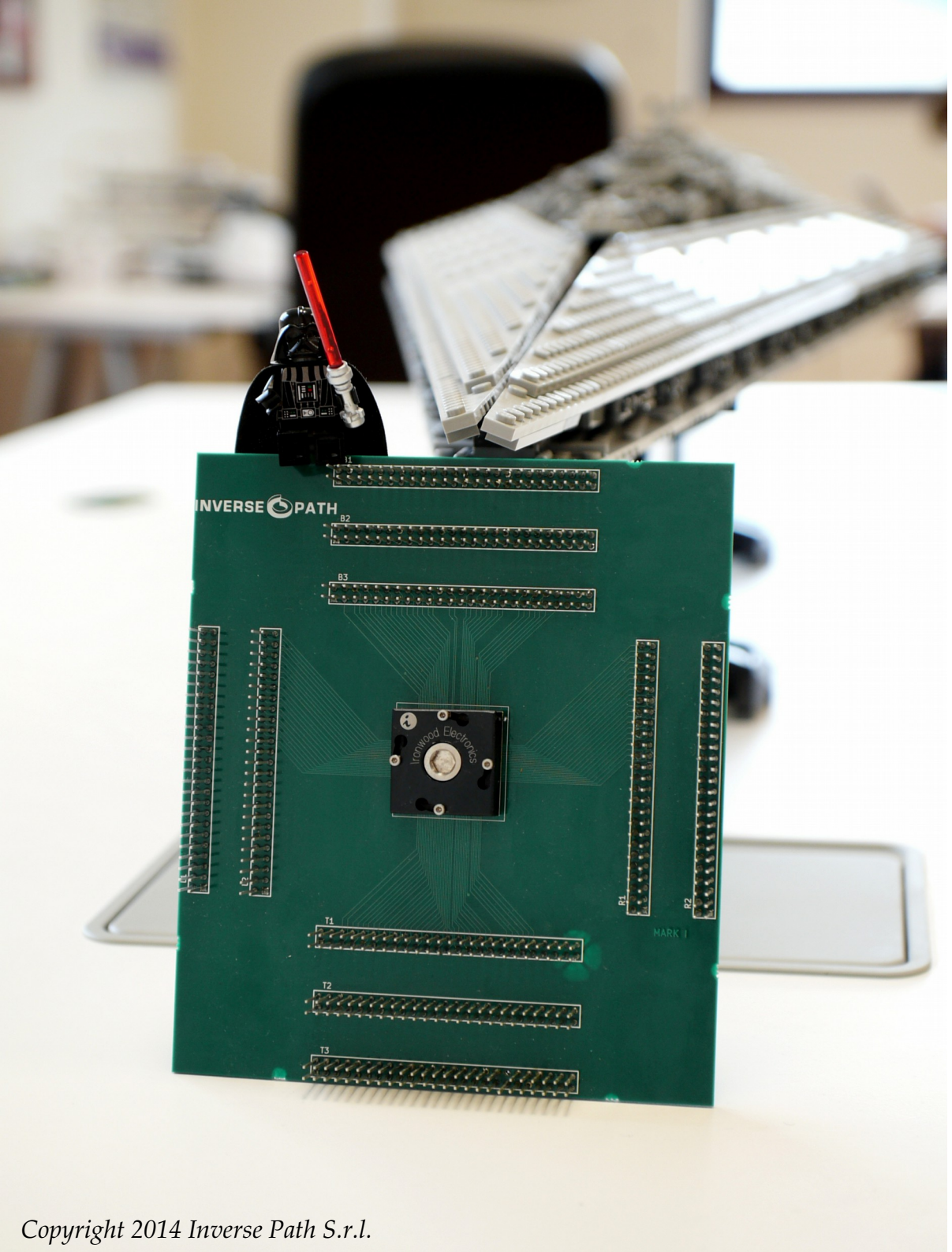
INVERSE PATH





INVERSE PATH

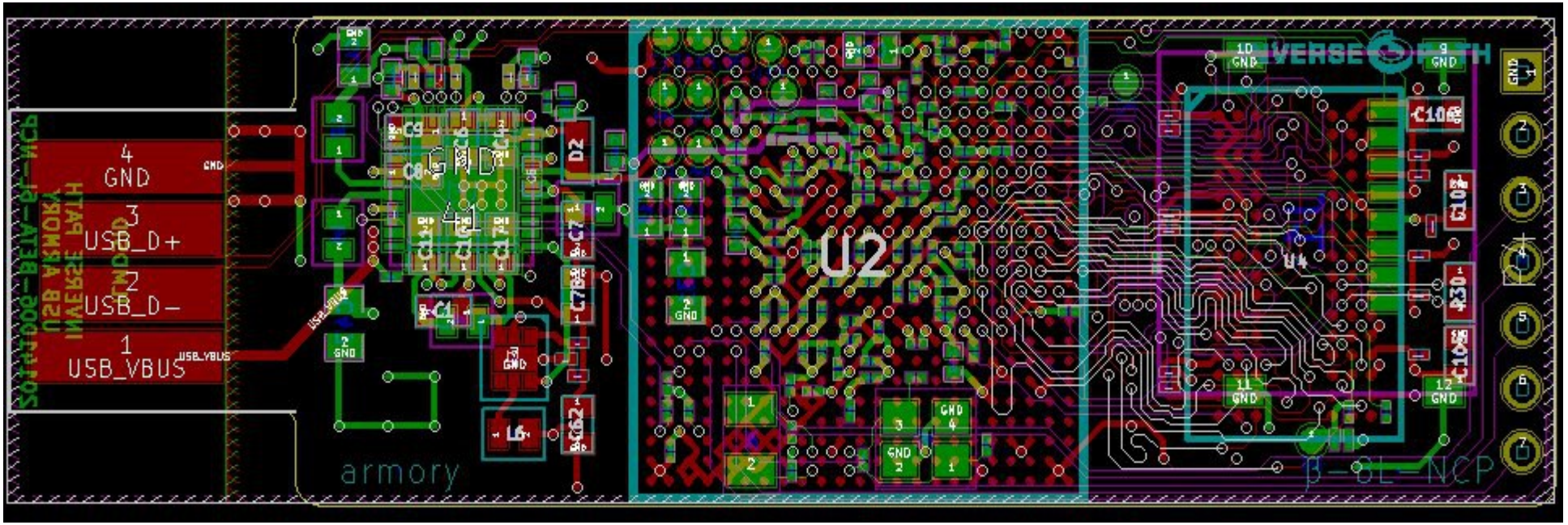


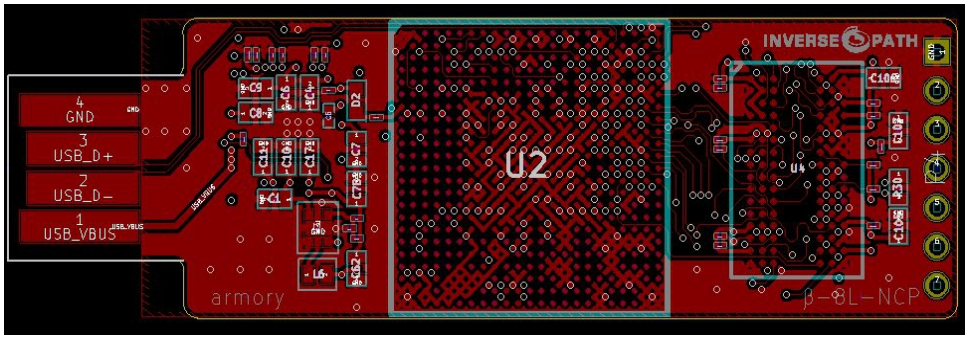


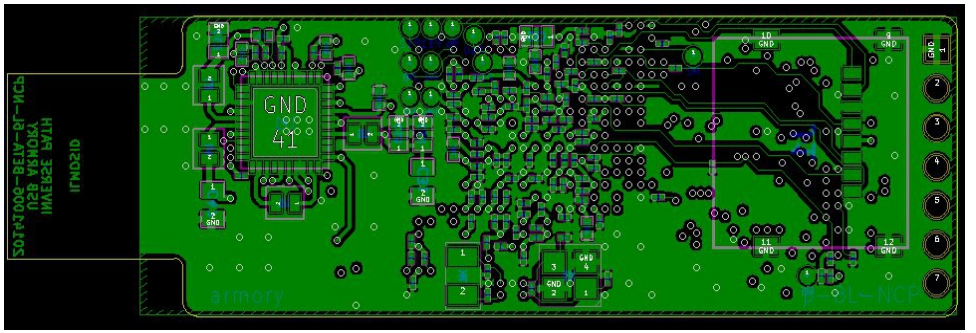
INVERSE PATH

Forging the USB armory

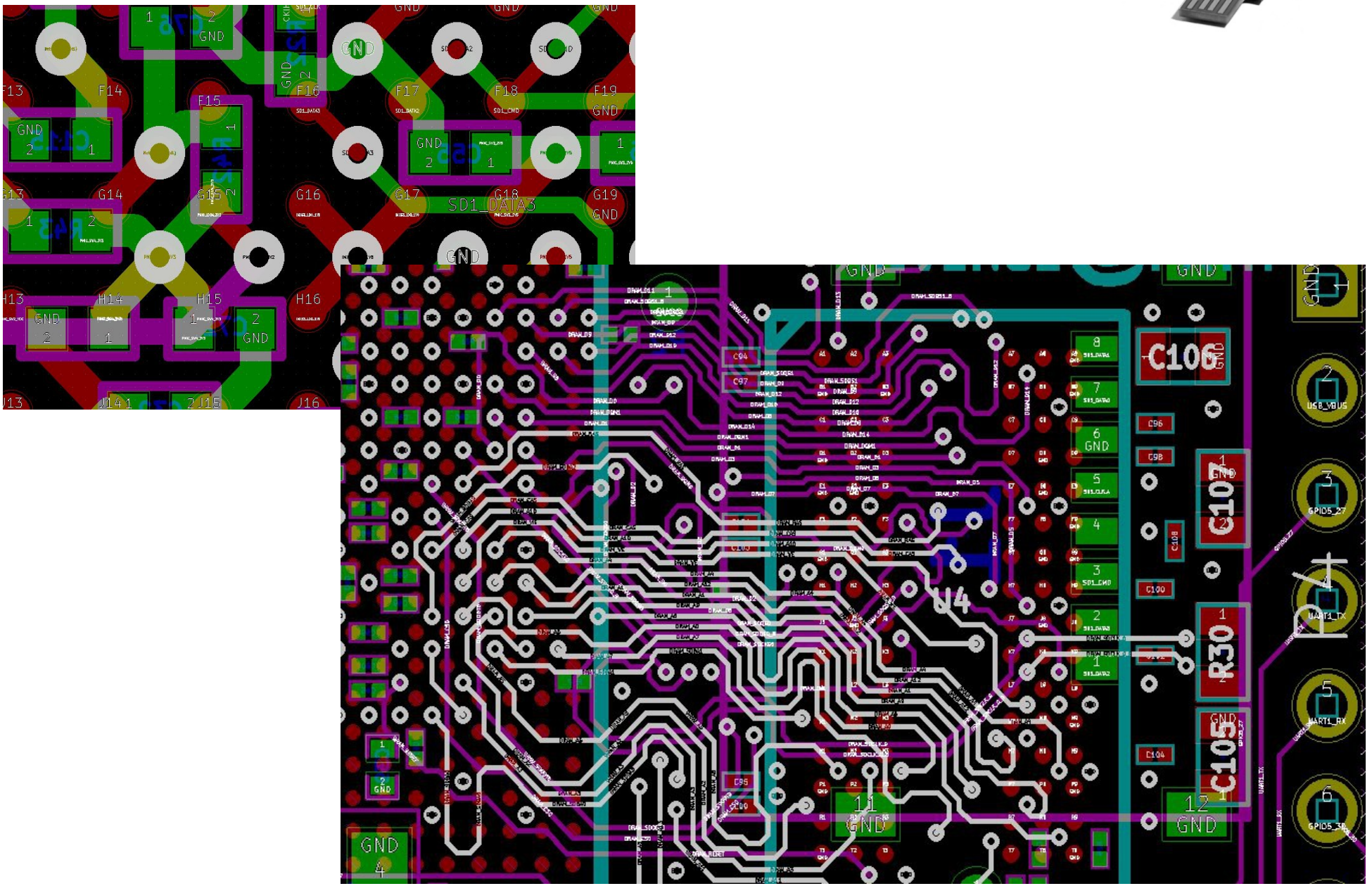
INVERSE PATH



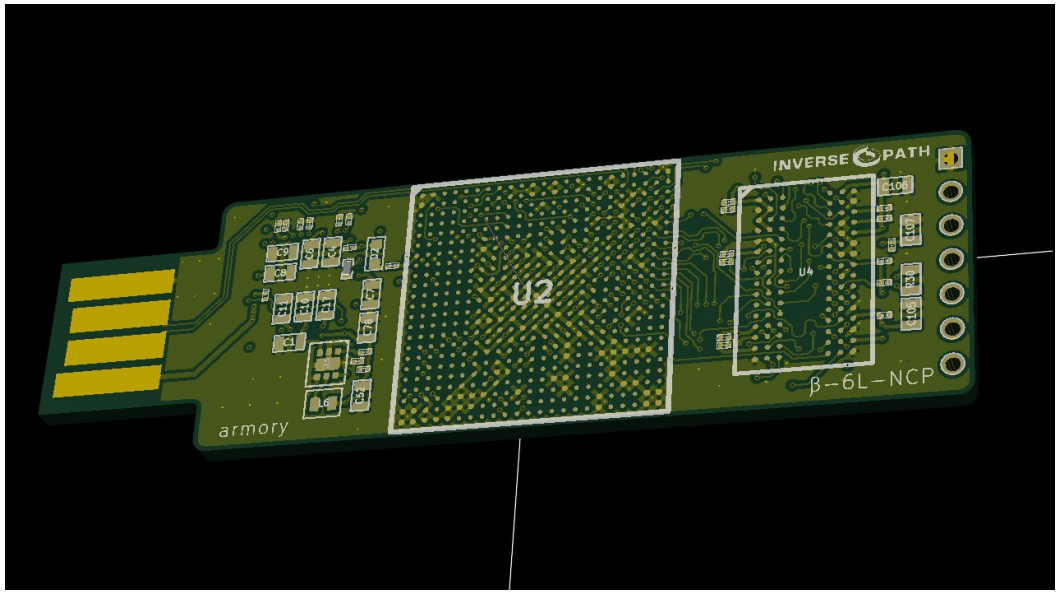


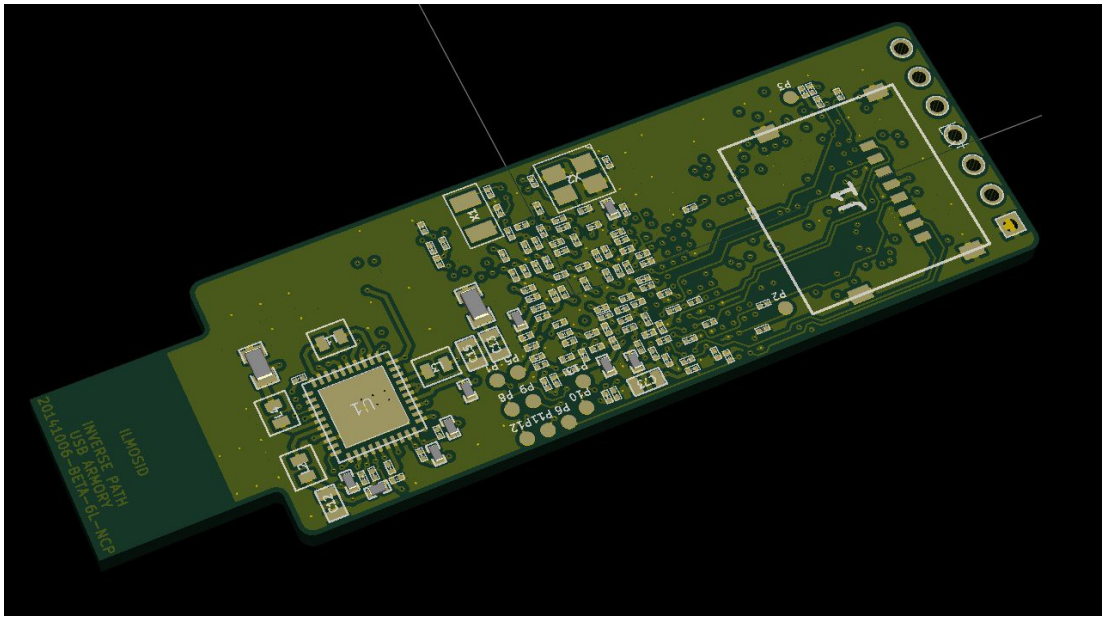


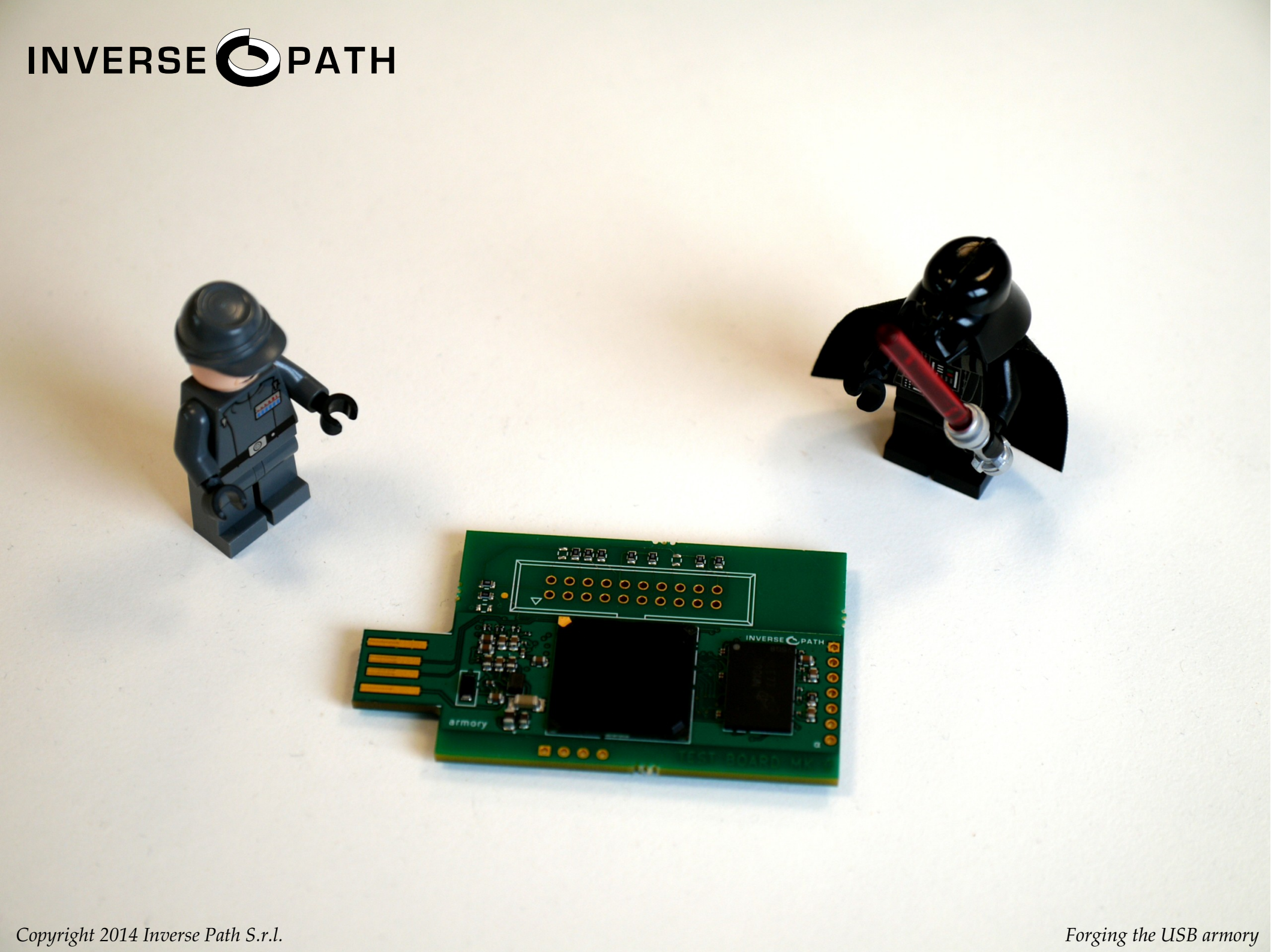
INVERSE PATH



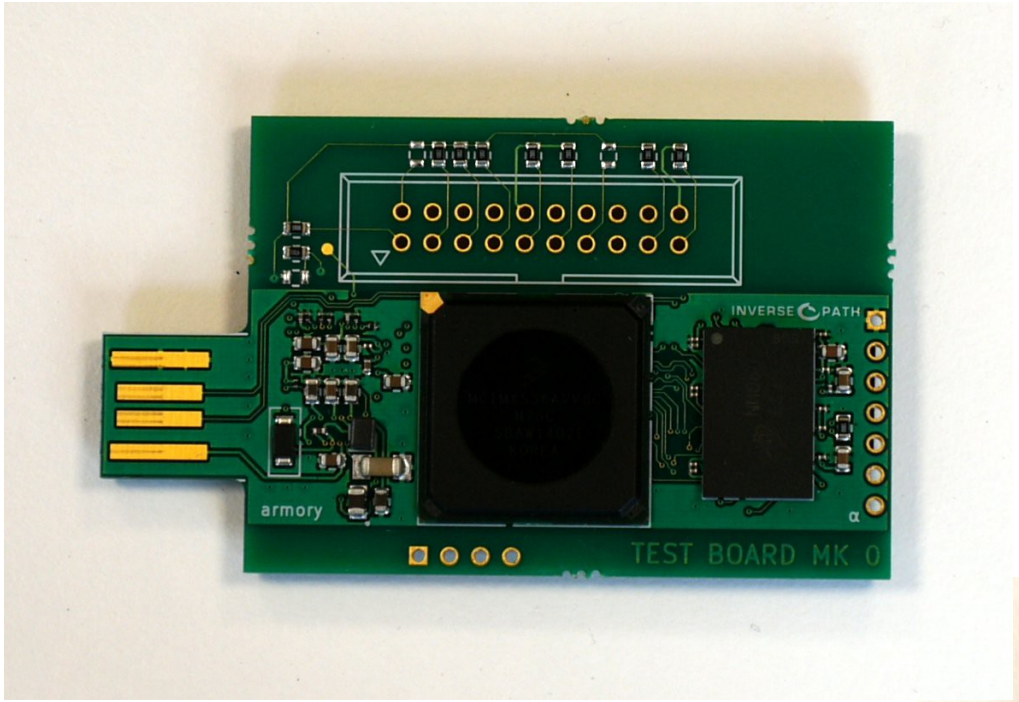
INVERSE PATH

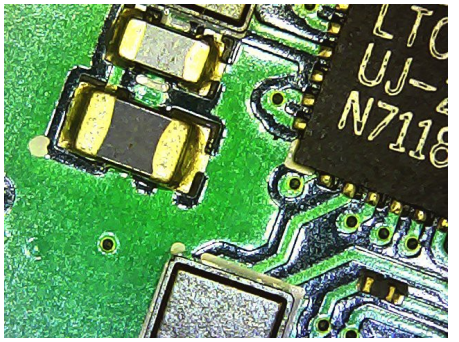


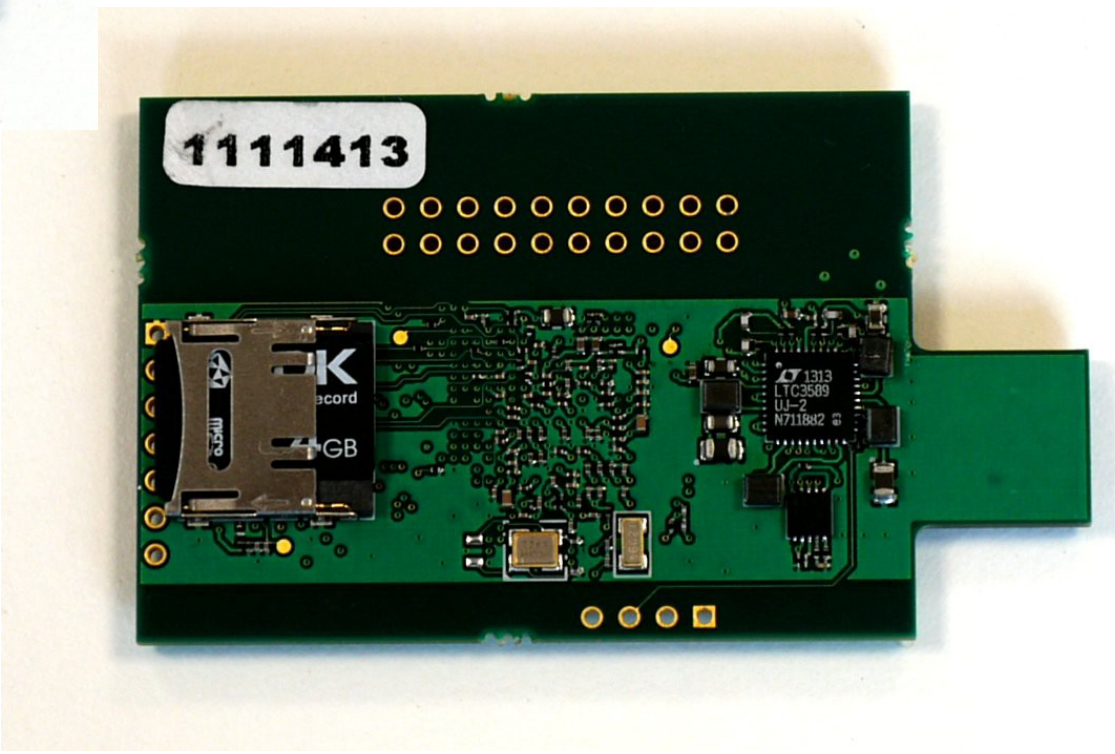


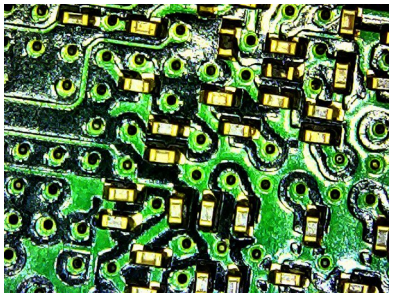


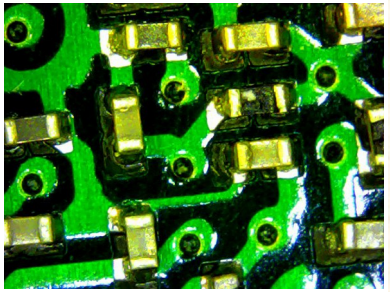
INVERSE PATH

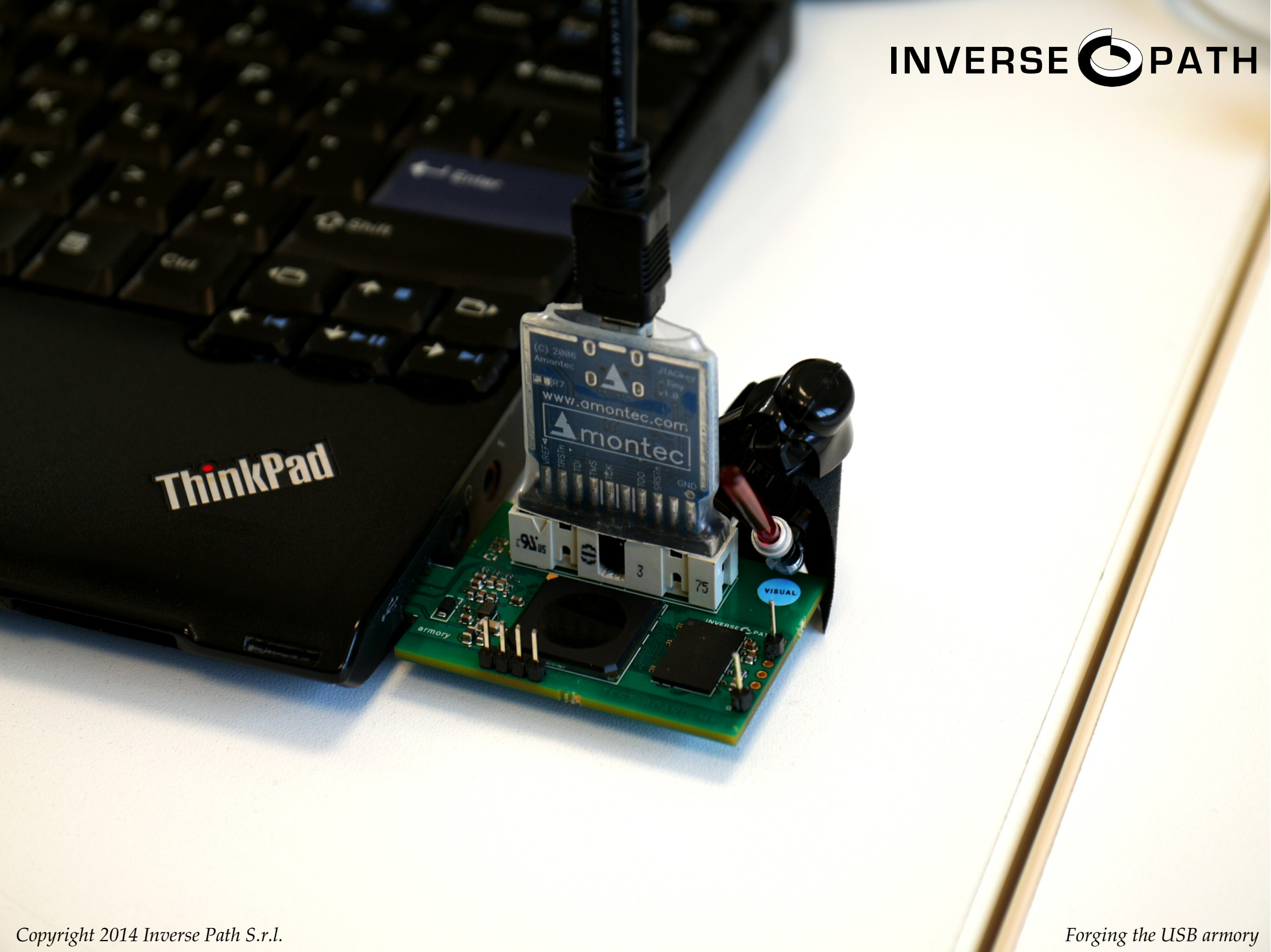


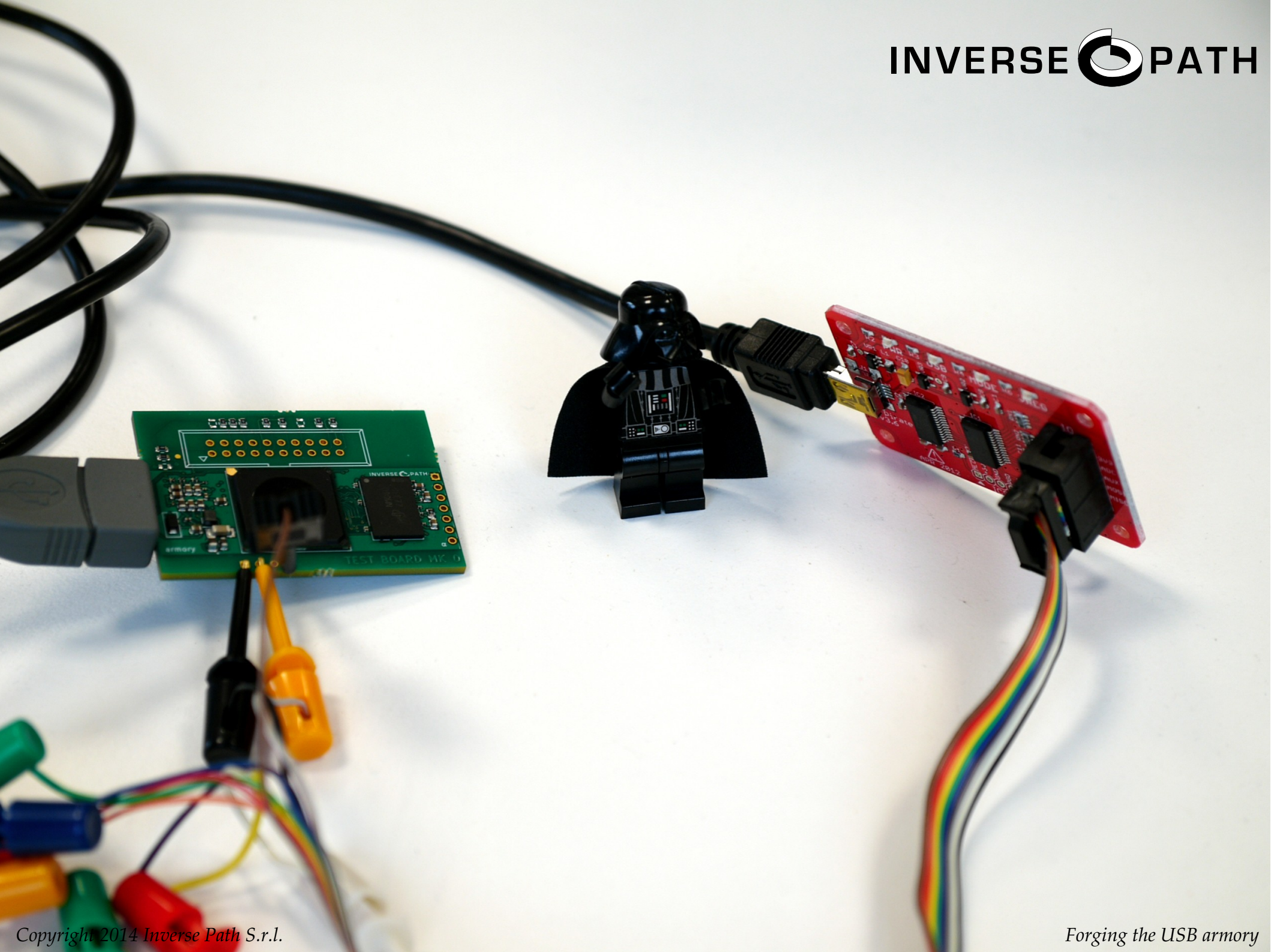


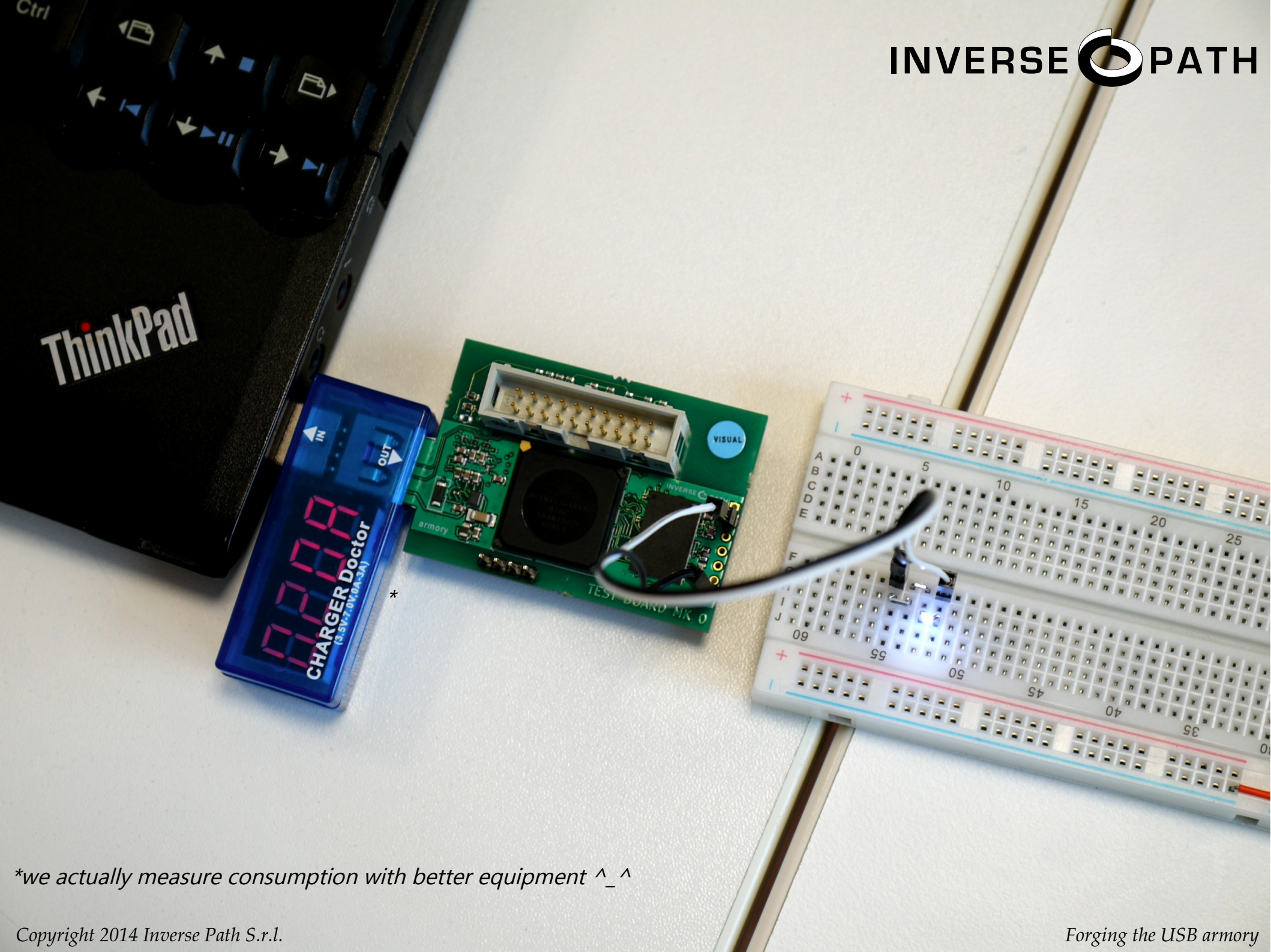












*we actually measure consumption with better equipment ^_^

INVERSE PATH

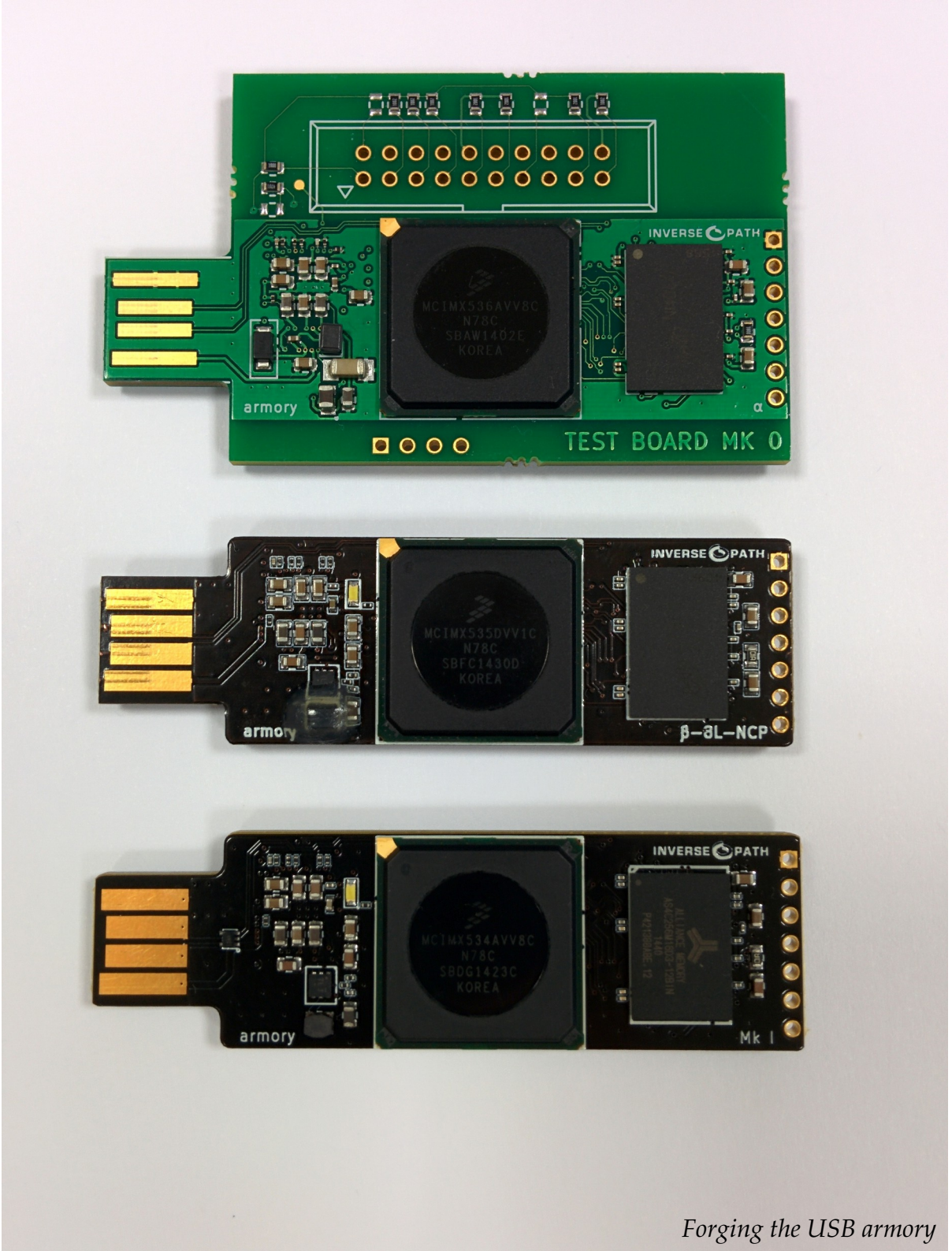
α

βs

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

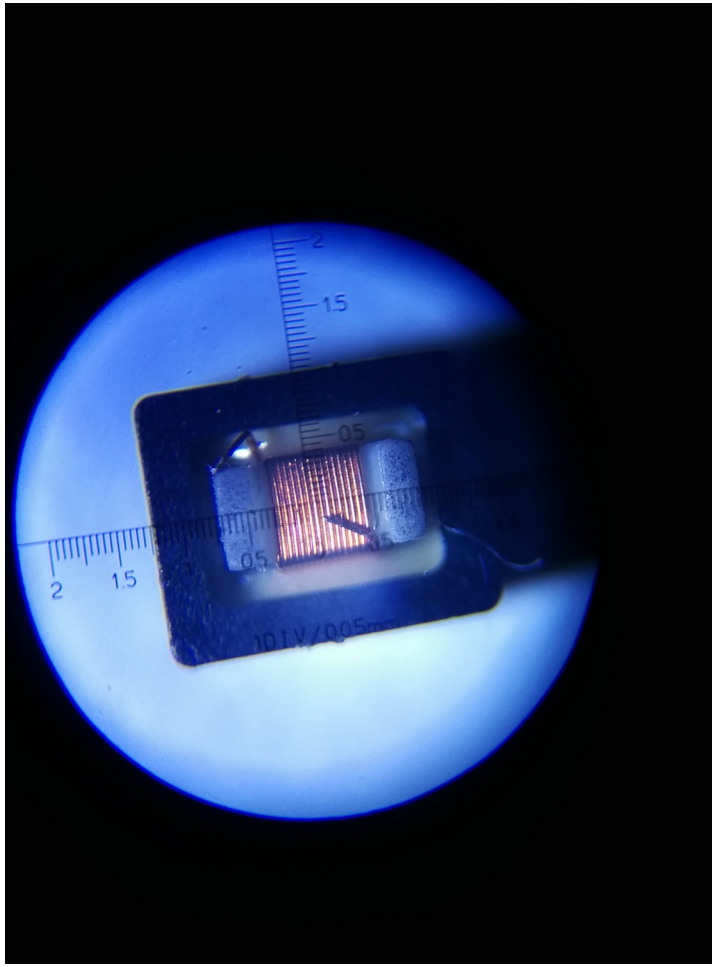
6L, 6L-DDR-LDO, 6L-DDR-NCP

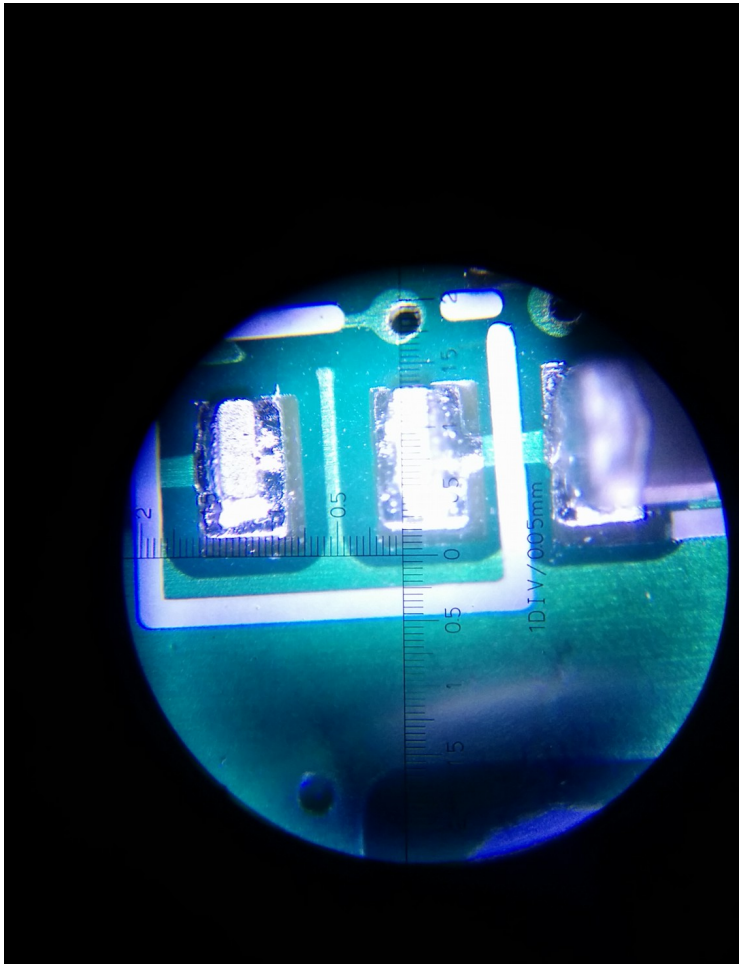
Mk I



Forging the USB armory

INVERSE PATH

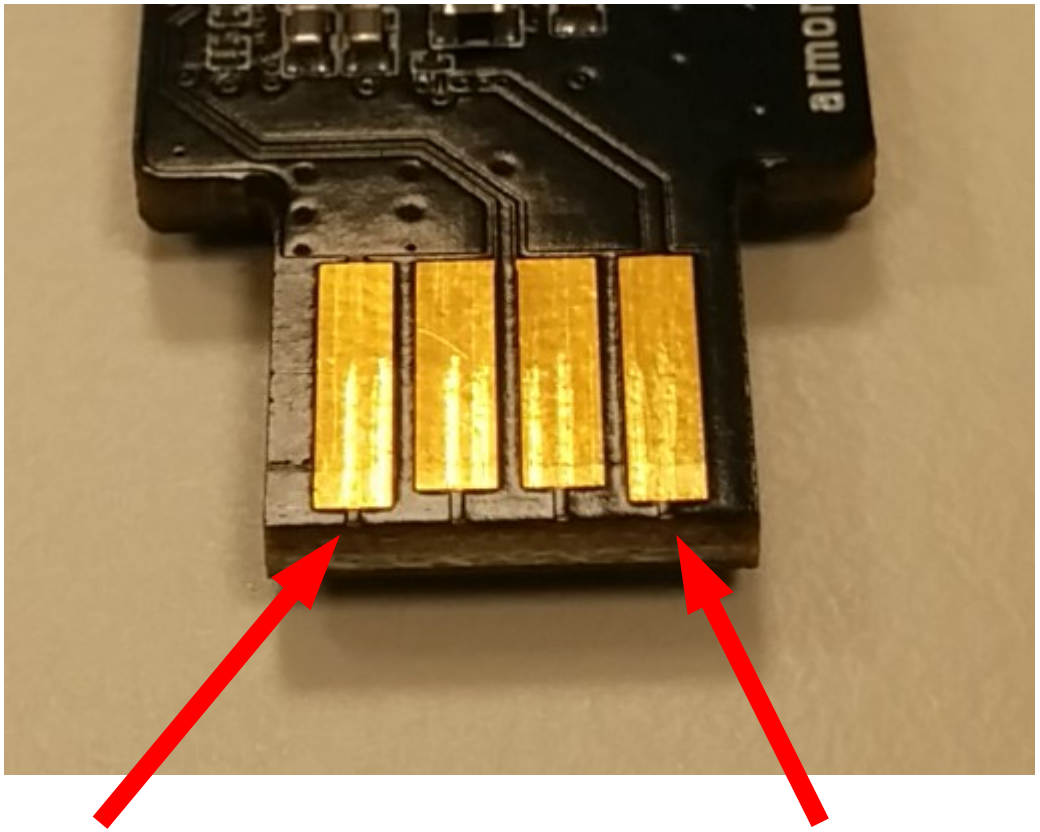


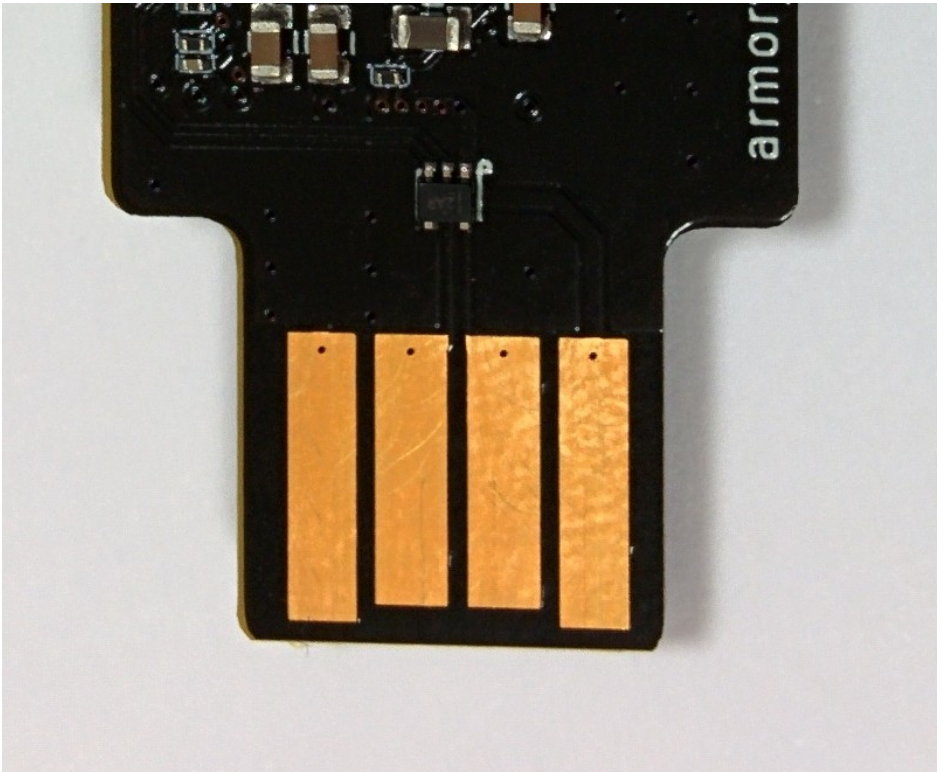


lessons learned #1

tiny inductors are fragile

INVERSE PATH





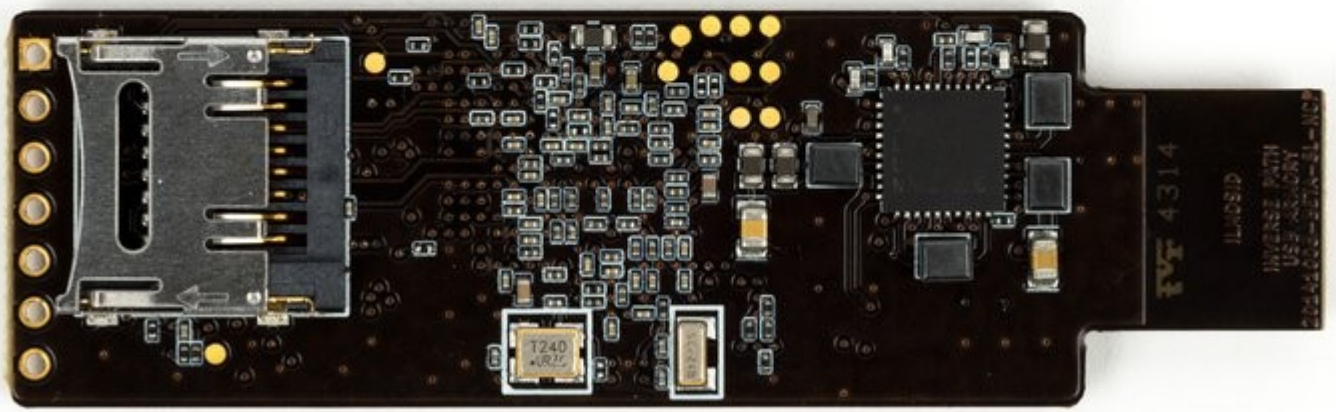
evil

good

lessons learned #2 (the five-second rule)

gold plating traces cause under-voltage on hot swap

INVERSE PATH



INVERSE PATH

Thank you!

Q & A

Andrea Barisani

<andrea@inversepath.com>