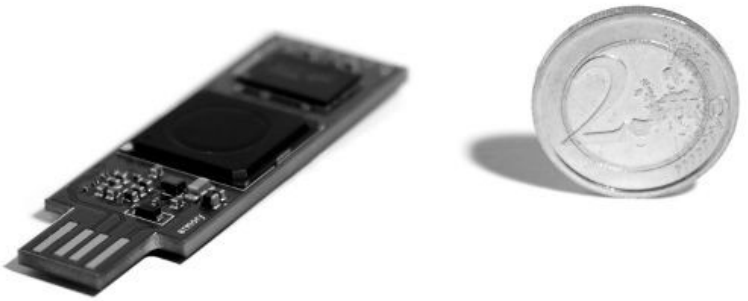
INVERSE PATH

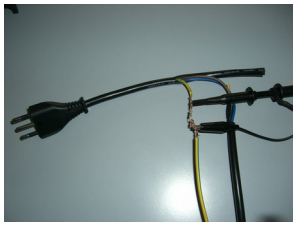
Forging the USB armory

Andrea Barisani
<andrea@inversepath.com>

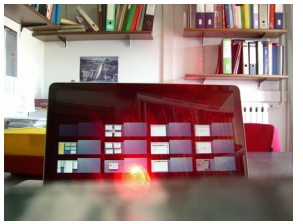


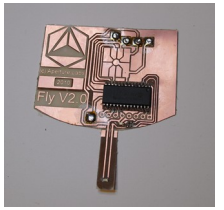
INVERSE PATH

2007: Unusual Car Navigation Tricks
Injecting RDS-TMC Traffic Information Signals



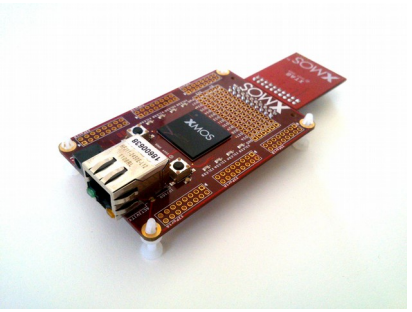
2009: Sniff Keystrokes With Lasers/Voltmeters
Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage





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



INVERSE PATH

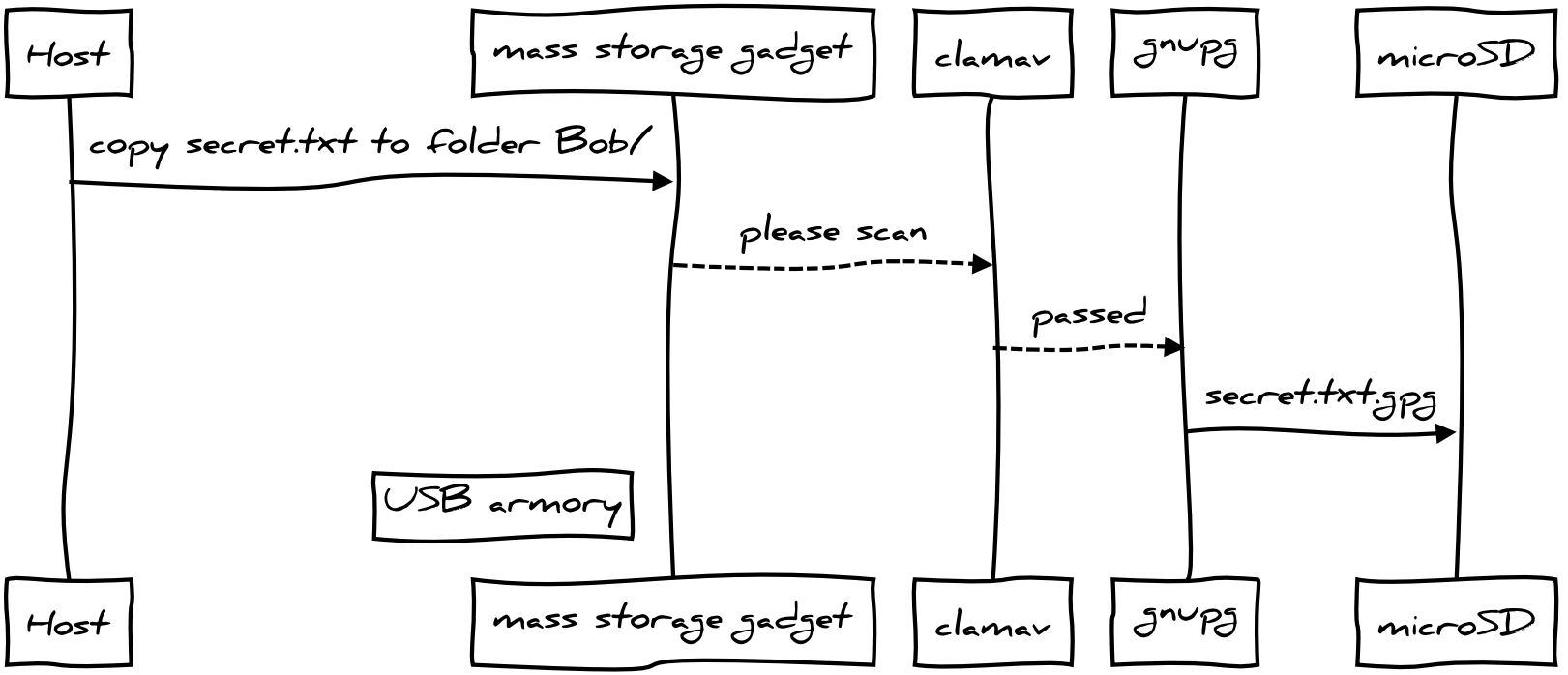
INVERSE PATH

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

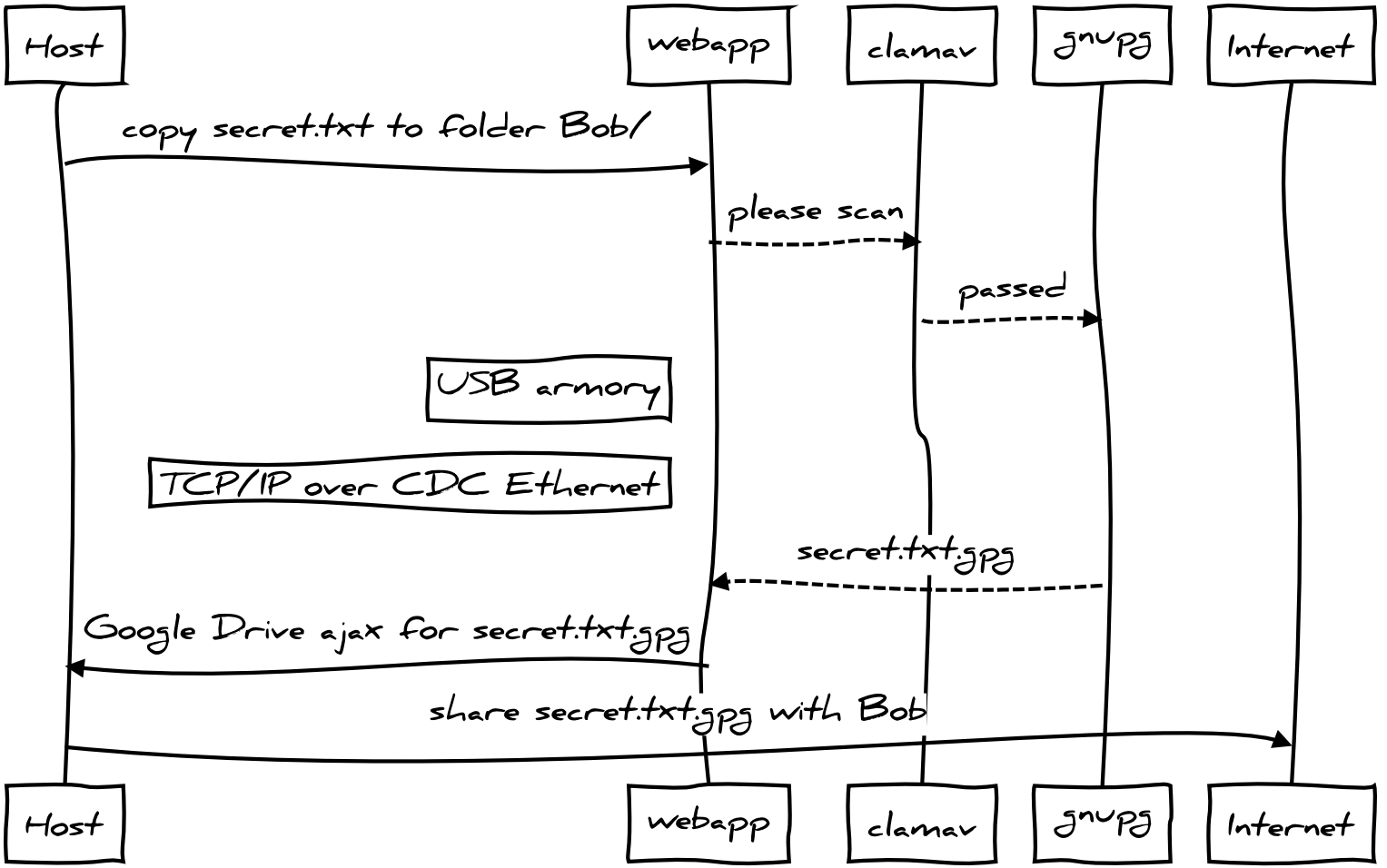
INVERSE PATH

enhanced mass storage



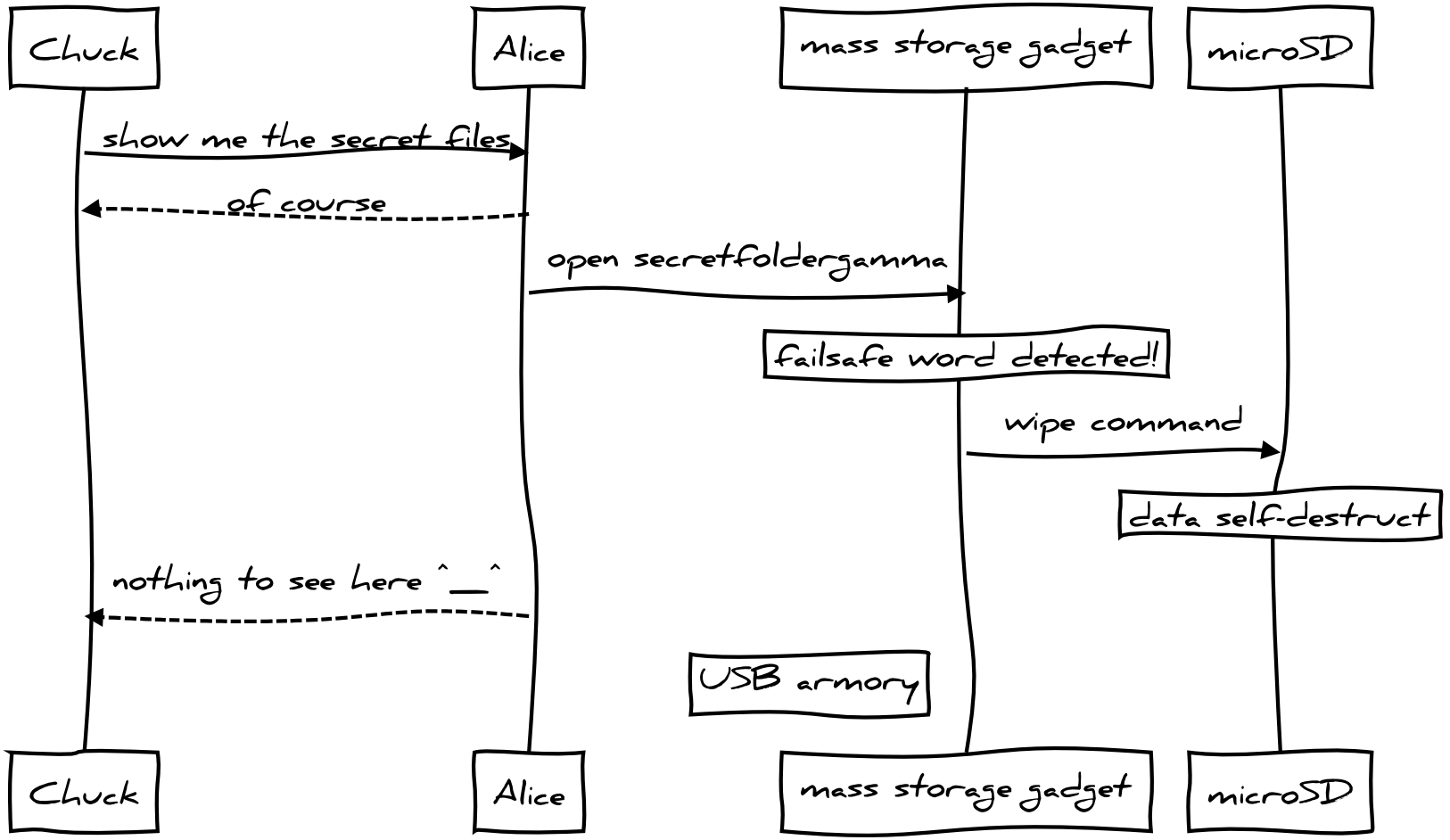
INVERSE PATH

enhanced mass storage



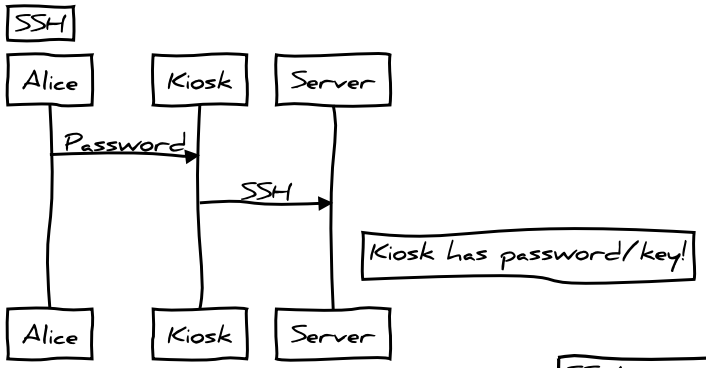
INVERSE PATH

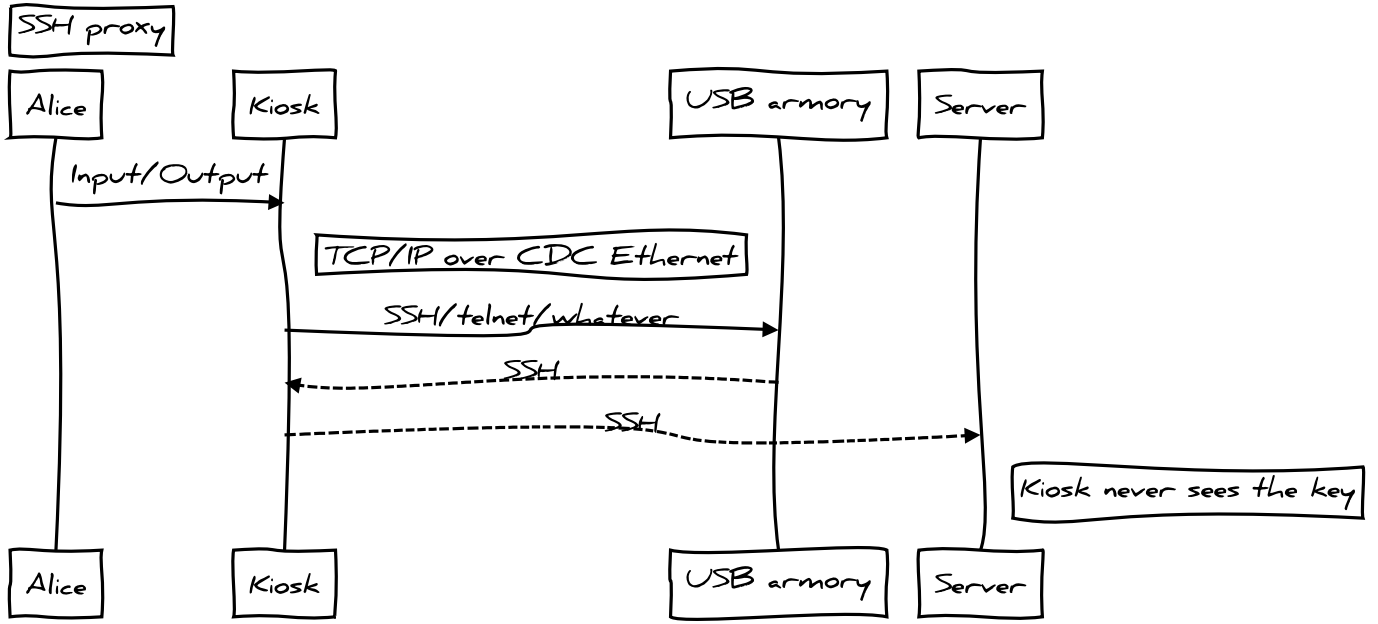
enhanced mass storage

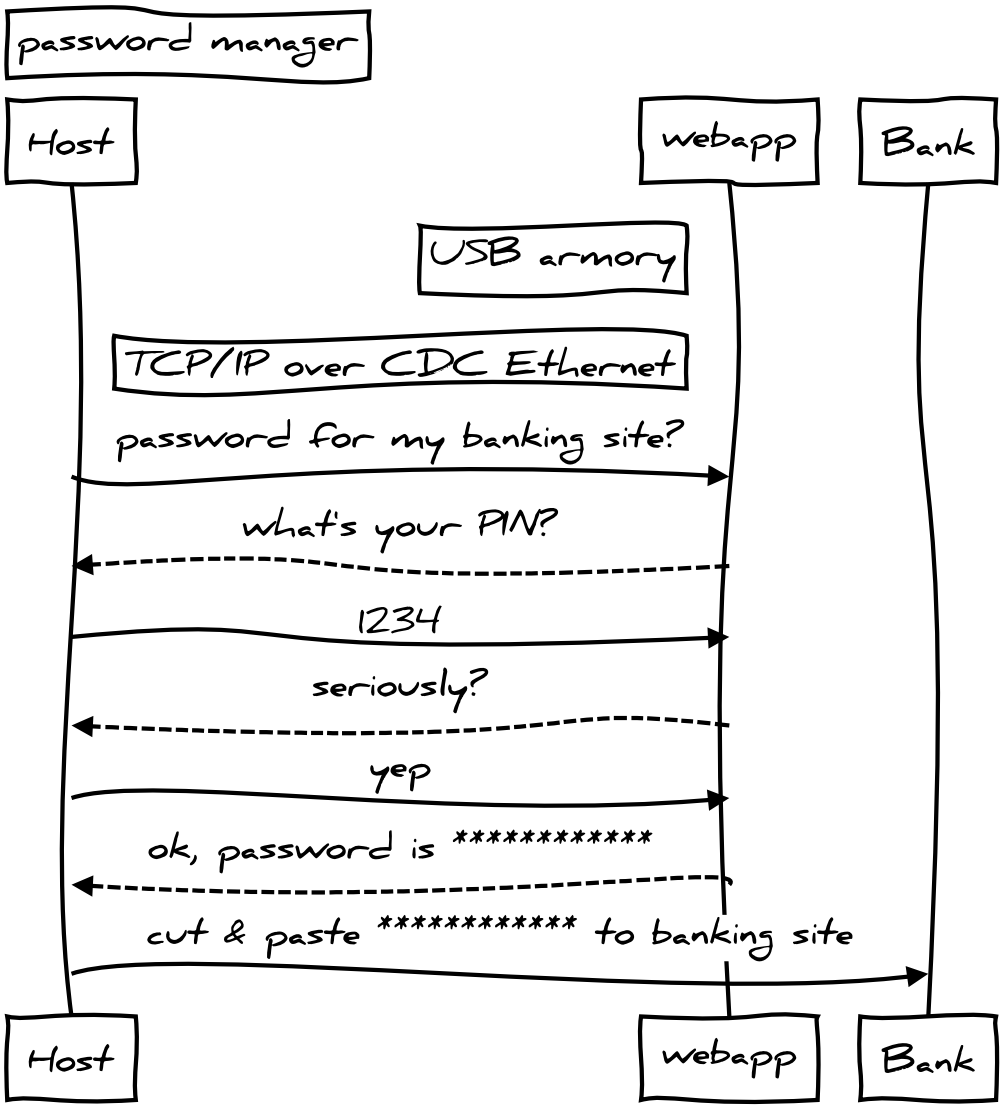


INVERSE PATH

SSH proxy





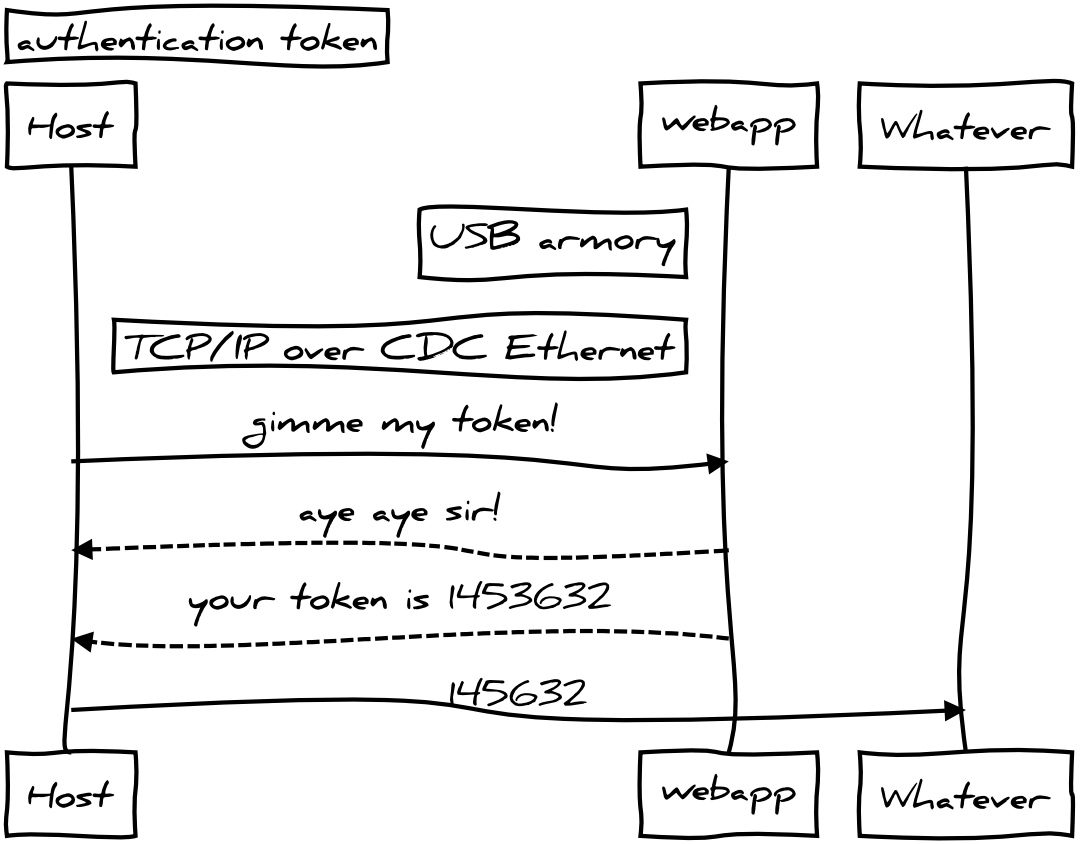


password manager

**trivial example, better options planned*

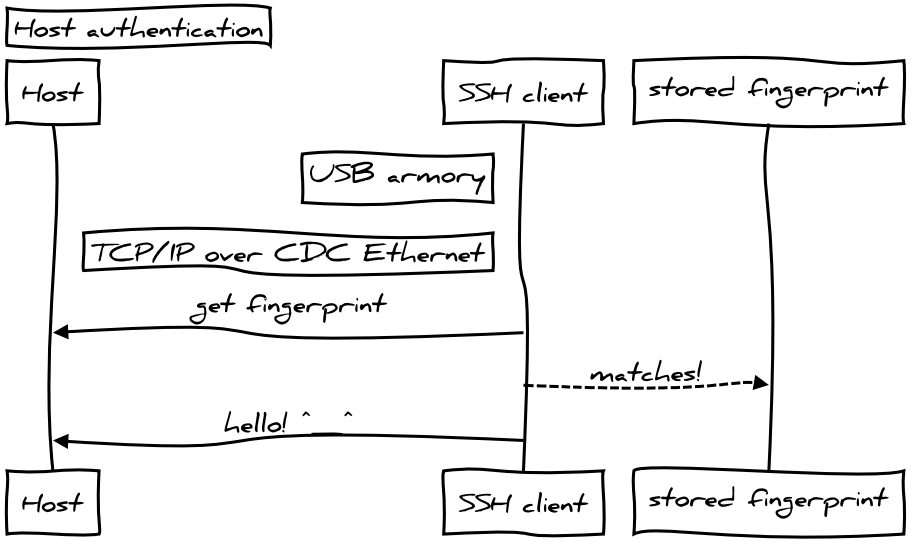
INVERSE PATH

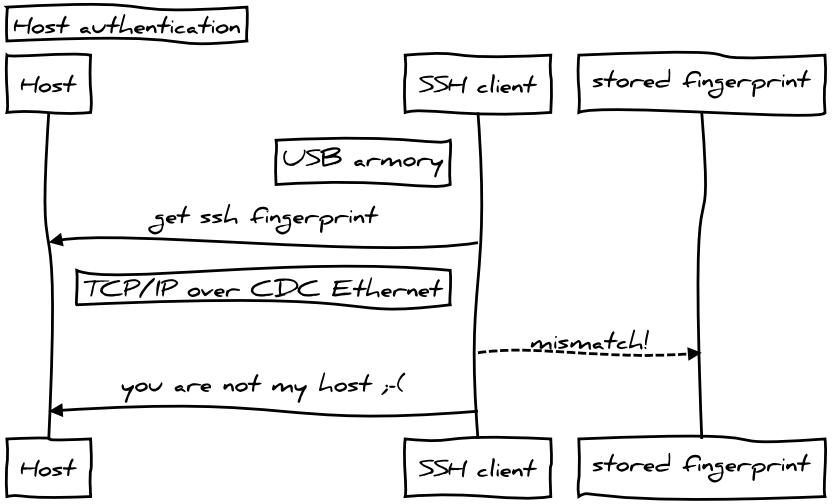
authentication token



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

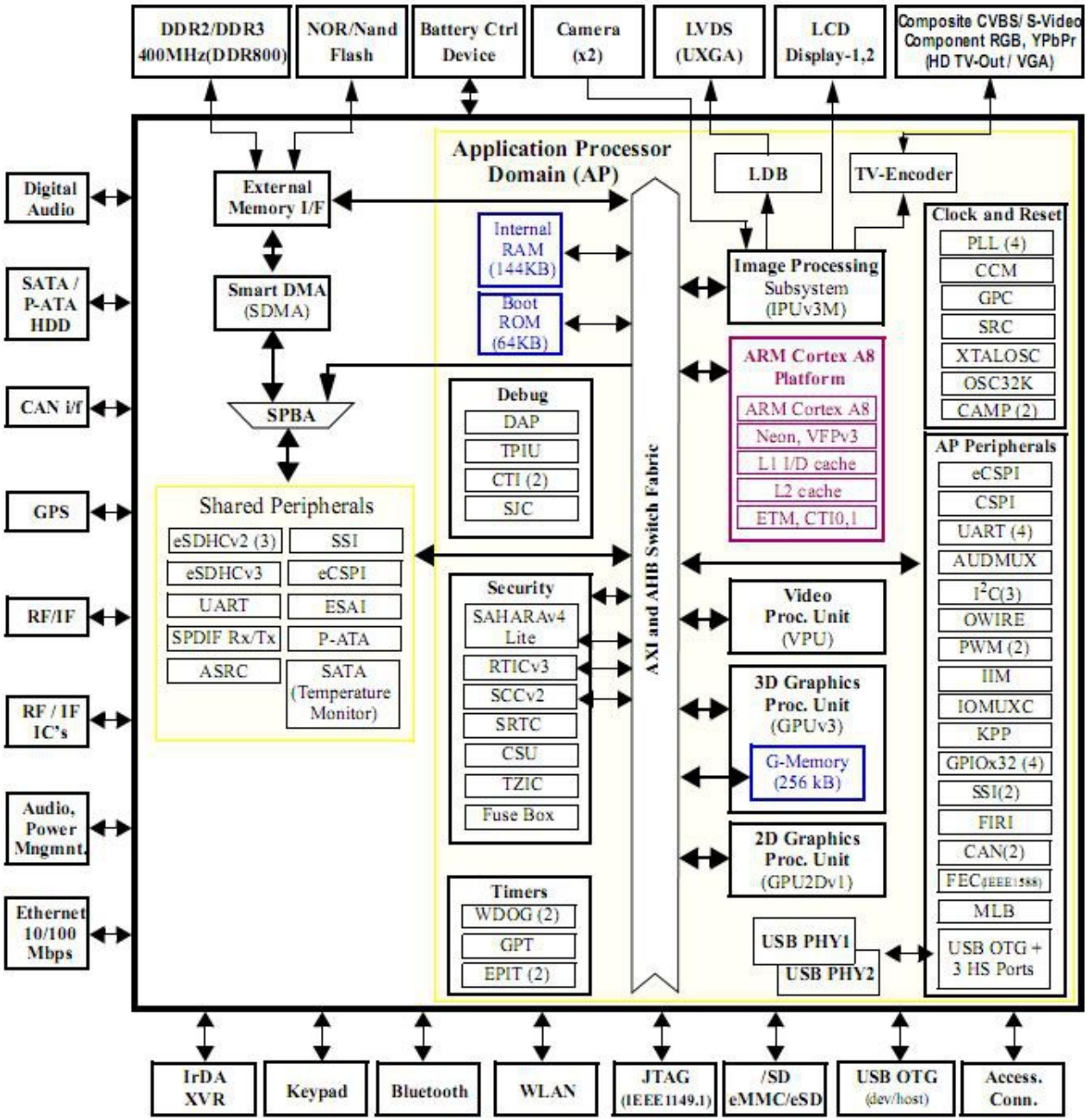
INVERSE PATH

Selecting the System on Chip (SoC)

Freescale i.MX53

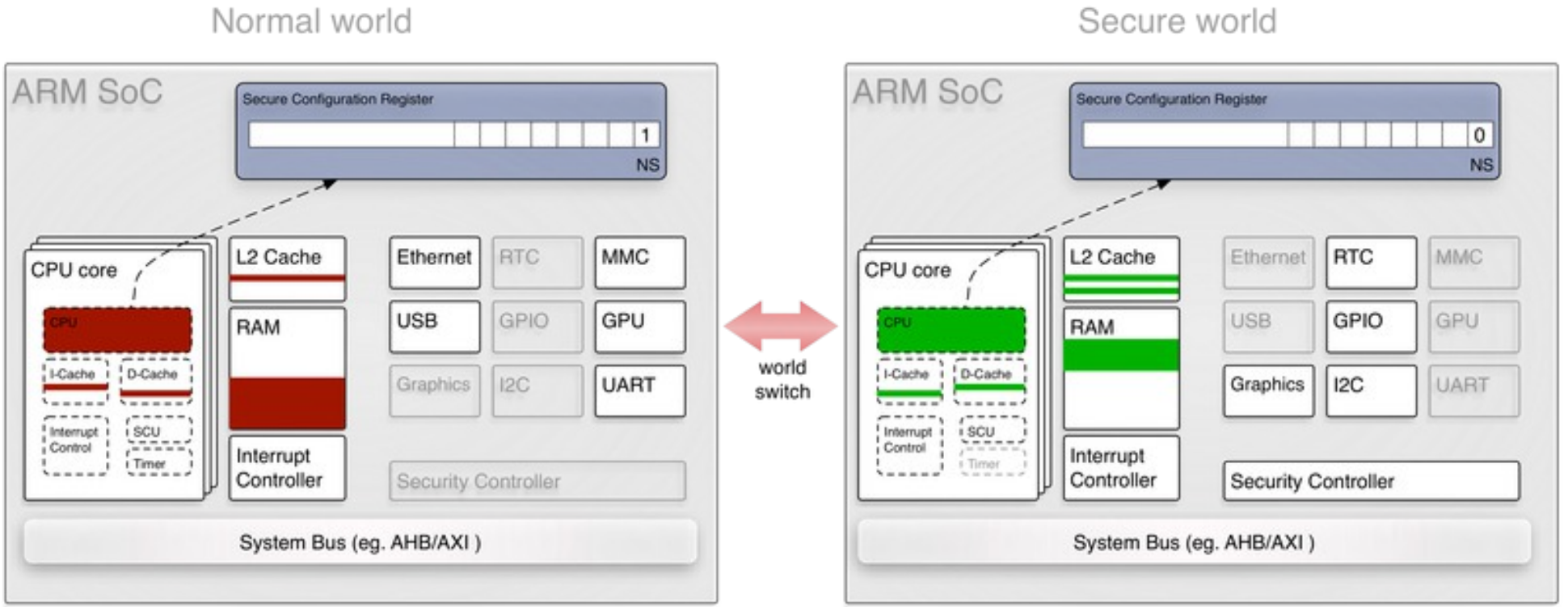
- ARM® Cortex™-A8 800-1200 Mhz
- almost all datasheets/manuals are public (no NDA required)
- Freescale datasheets are “ok” (far better than other vendors)
- ARM® TrustZone®, secure boot + storage + RAM
- detailed power consumption guide available
- excellent native support (Android, Debian, Ubuntu,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

INVERSE PATH



INVERSE PATH

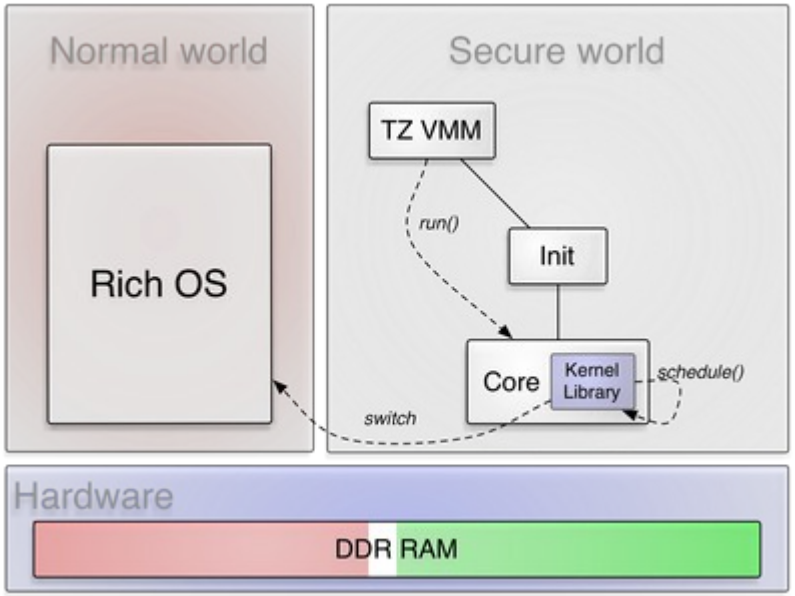
ARM® TrustZone®

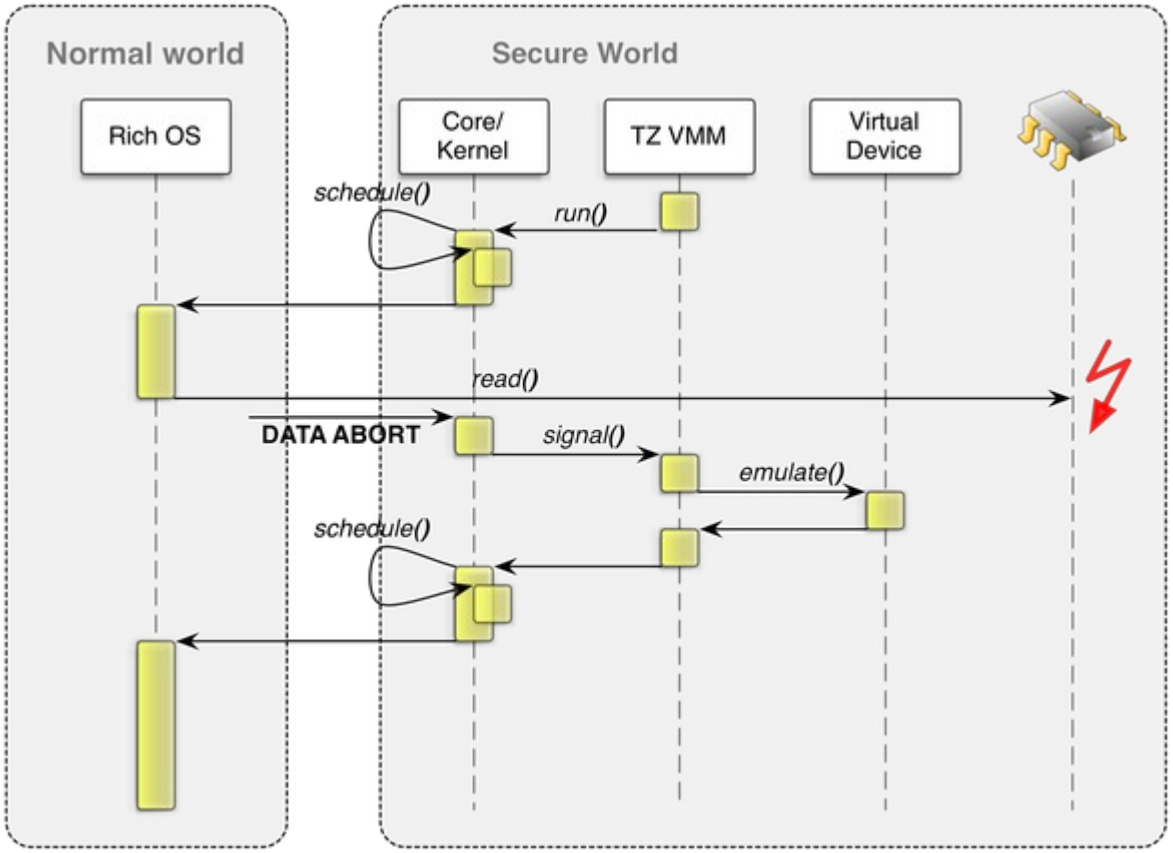


http://genode.org/documentation/articles/trustzone

INVERSE PATH

ARM® TrustZone®





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

INVERSE PATH

Development timeline

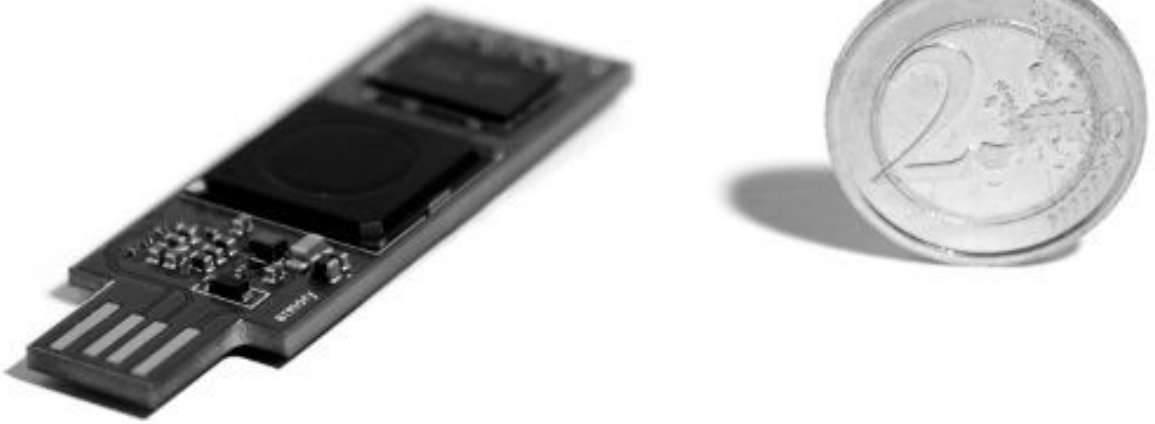
- 2014/01: first concept idea (based on AT91RM9200)
- 2014/03: schematics development begins
- 2014/04: PCB layout for breakout/prototyping board
- 2014/08: order for alpha board manufacturing
- 2014/09: USB armory alpha board arrives
- 2014/10: project announcement
- 2014/10: order for 7 optimized revisions against alpha design
- 2014/11: beta revisions arrive and are evaluated

future planning

- 2014/11: design finalization and first batch production
- 2014/12: shipping

INVERSE PATH

armory



open source hardware

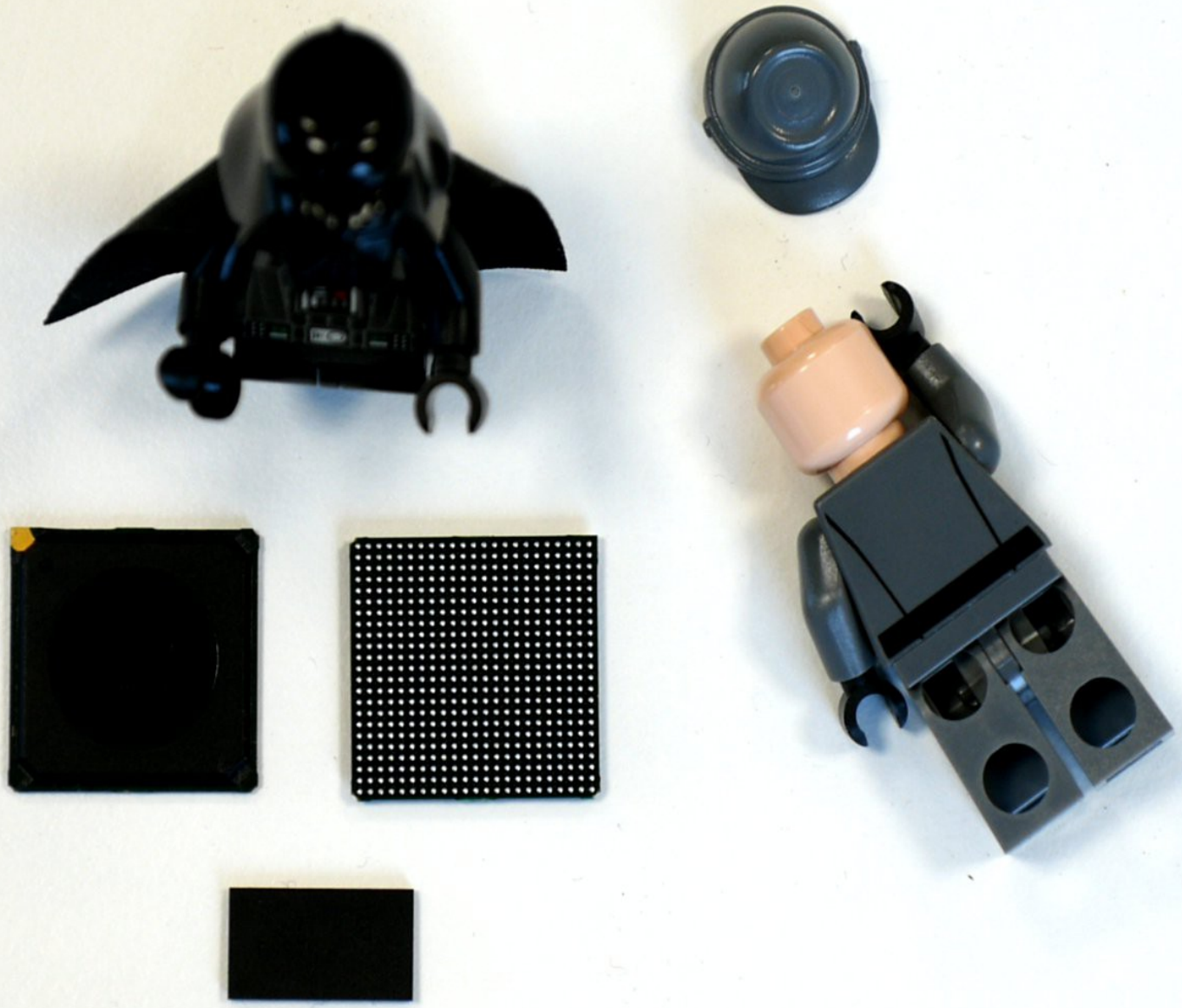
http://inversepath.com/usbarmory

open source

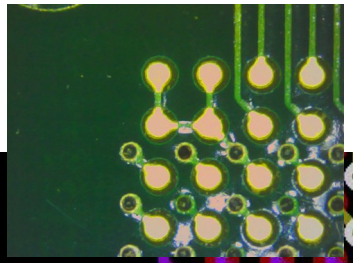
INVERSE PATH

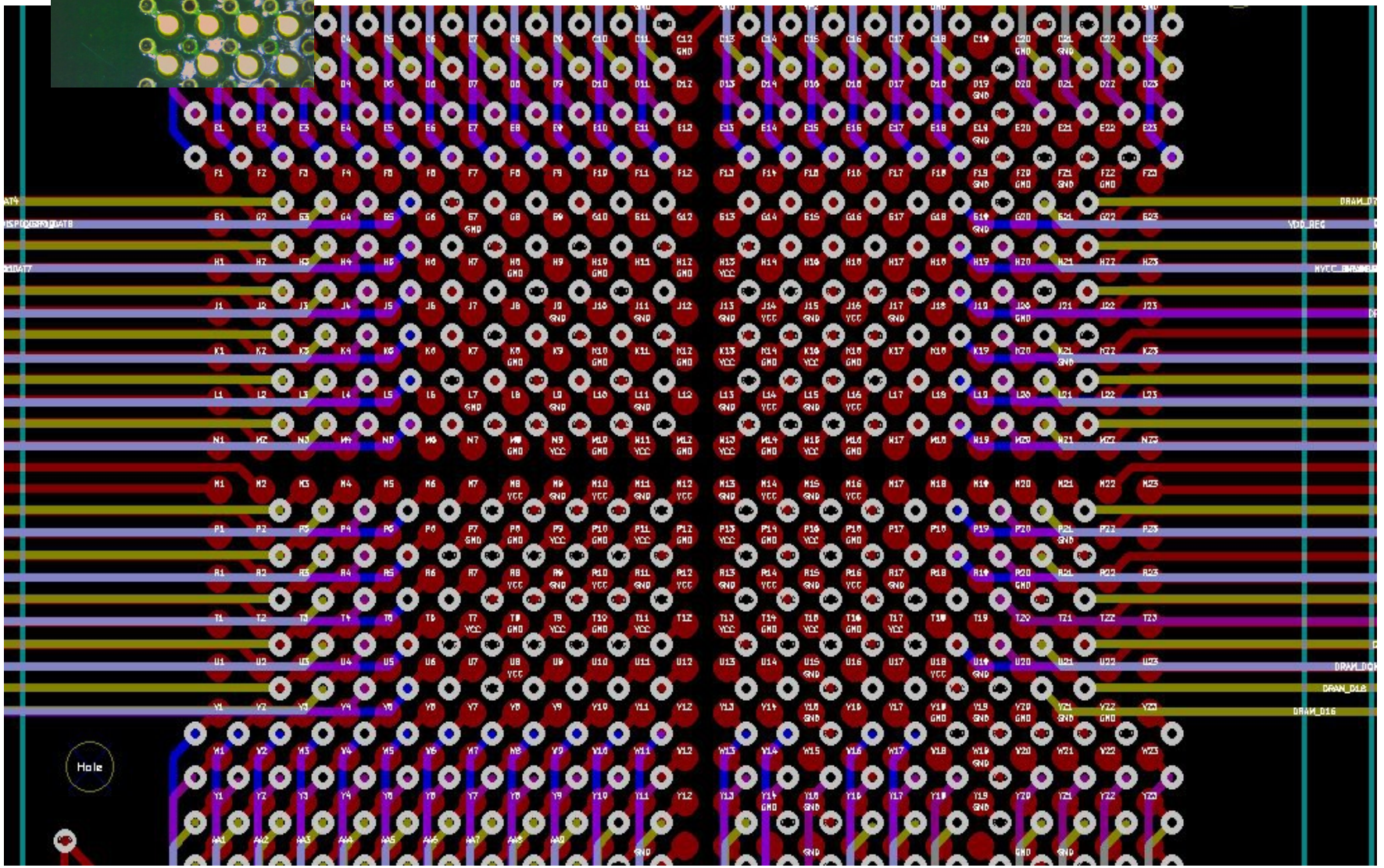
USB armory - Open source flash-drive-sized computer

- 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

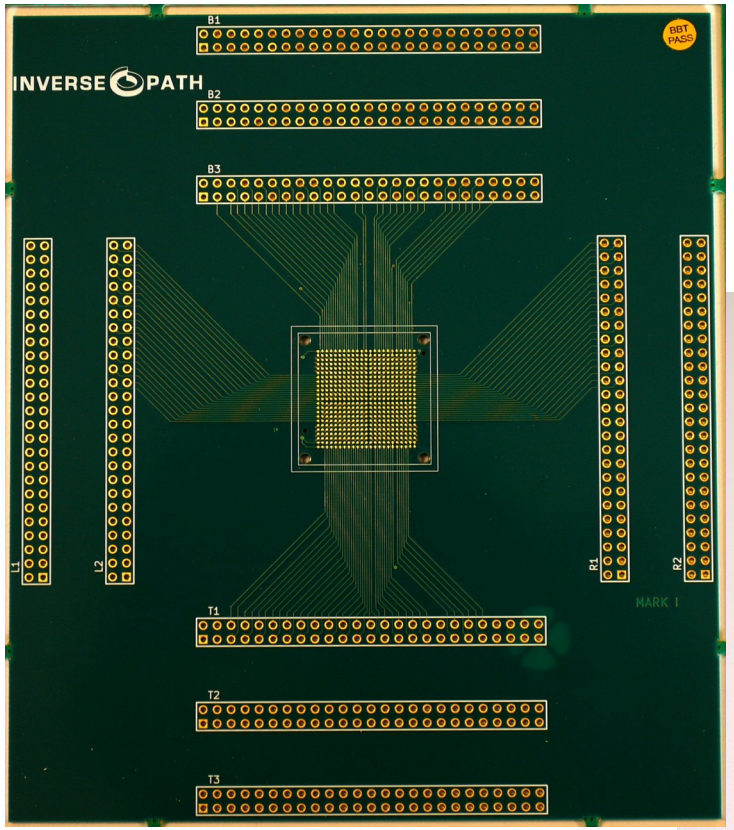


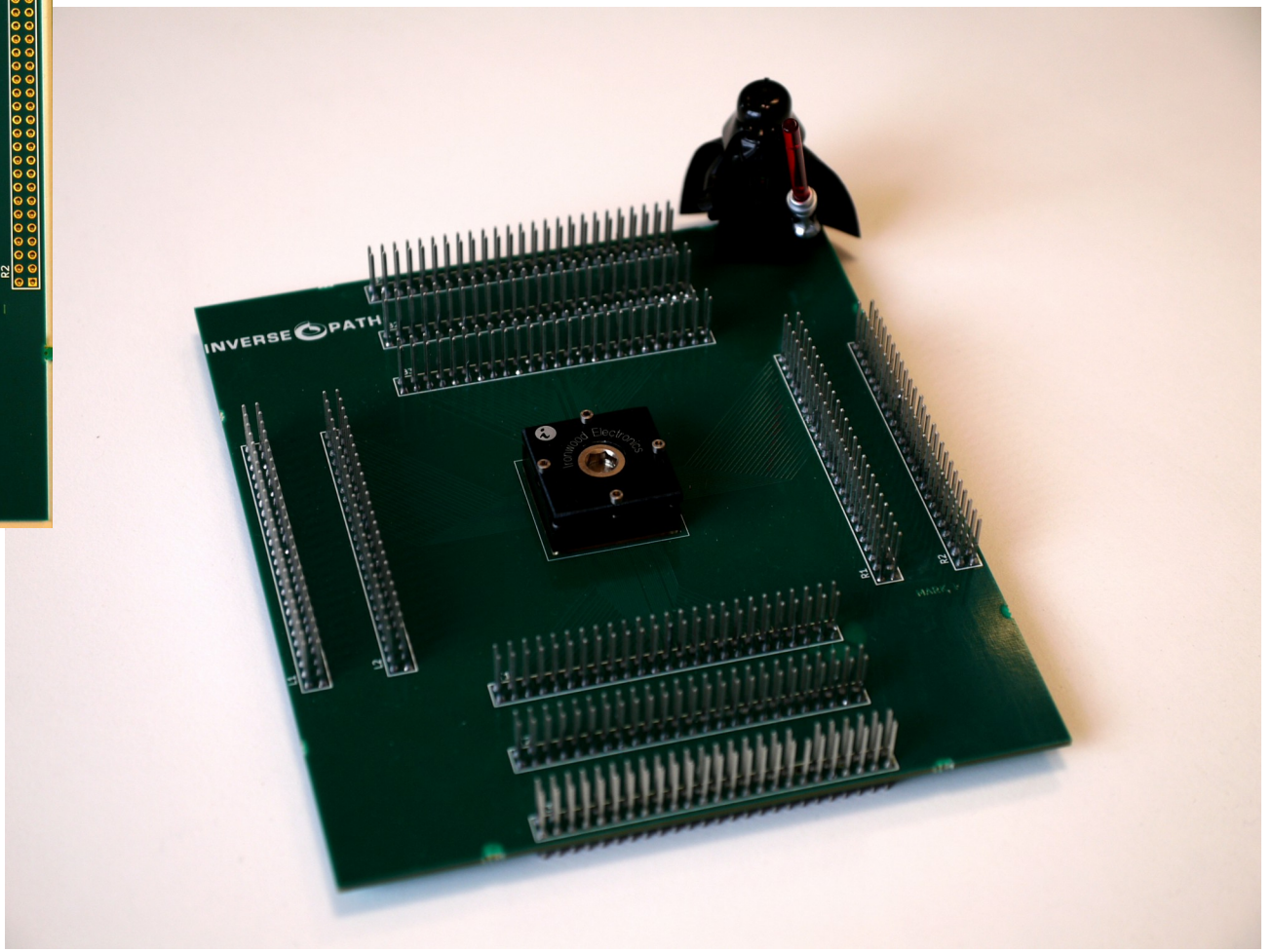
INVERSE PATH



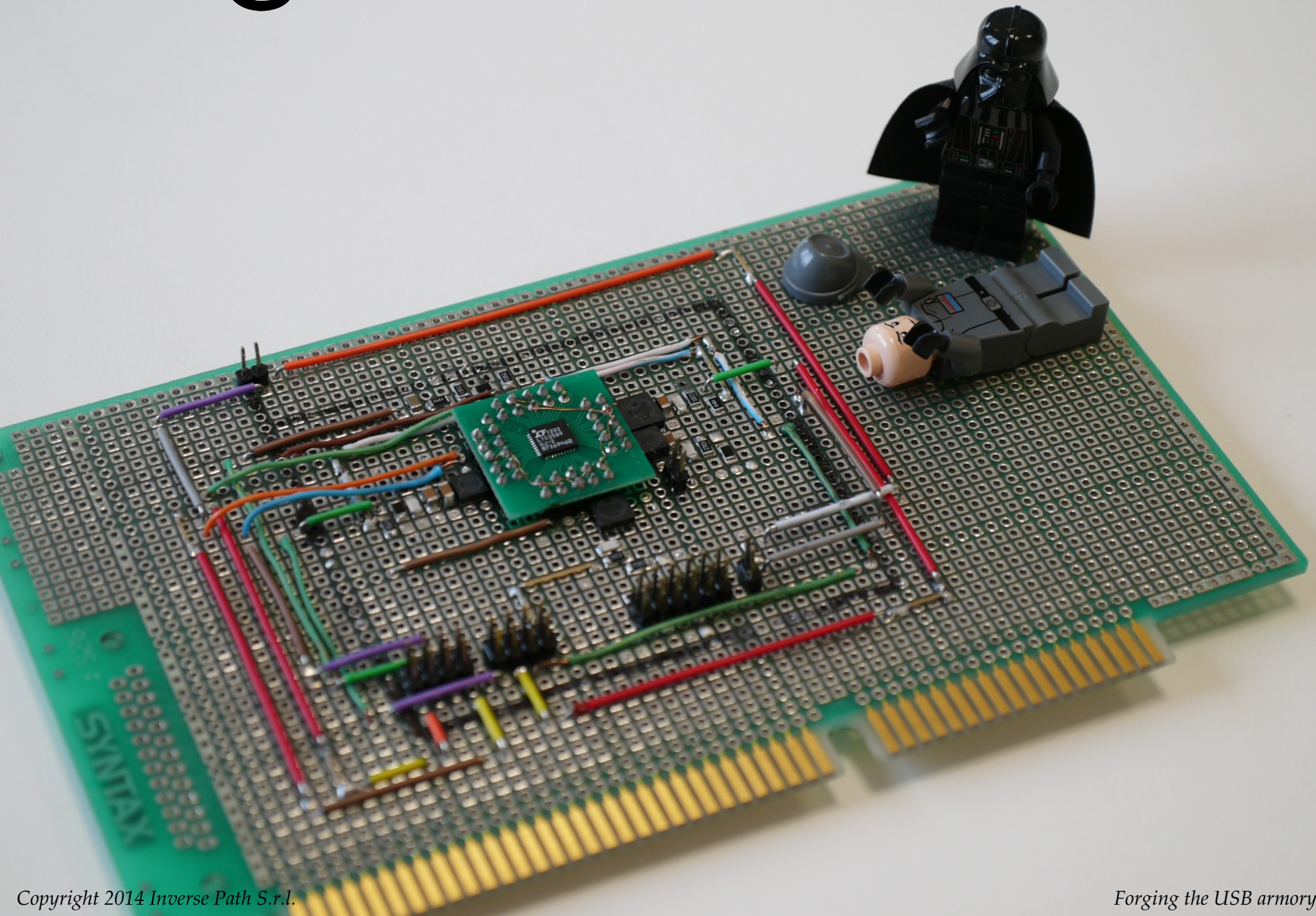


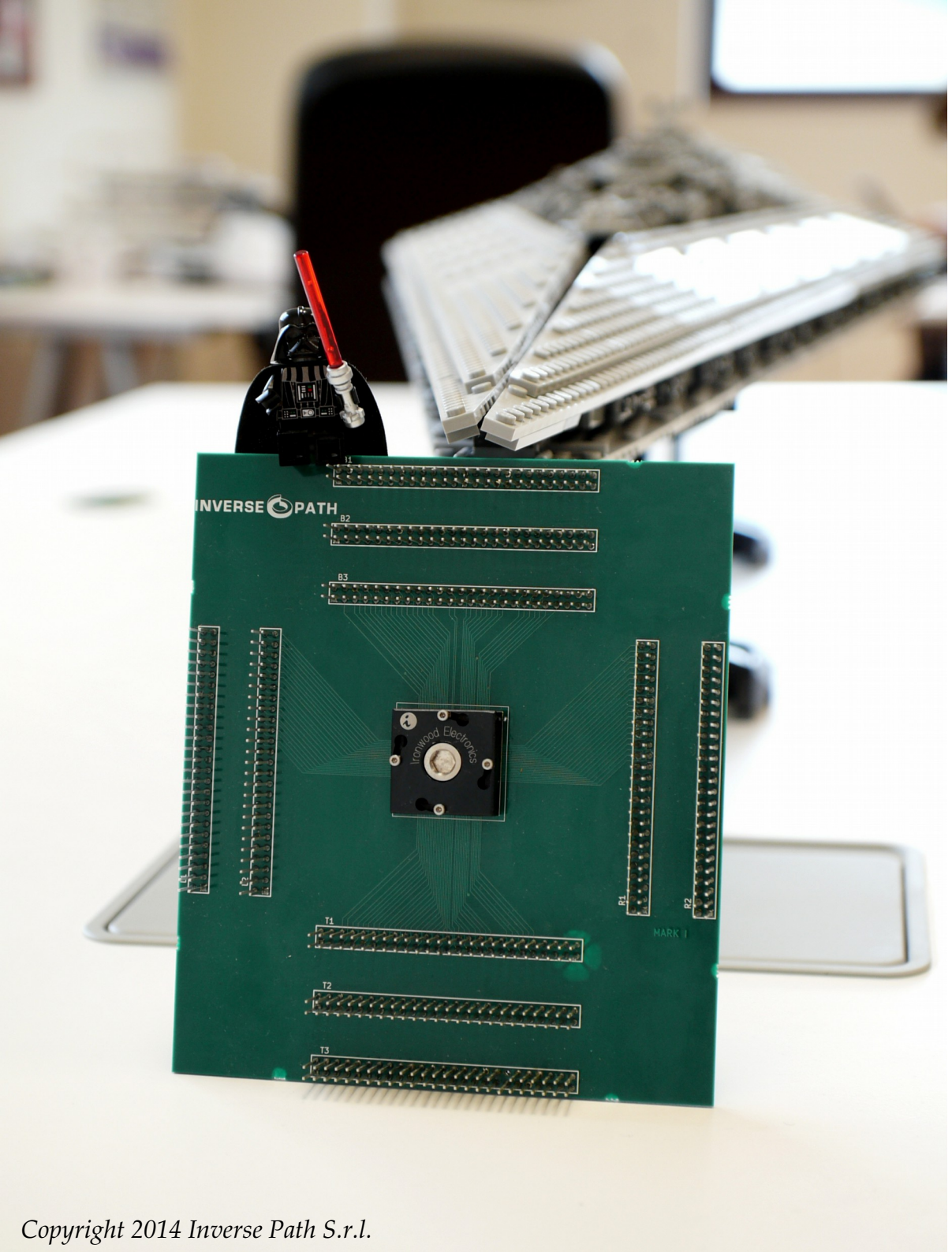
INVERSE PATH





INVERSE PATH

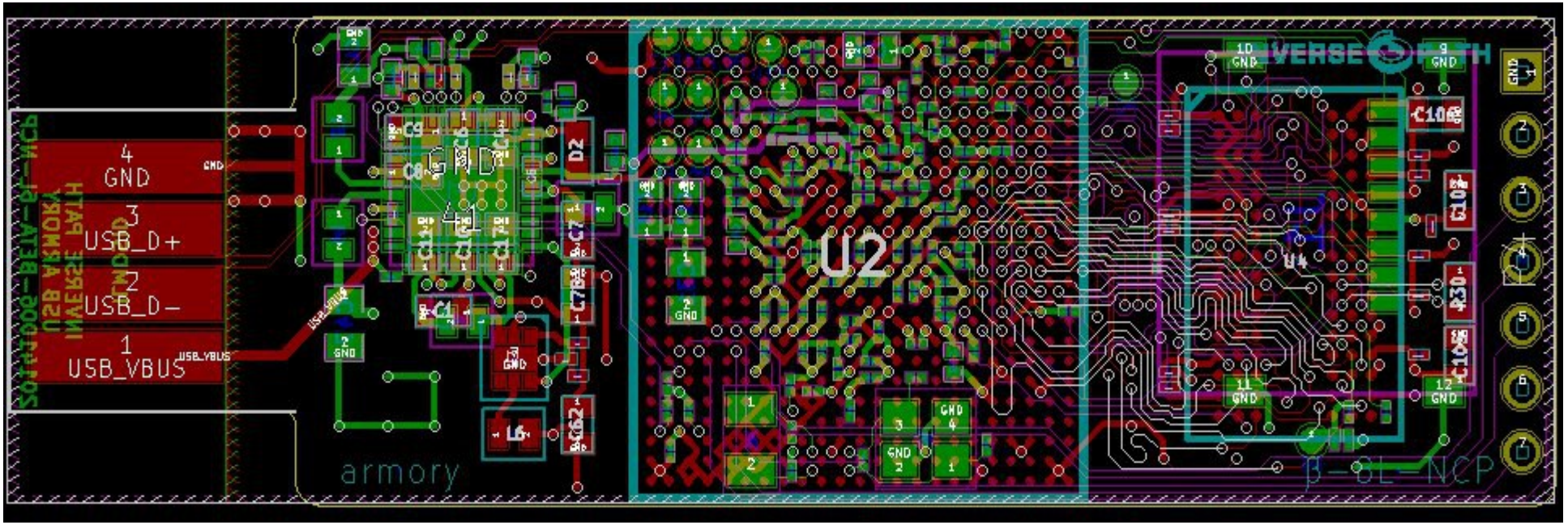


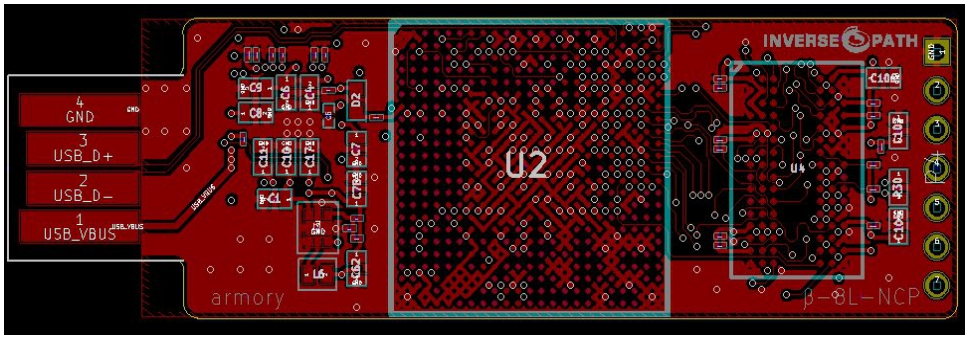


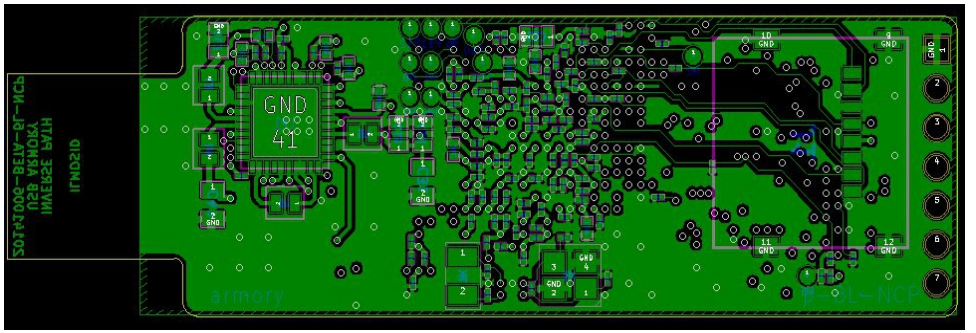
INVERSE PATH

Forging the USB armory

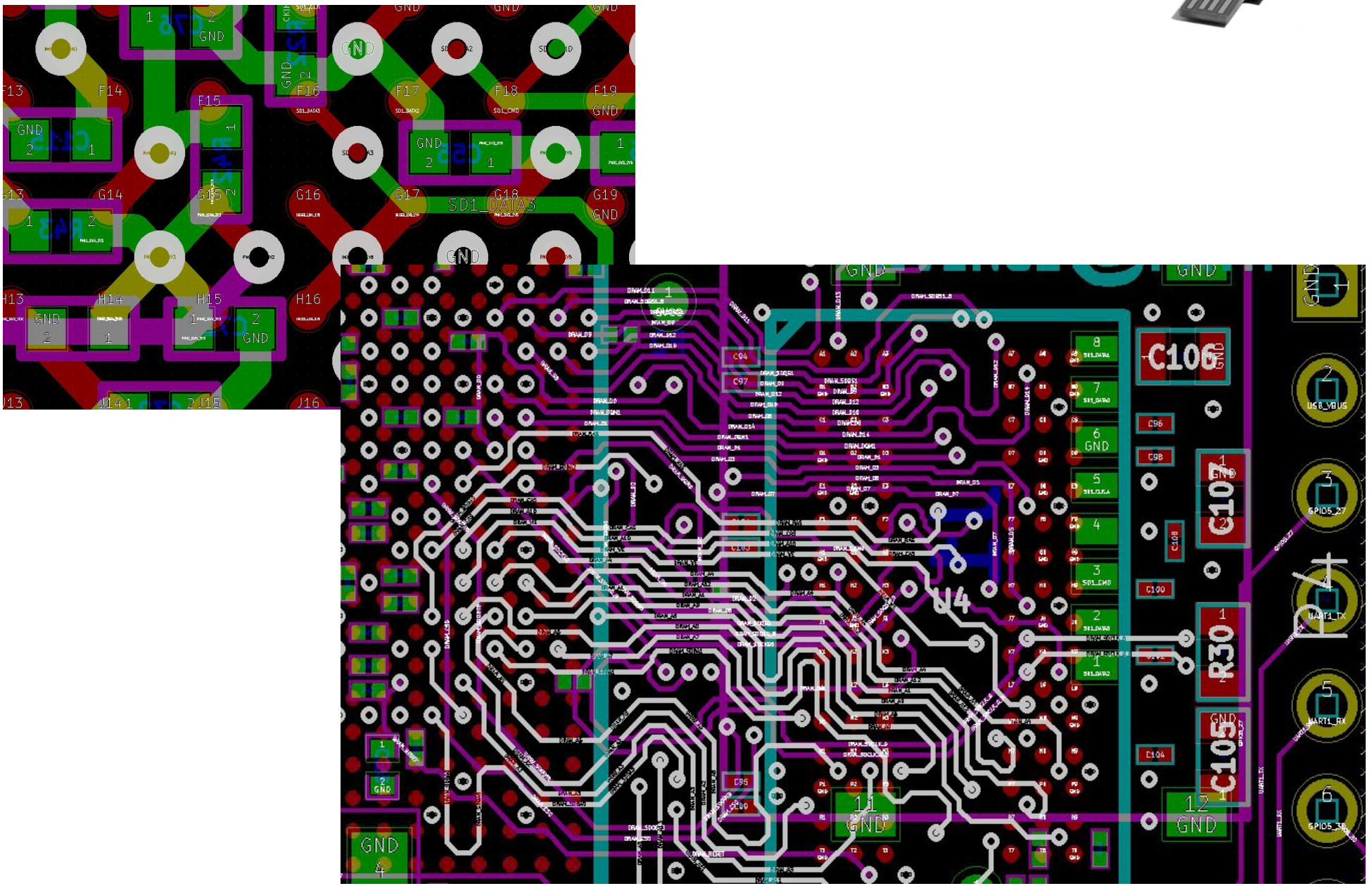
INVERSE PATH



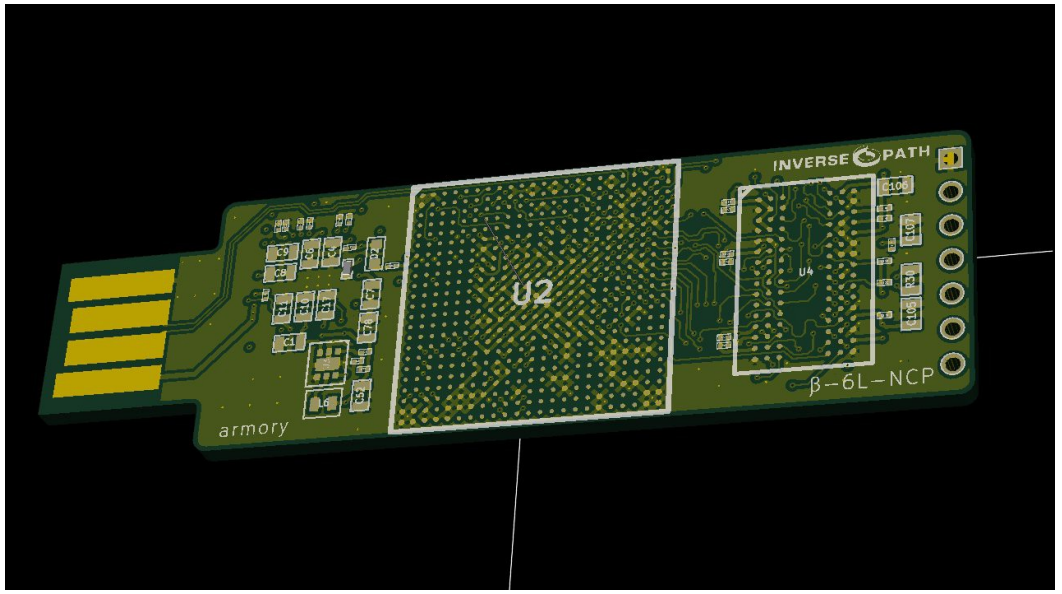


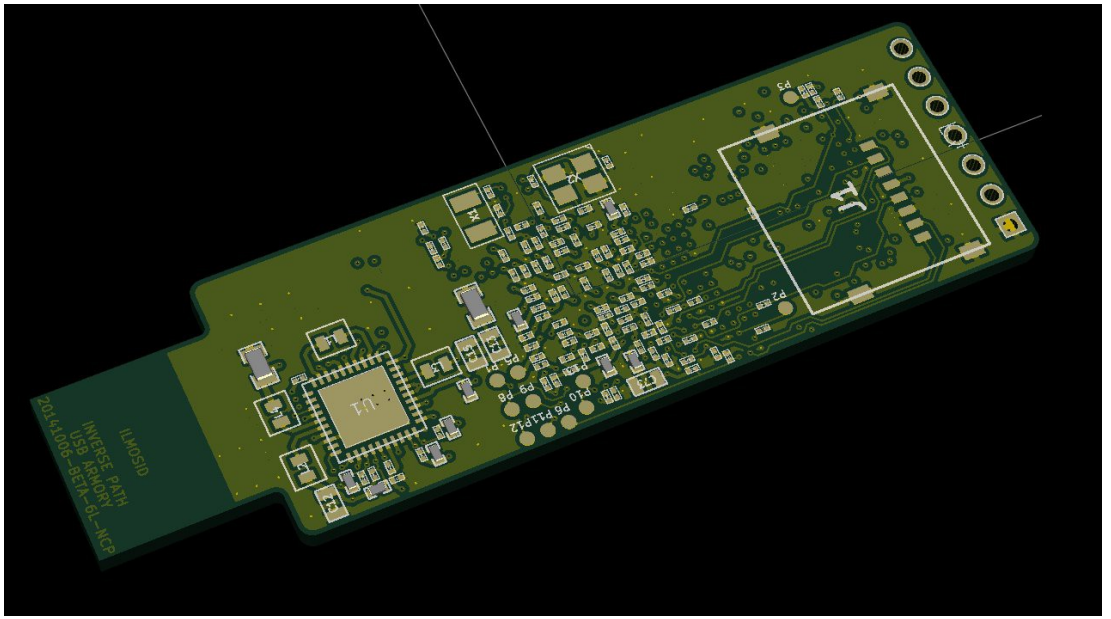


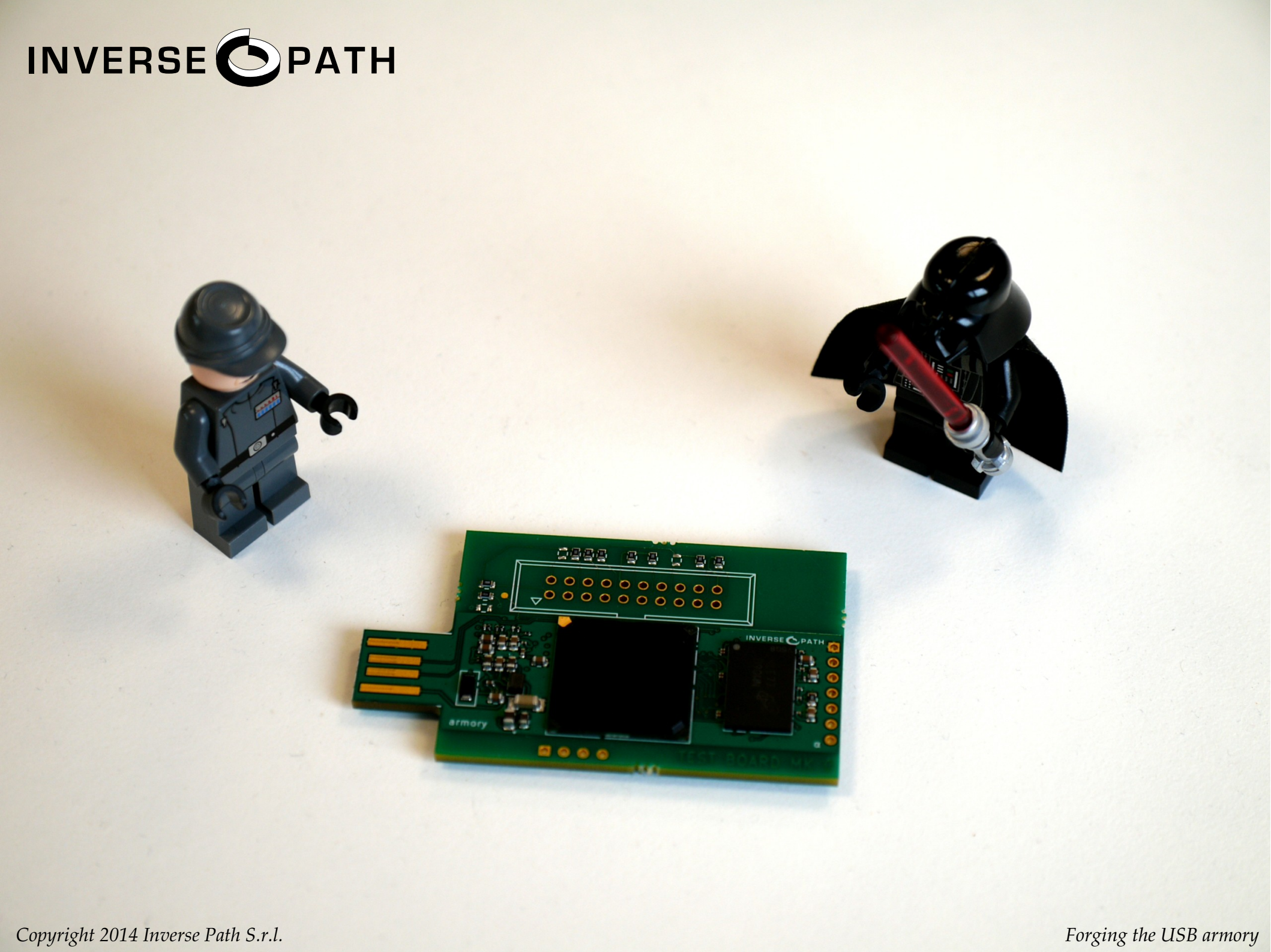
INVERSE PATH



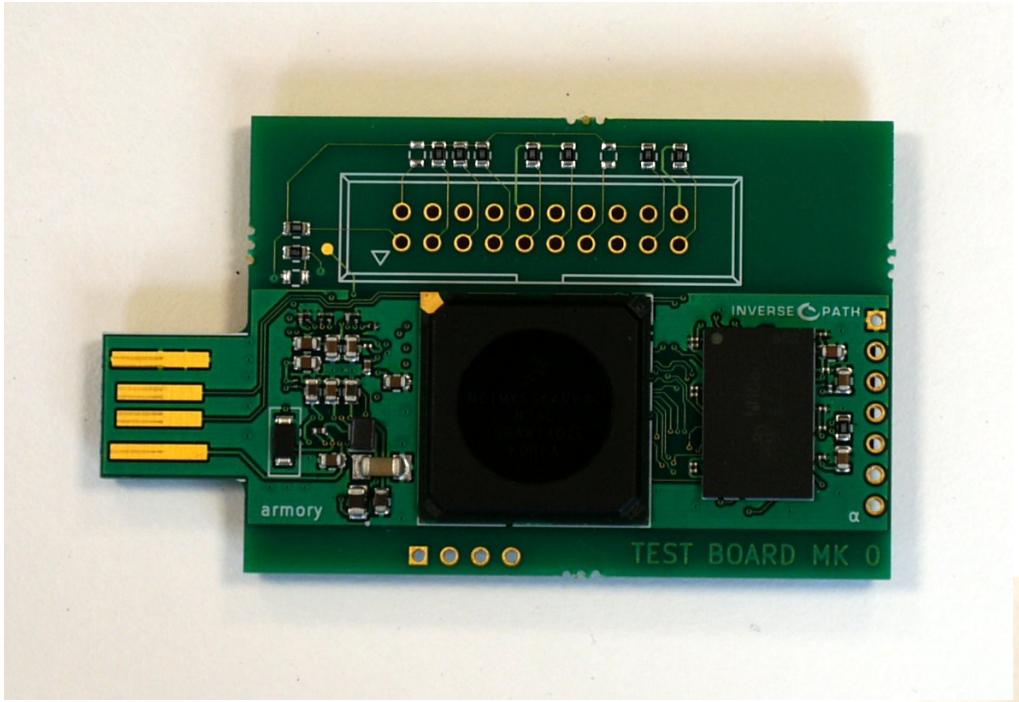
INVERSE PATH

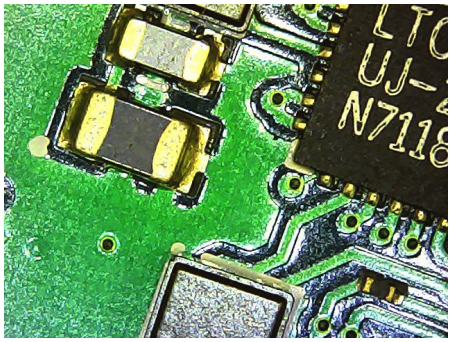


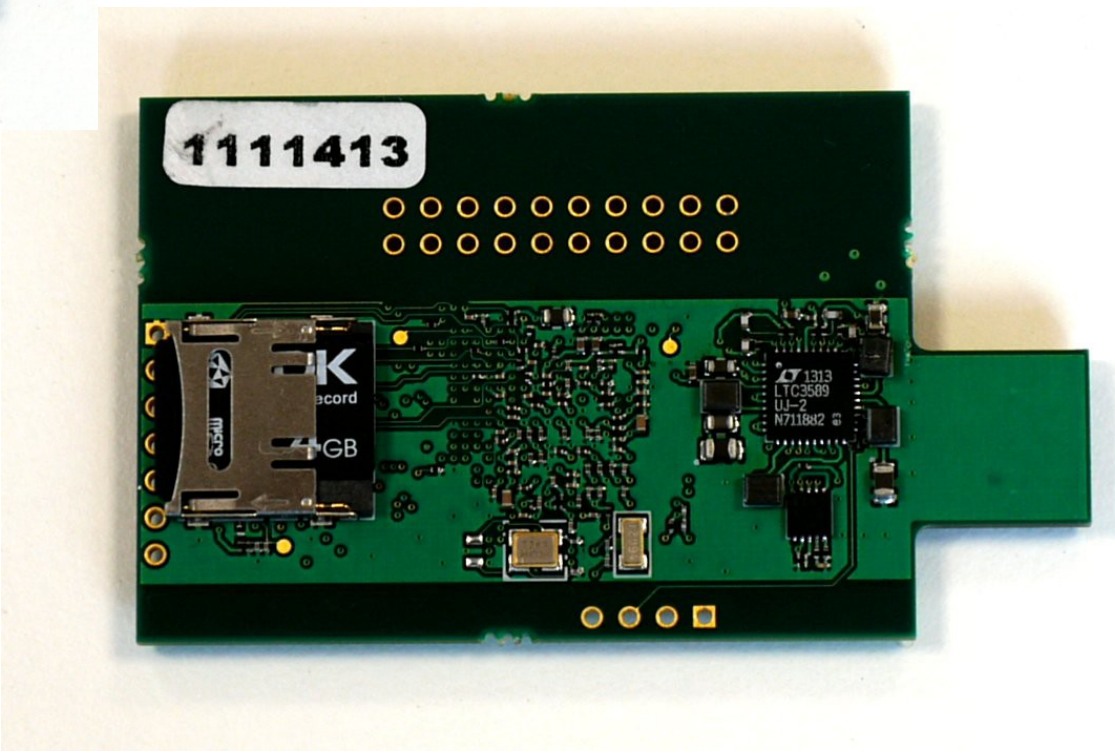


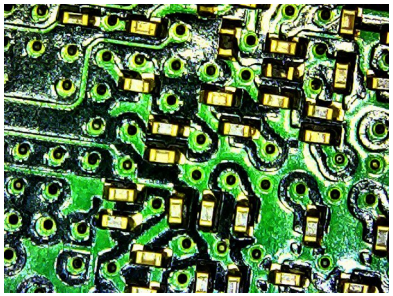


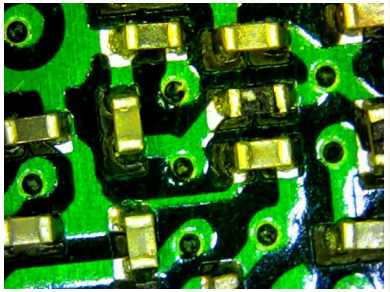
INVERSE PATH

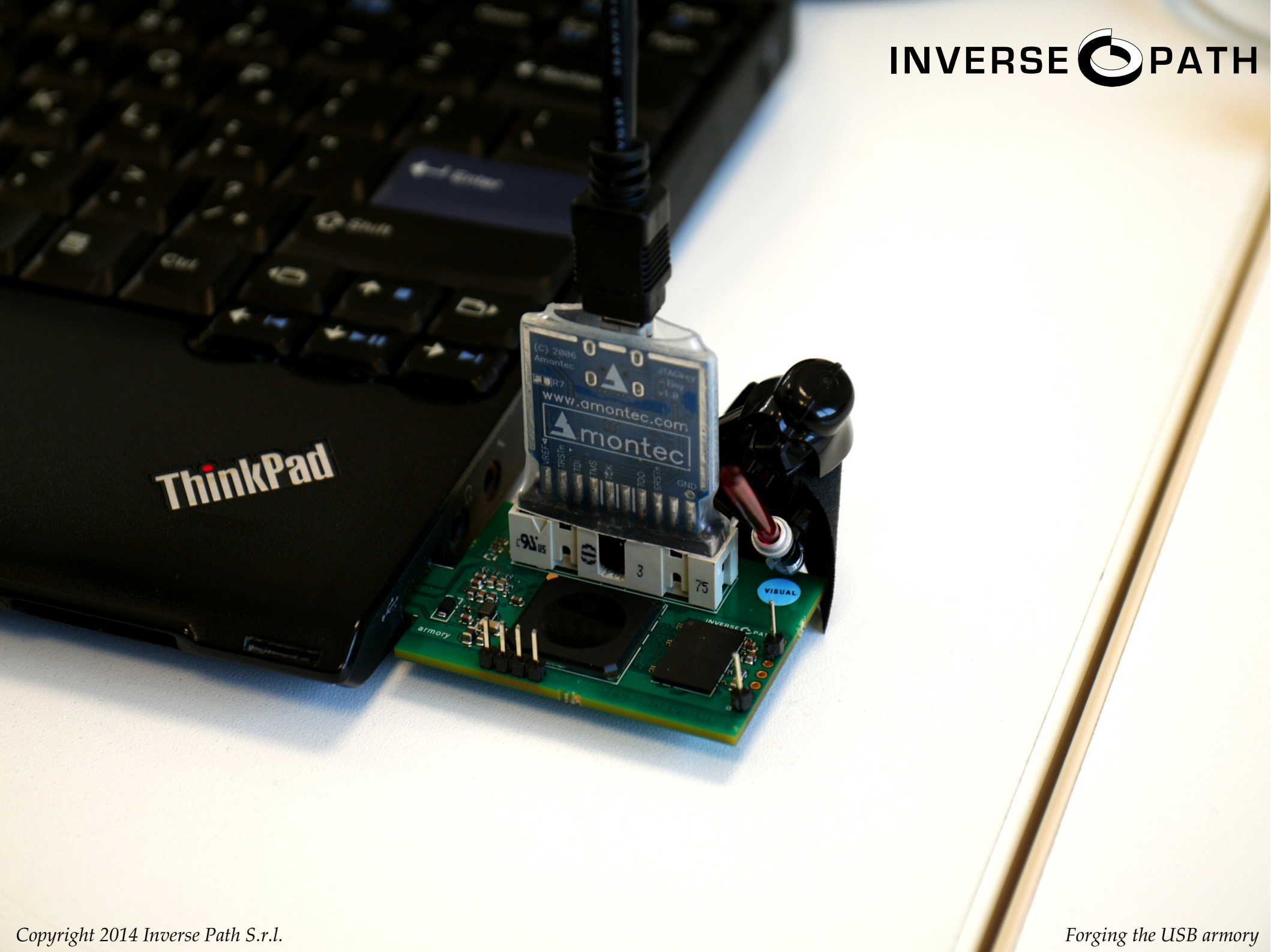


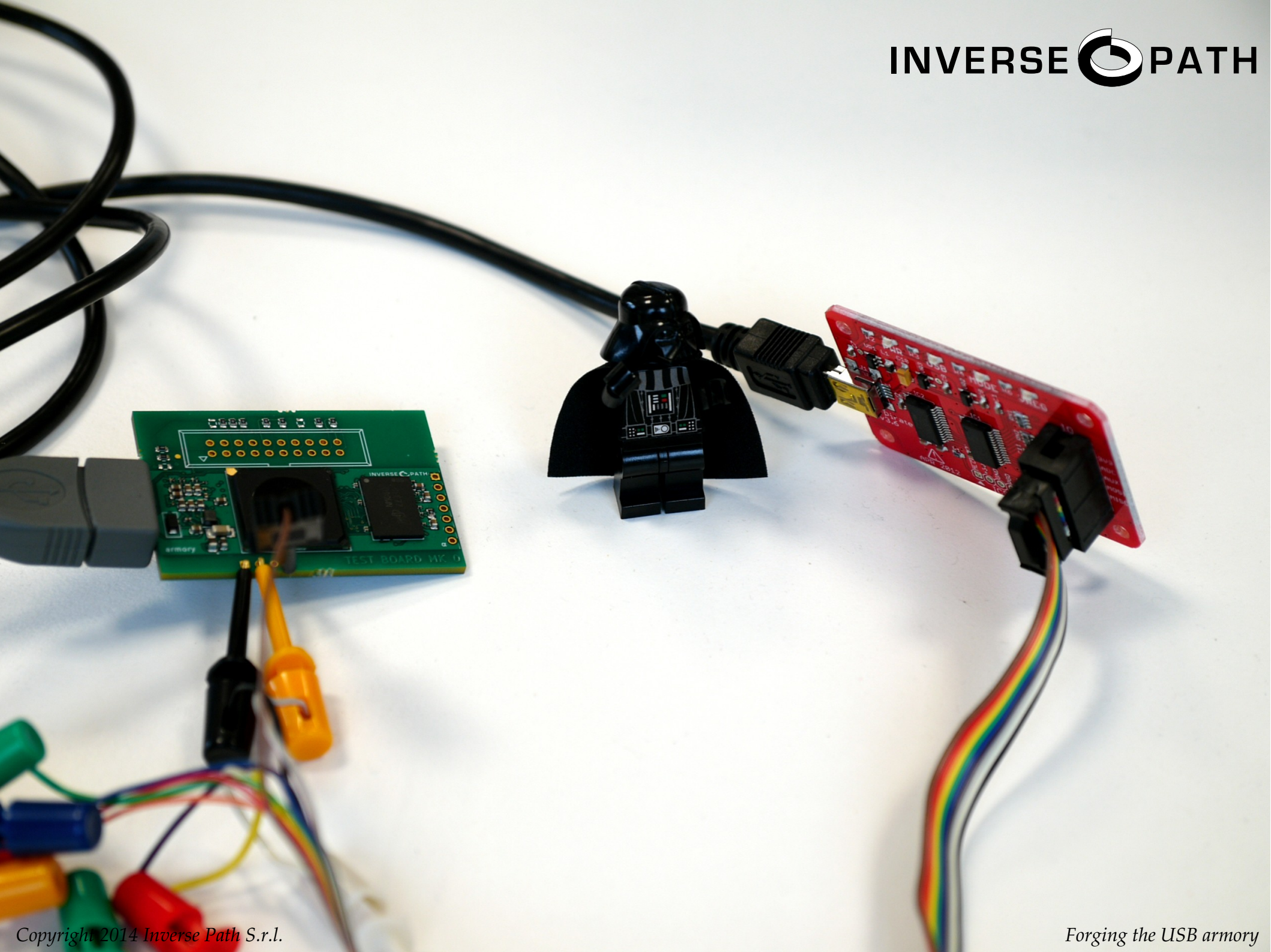


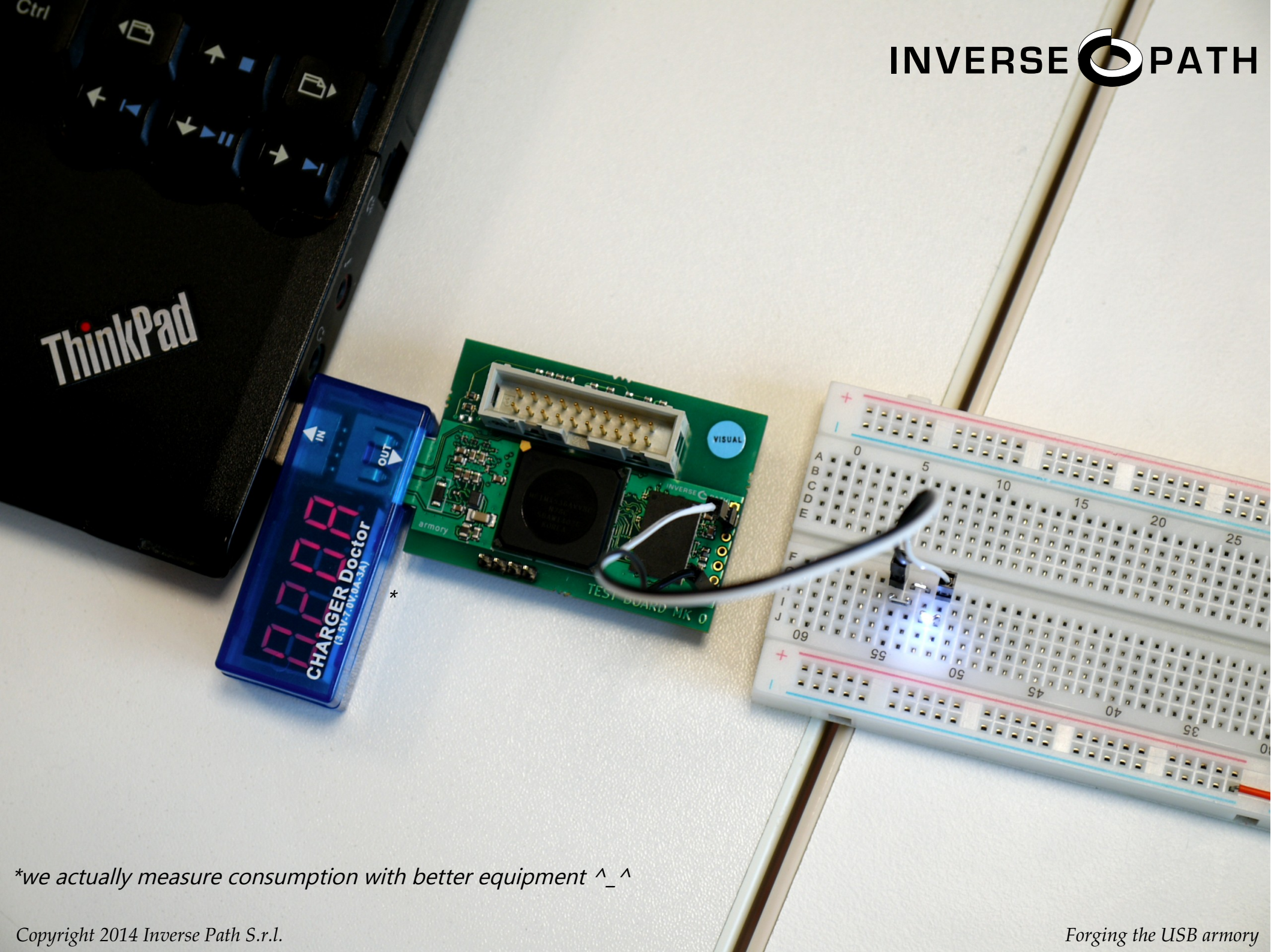






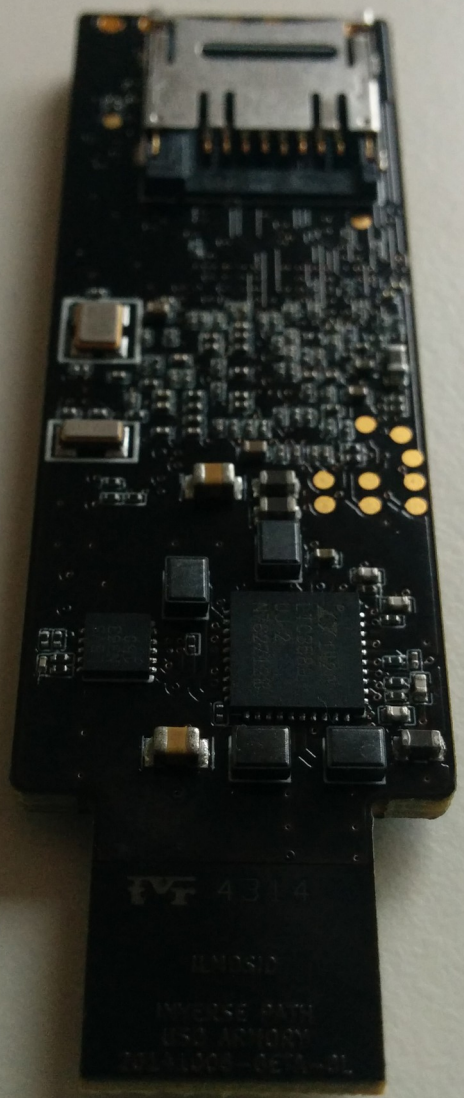


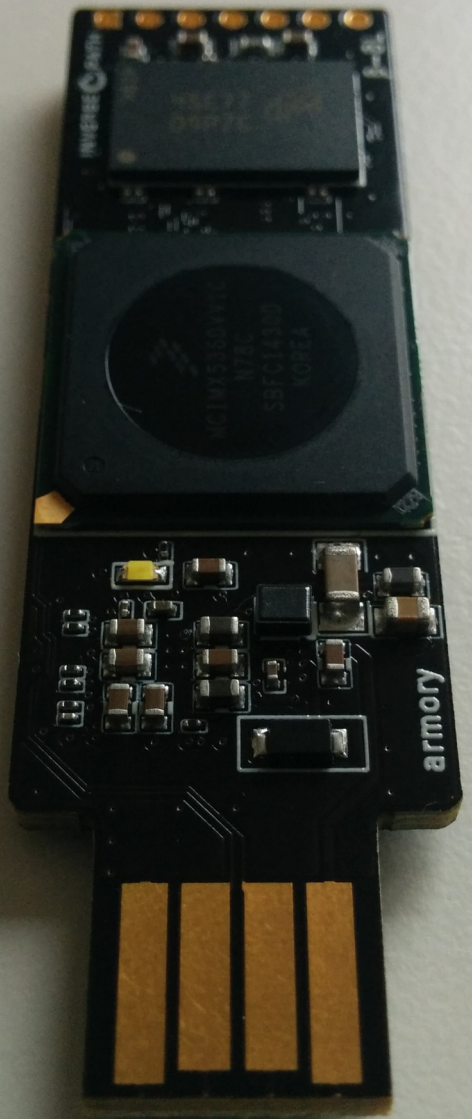




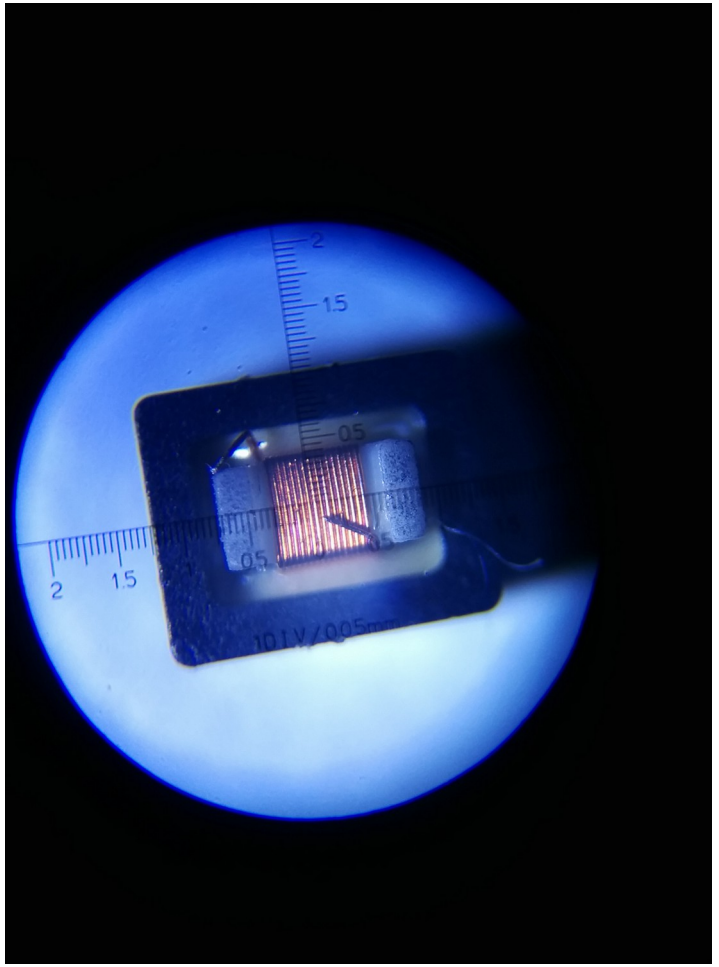
*we actually measure consumption with better equipment ^_^

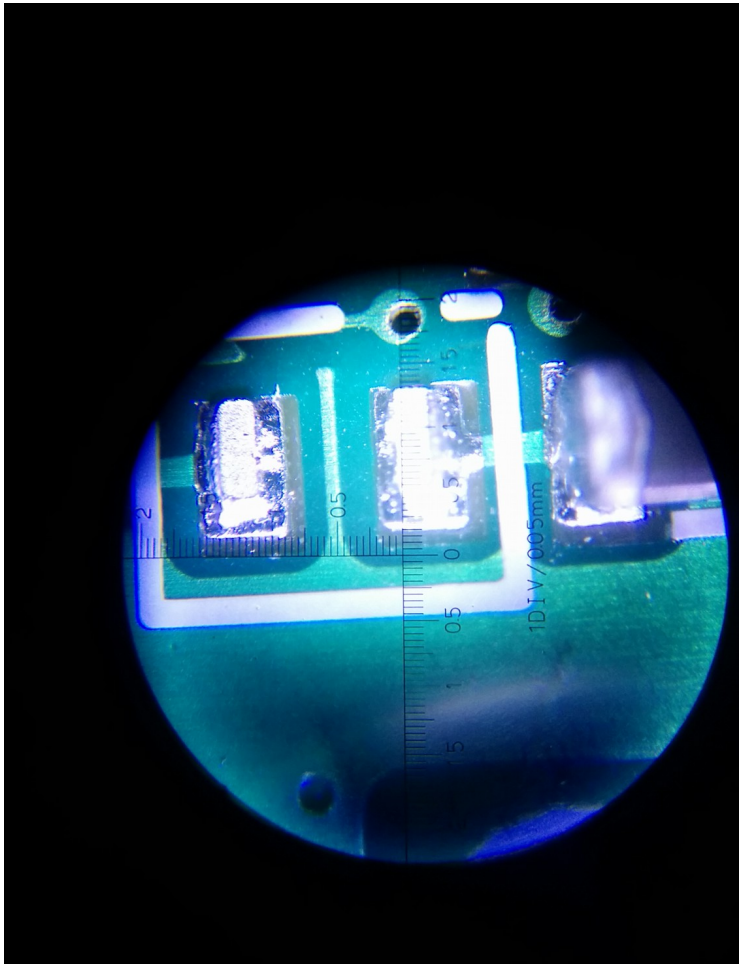
INVERSE PATH





INVERSE PATH

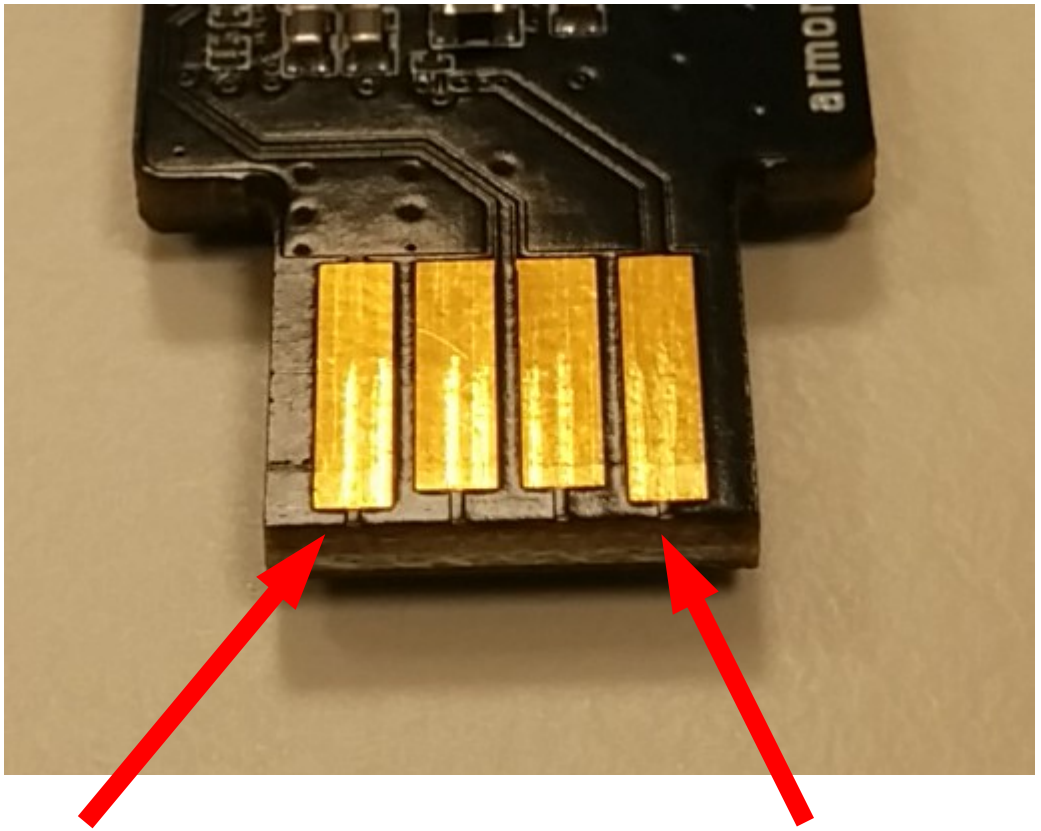




lessons learned #1

tiny inductors are fragile

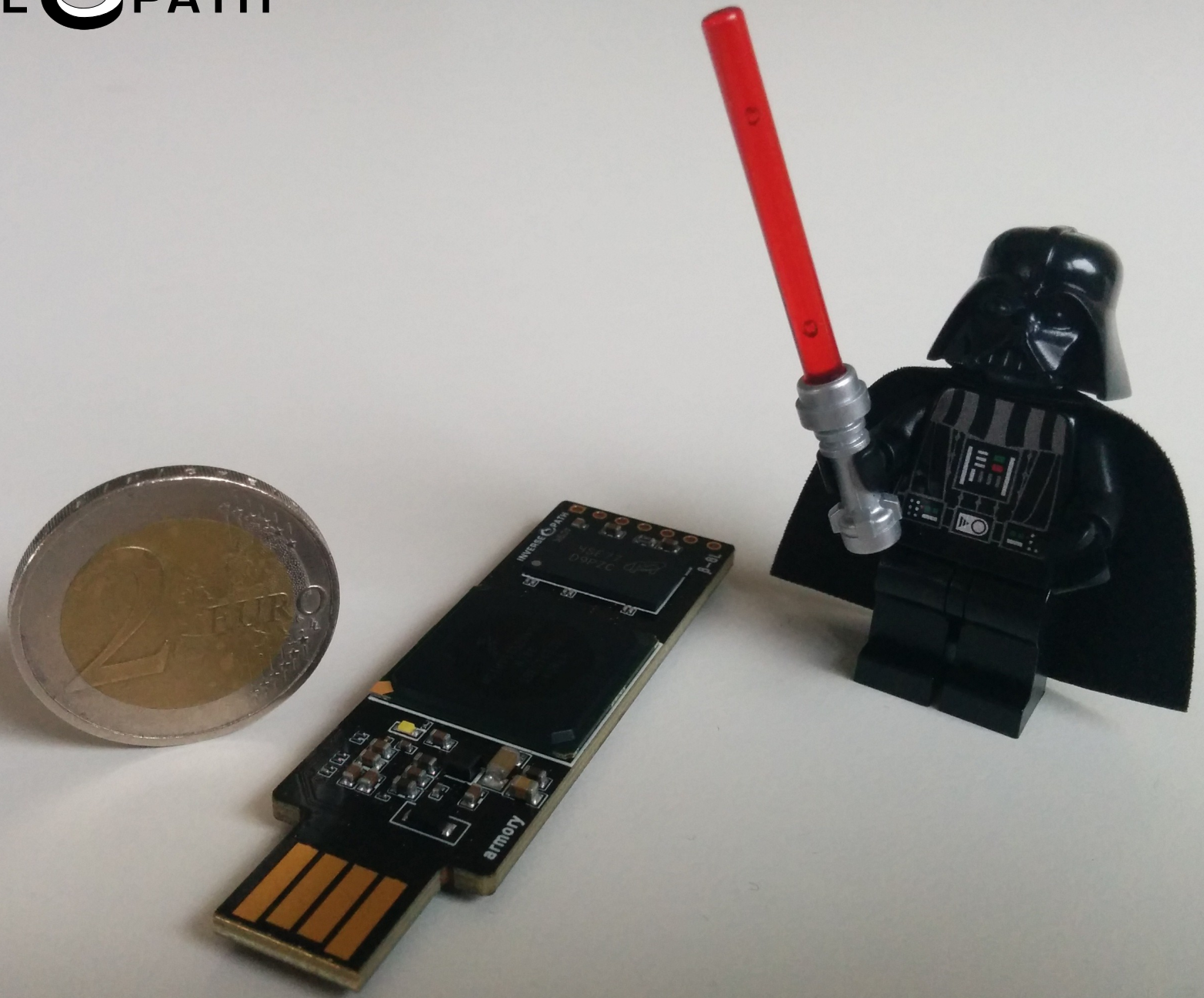
INVERSE PATH



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>