Hardware Trojan Attacks with PCBs: Theory and experimental evaluation

Dominik Klein

Federal Office
for Information Security

This talk is based on

Ievgen Kabin, Jan Schaeffner, Alkistis Sigourou, Dmytro Petryk, Zoya Dyka, Peter Langendoerfer
Leibniz Institute for High Performance Microelectronics (IHP), Frankfurt (Oder)

Dominik Klein, Sven Freud
Bundesamt für Sicherheit in der Informationstechnik, Bonn

Stealth Attacks on PCBs: An experimental plausability analysis. CSR 2024.

Technical Report: Prüfung von Manipulationsmöglichkeiten von Hardware in verteilten Fertigungsprozessen (**PANDA**)

Bundesamt für Sicherheit in der Informationstechnik, Bonn

The Bloomberg Report(s)

Businessweek | Feature

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley

Apple, Amazon deny Bloomberg report on Chinese hardware attack

By **Reuters**

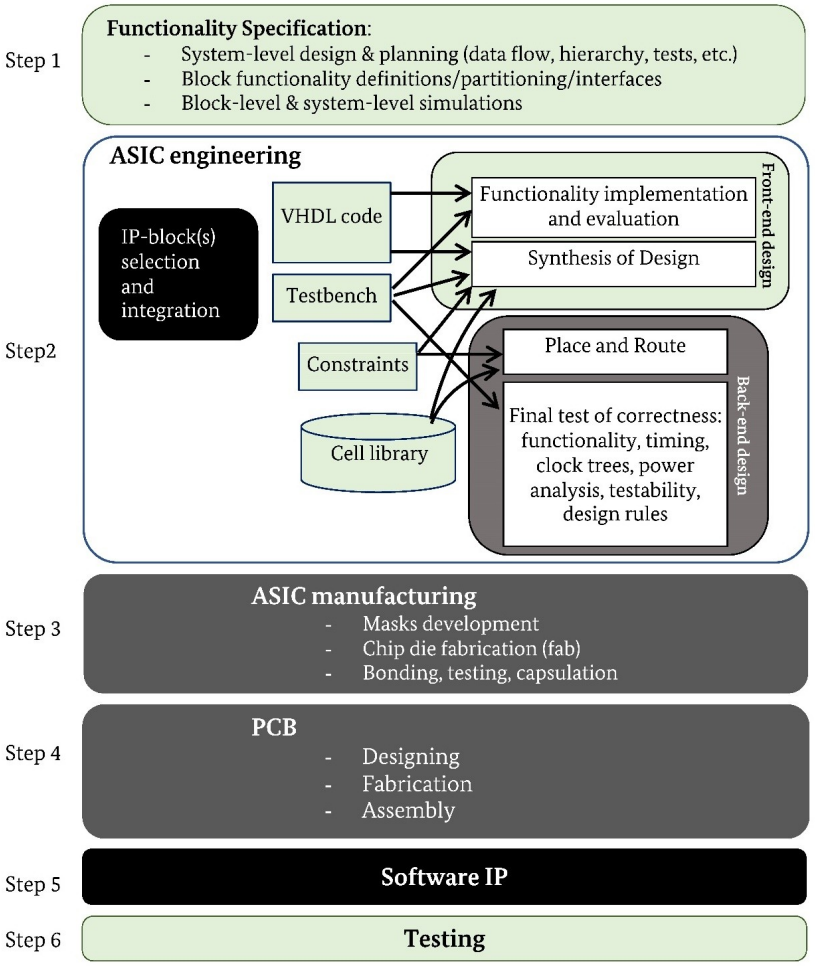
October 4, 2018 11:11 PM UTC · Updated ago

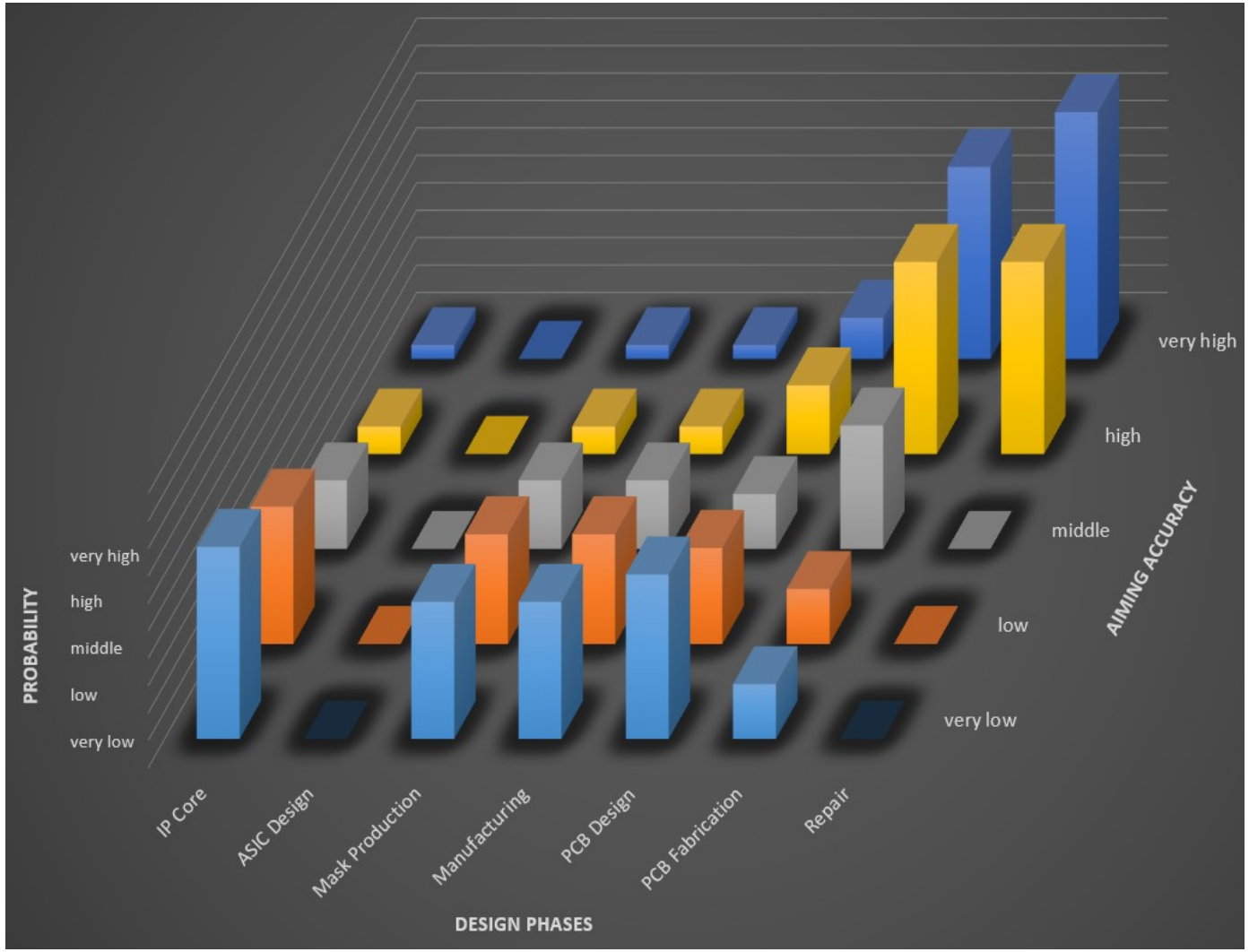
Aa

Chip Supply Chain Risks & Experiments

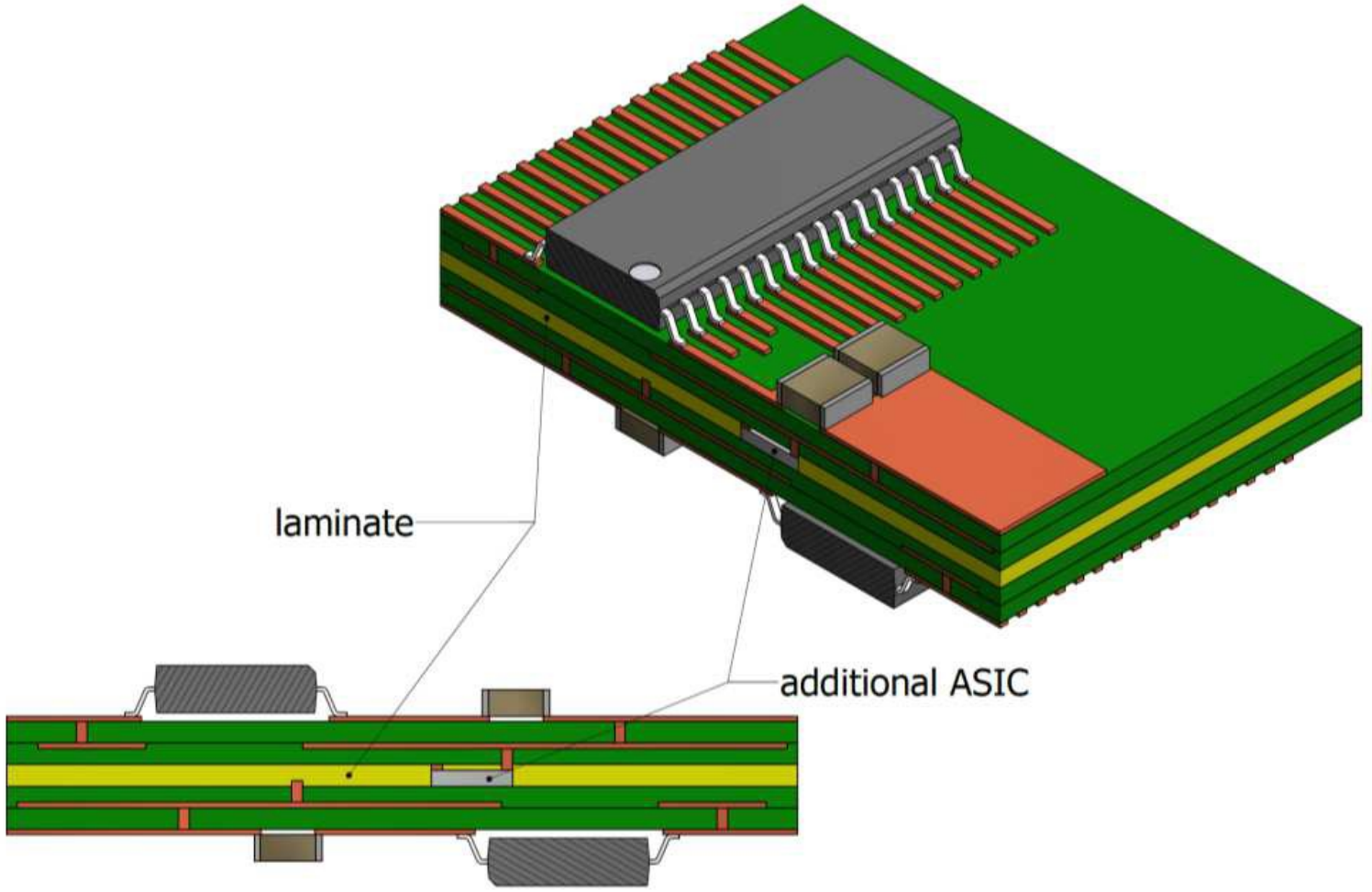
- **What is the current threat landscape in the chip supply-chain?**
  - *exclude* insider threats
- **What about detection that has the ability to *scale*?**
  - visual inspection
  - x-ray imaging
- **Two Experiments:**
  - detection of trojan in FPGA
  - hiding and detecting chips in PCBs (only physical placement!)

Chip Supply Chain Risks



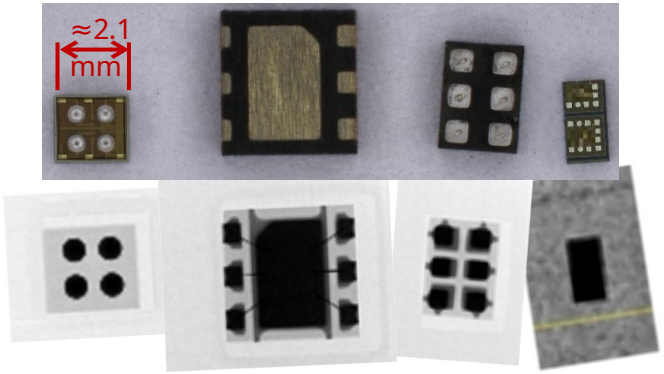


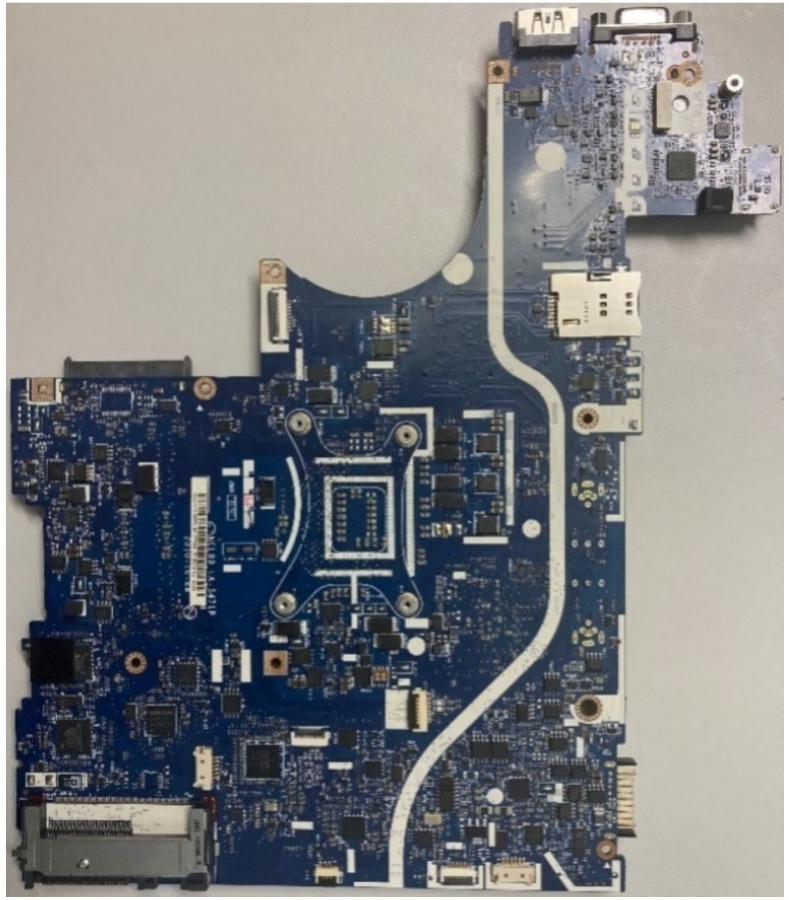
PCB Trojan



Experiments

- notebook mainboard
- various smaller chips

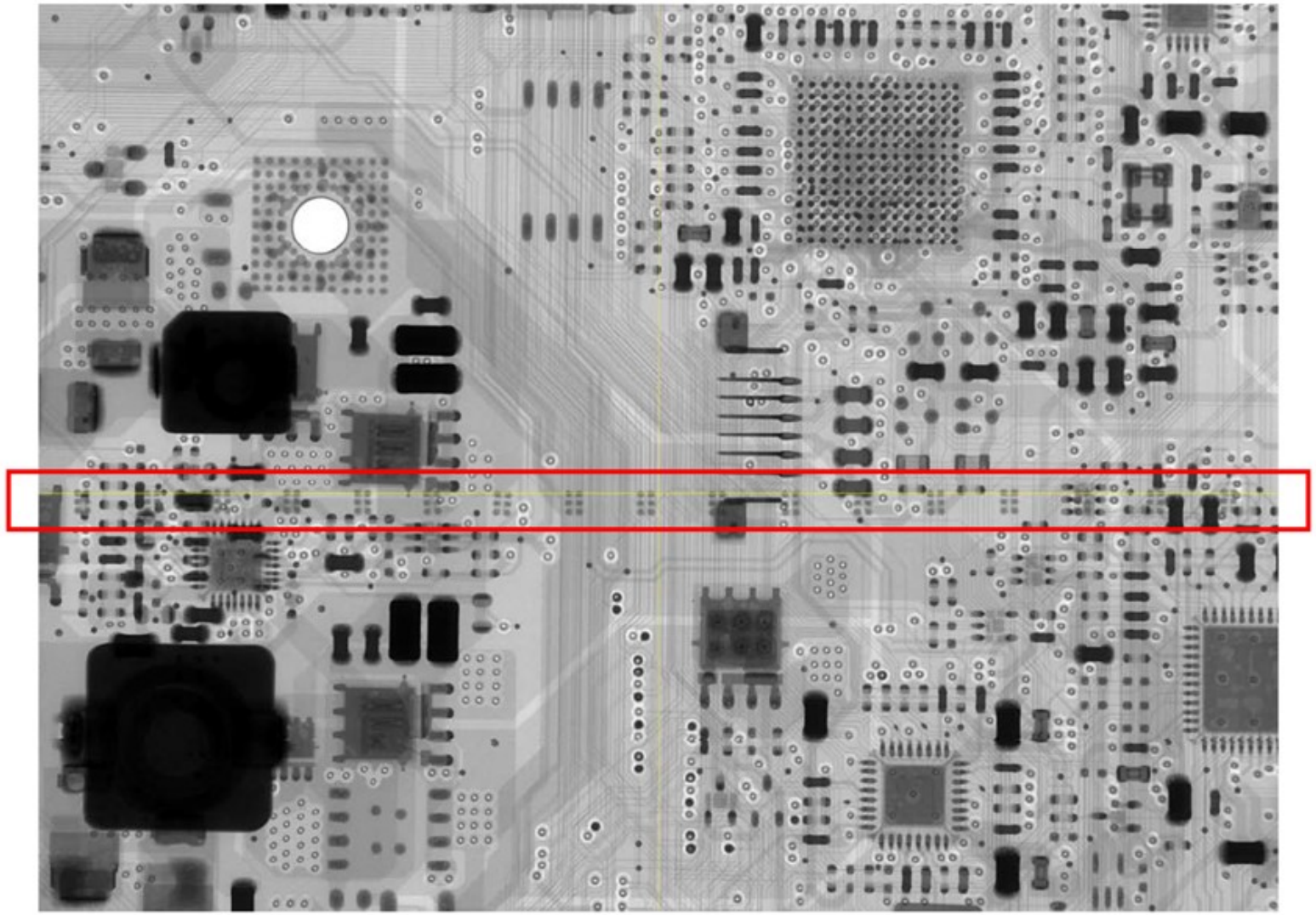




Chips on the PCB

some chips can be easily
spotted on X-ray images,

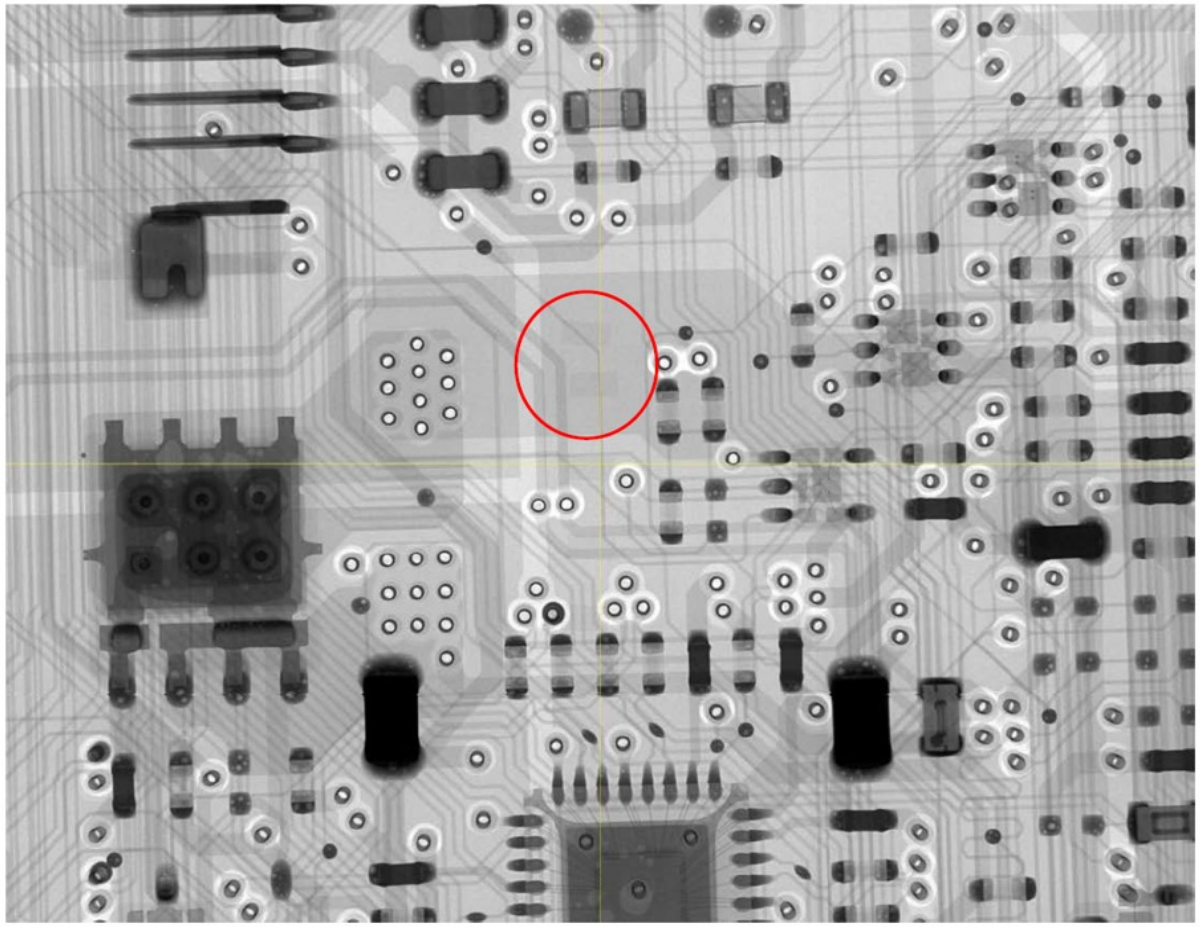
(here for an NXP A1006TL/TA1NXZ)

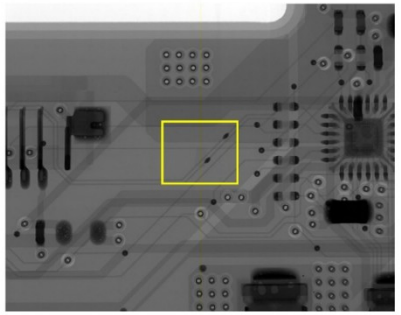


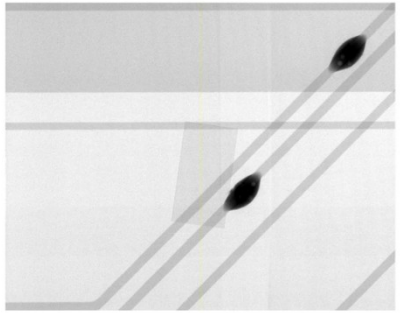
Chips on the PCB

custom chip from IHP with
aluminium bonding wires

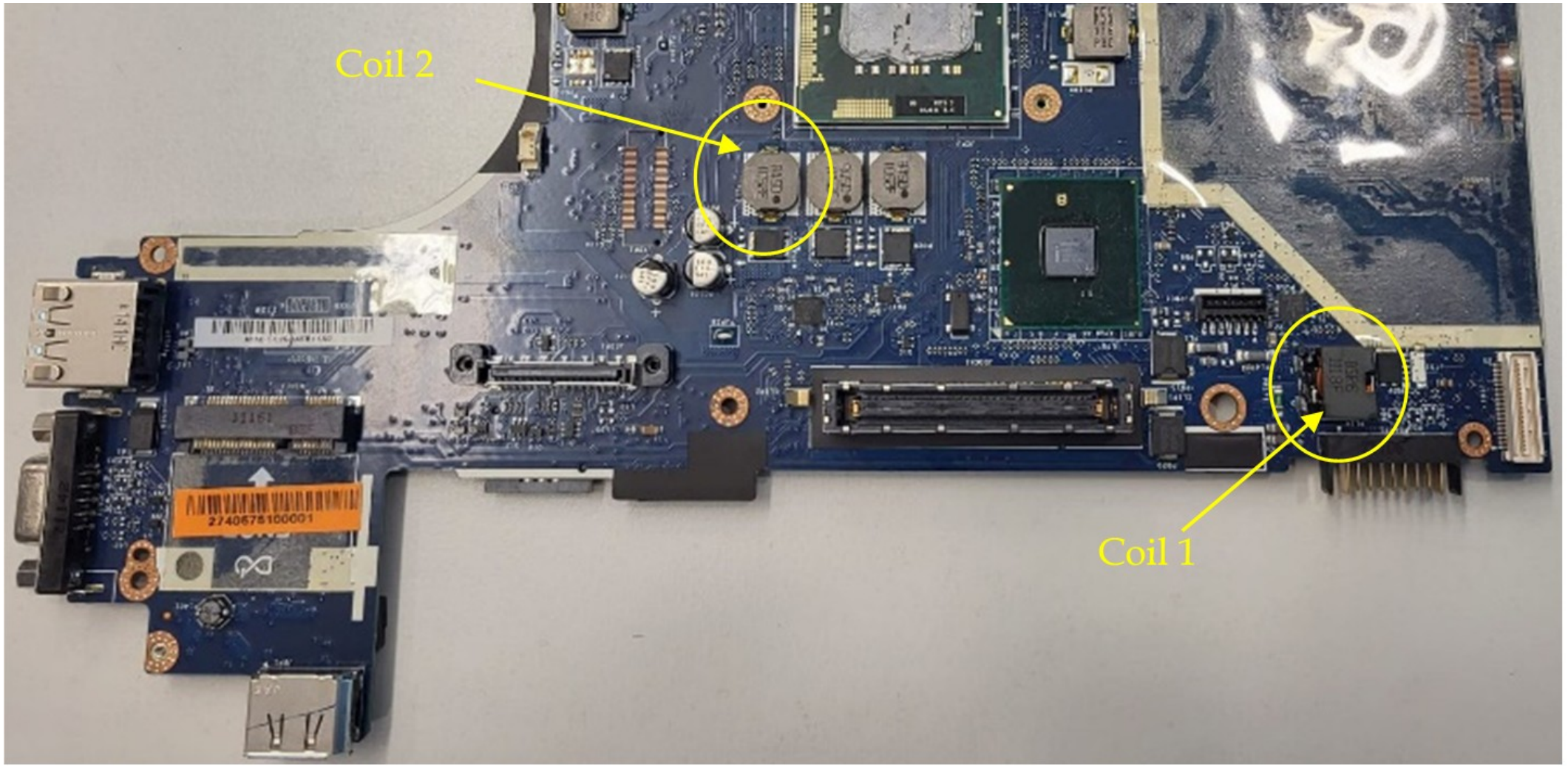
chip would likely disappear
in noise if carefully placed





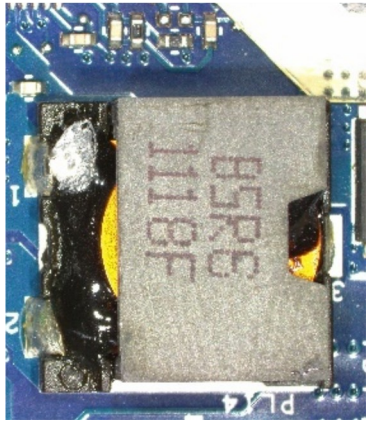


Utilizing Coils

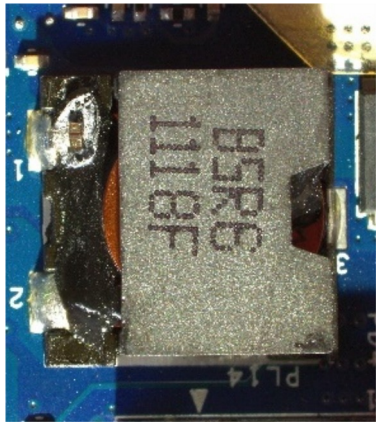


Coil 1: Hiding in Compound

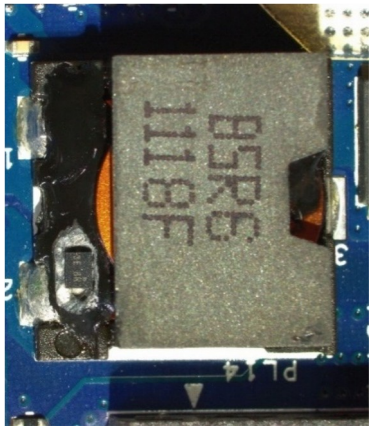
Original PCB



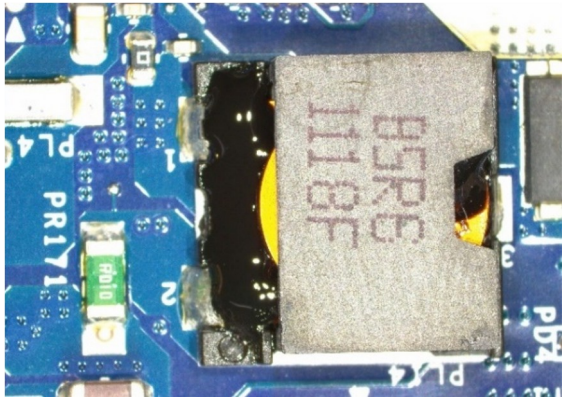
small hole drilled in potting compound



first chip attached

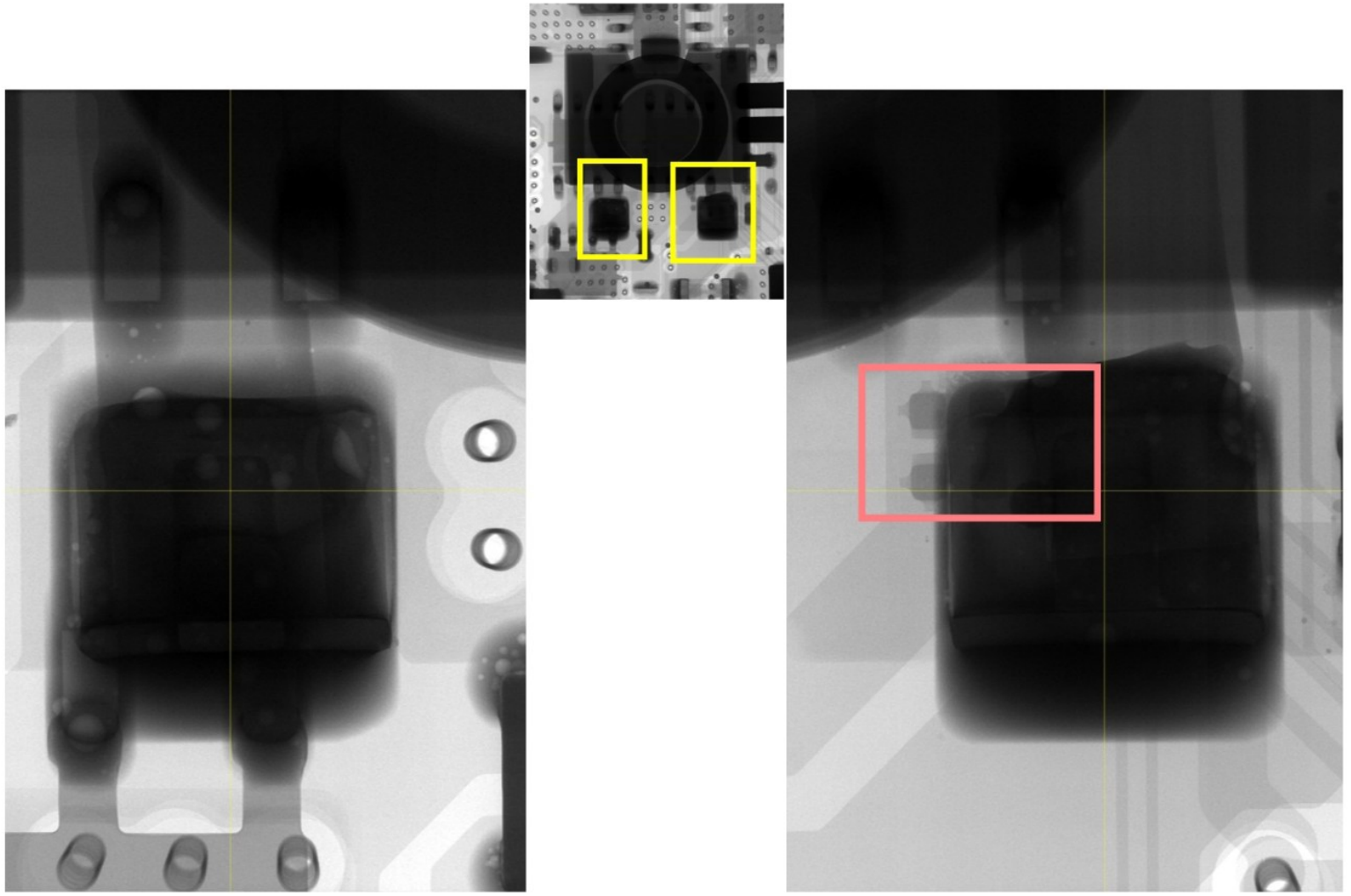


another chip attached



re-filling and cleanup

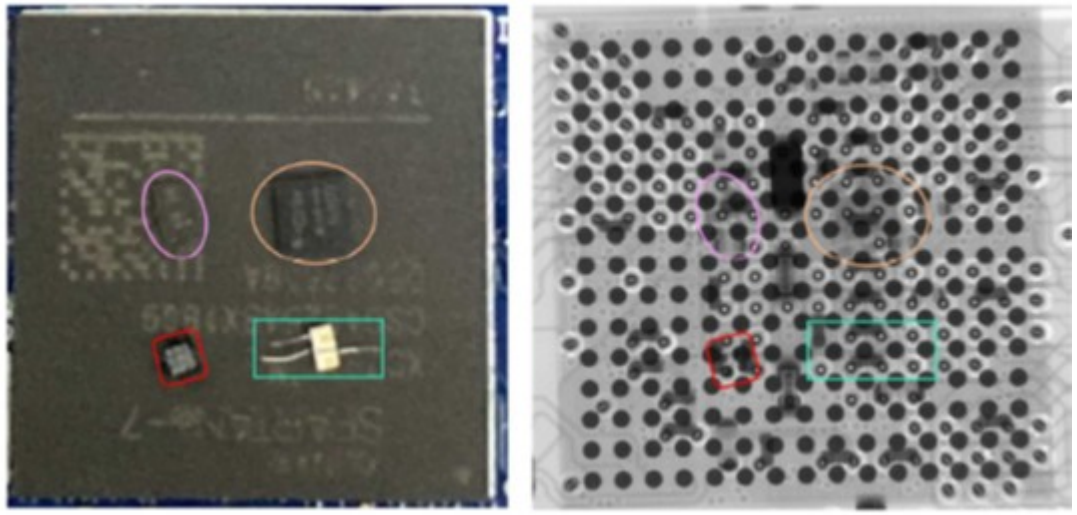
Coil 1: Hiding in Compound



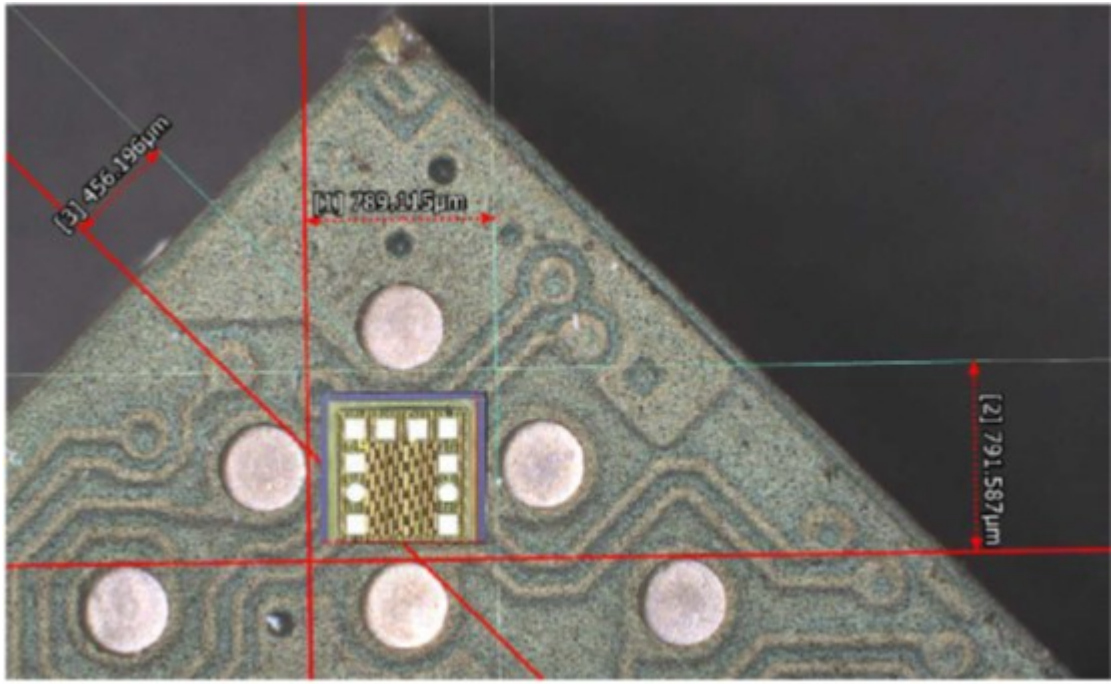
left: first chip cannot be seen in the x-ray image

right: second chip is visible in the x-ray image (cf. red rectangle) but difficult to spot

Hiding within BGA



Optical (left) and x-ray (right) images



Spartan 7 in BGA package (backside): Using the distance between pins to hide an extra chip

Summary

- Bloomberg report questionable, but attack seems technically feasible
- executed properly, PCB trojans would likely often be undetected
- only physical placement investigated here
  - electrical and logical integration, and interaction with main system left open
- countermeasures:
  - trustworthy suppliers
  - in-depth analysis for mission-critical systems
  - *digital sovereignty*

Thank you for your attention!

Dominik Klein
Head of Division

Division T11 – Chip Security

Dominik.Klein@bsi.bund.de
Phone: +49 228 9582-0

Federal Office for Information Security (BSI)
Godesberger Allee 87, 53175 Bonn

www.bsi.bund.de

Federal Office
for Information Security

Follow us: