TRUSTED ELECTRONICS

Dr. Horst A. Gieser – Head of Analysis & Test at Fraunhofer EMFT

Co-Chair of Analysis Group Velektronik – Vertrauen ist besser

Chair of Analysis Group Fraunhofer TRAICT -Project

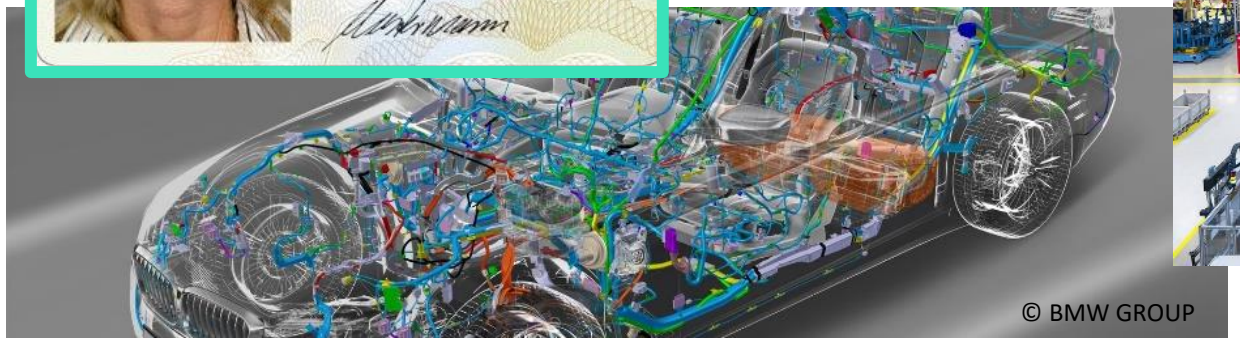
EMFT-Coordinator Trusted Electronics Bavaria

Horst.Gieser@emft.fraunhofer.de

Session: Sustainable, Green & Trusted Electronics @

Fraunhofer Forschungsfabrik Mikroelektronik Deutschland edacentrum gefördert vom Bundesministerium für Bildung und Forschung Fraunhofer EMFT

Today Electronics Everywhere – requiring different levels of trust

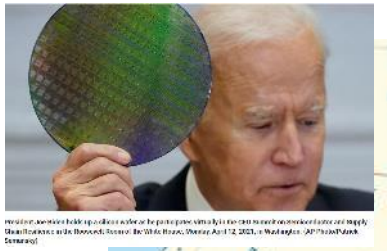


https://hbr.org/2021/02
/why-were-in-the-midst-of-a-global-semiconductor-shortage

Fraunhofer
Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom
Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Today: Global Microelectronics – Global Value – Local Risk

Digital Souveregnty Europe



FoxNews 13.10.2021

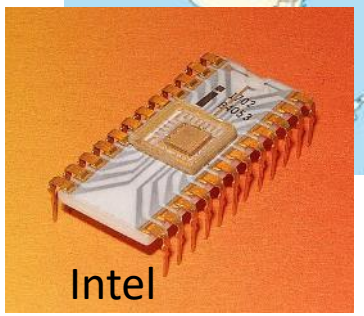
U.S.A.

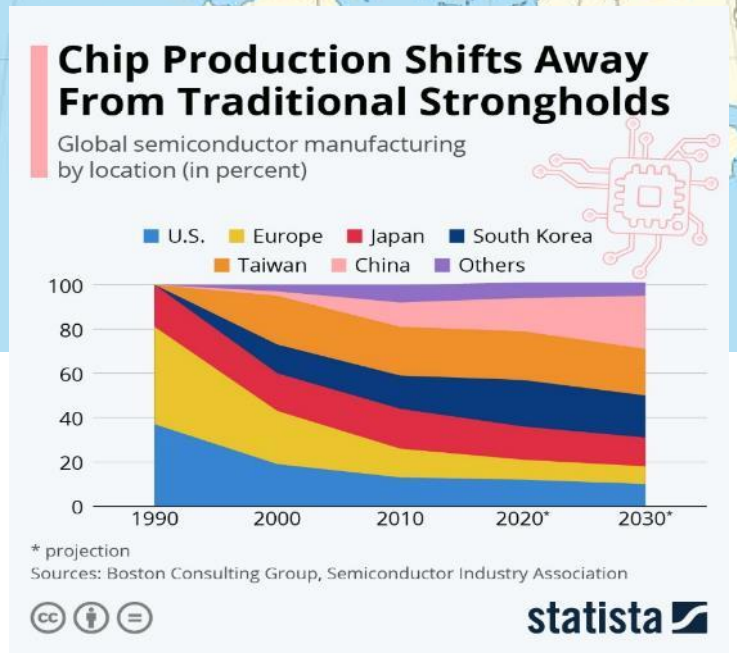
China

South Korea

Japan

Taiwan



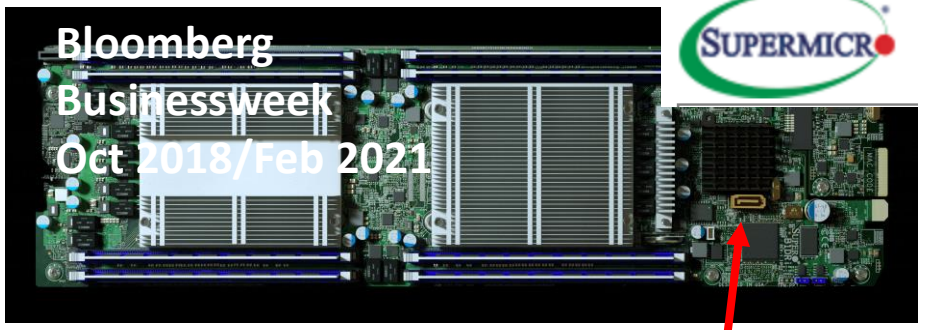


Yesterday the Citizens of Troja…

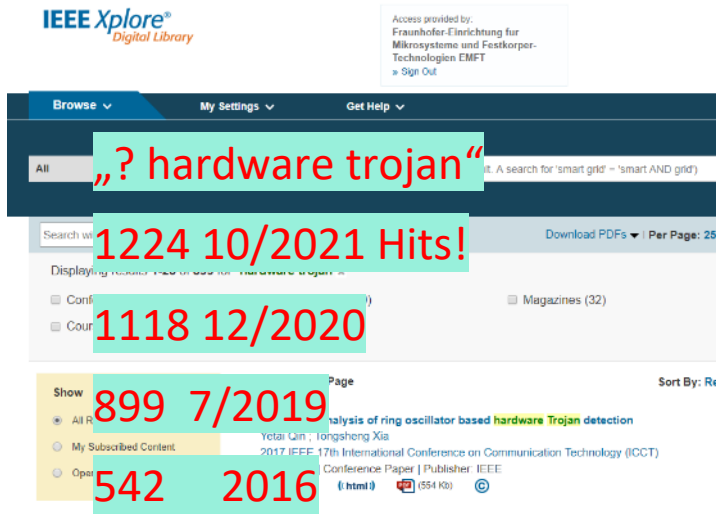
Troja. Spielfilm, USA, Malta, England, 2004, 156 Min., Regie: Wolfgang Petersen,

Today
– yes, we are vulnerable

Motivated by
NSA CottonmouthX

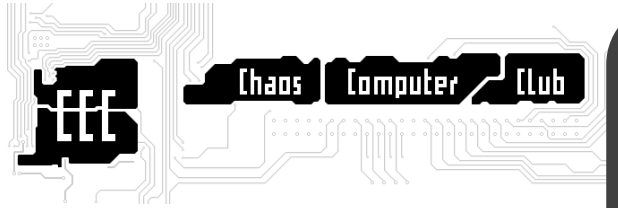


- Hundreds of new SW- virus /day
- Flaws in Design, Implementation & Supply Chain
- Compromised Hardware (Encryption, Data Leaks, Remote Control, RNG)
- Counterfeited Devices



e.g. Cyber Security

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation



Von National Security Agency - https://www.nsa.gov/resources/everyone/digital-media-center/image-galleries/places/, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=16450

Fraunhofer
Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Strong Motion for Trusted Electronics

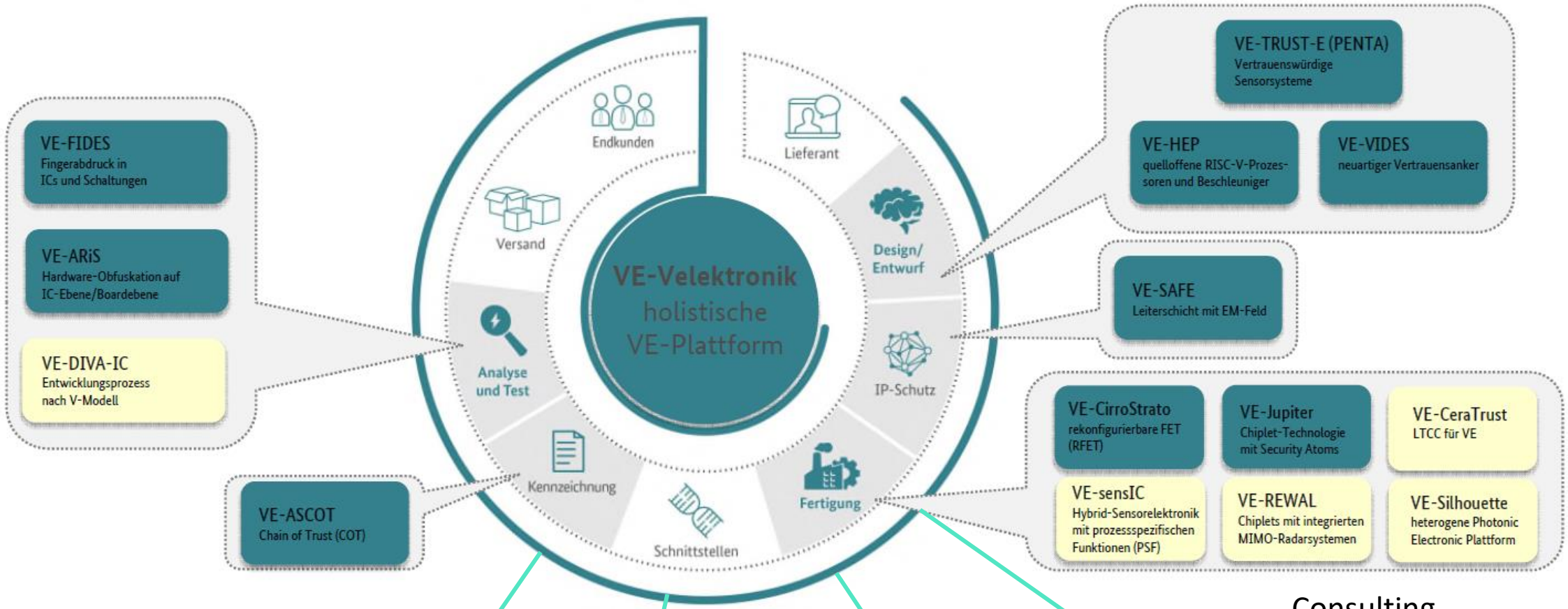
- European, national and state authorities fortunately see and fund
- Trusted Electronics as a Conditio Qua Non for Digital Souvereignty in Global Supply Chains
- Partners from Industry and Academia are sharing the vision and are joining forces building strong alliances offering solutions for trust

- Selected current projects with Fraunhofer
  - BMBF ZEUS-Program with Vertrauenswürdige Elektronik platform
  - BMBF R&D Projects SyPASS & RESEC
  - BMBF TRAICT Trusted Resource Aware ICT
  - BMBF FMD Analysis Equipment
  - Bavaria TREB Trusted Electronics Bavaria

Velektronik
Vertrauen ist besser

Fraunhofer Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Topics addressed within BMBF funded 15 ZEUS-projects



Velektronik
Vertrauen ist besser

Trust by | Design | Manufacturing | Analysis

- Consulting
- Services
- Standardization

Fraunhofer Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Fraunhofer Network 4 Advanced Analysis

Formation initiated in the FhG /BMBF TRAICT-Project

System in the Box → Transistor

Target Definition

- Conditions
- Recherche Documentation
- Analysis concept
- Preparation Prestudy

Non-Destructive

passive

- XRAY
- Ultrasonic
- Thermal
- Inductive Fingerprinting
- Eddy Current

active

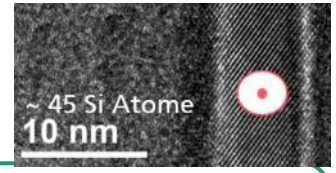
- Electrical Test
- EM-Emission
- Transient Thermal LockIn
- Photoemission
- LaserVoltageProbing

Report

Destructive

- Package – opening/removal
- Infrared analysis
- Technology analysis
- Delayering
- Chip Scanning
- Layout Extraction
- Circuit Extraction

CC-EAL6



XRAY nCT, AFAM

comparison

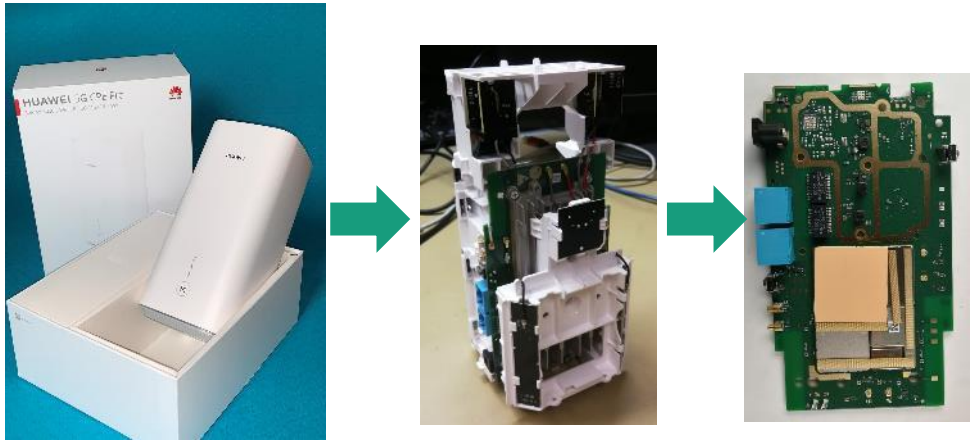
comparison

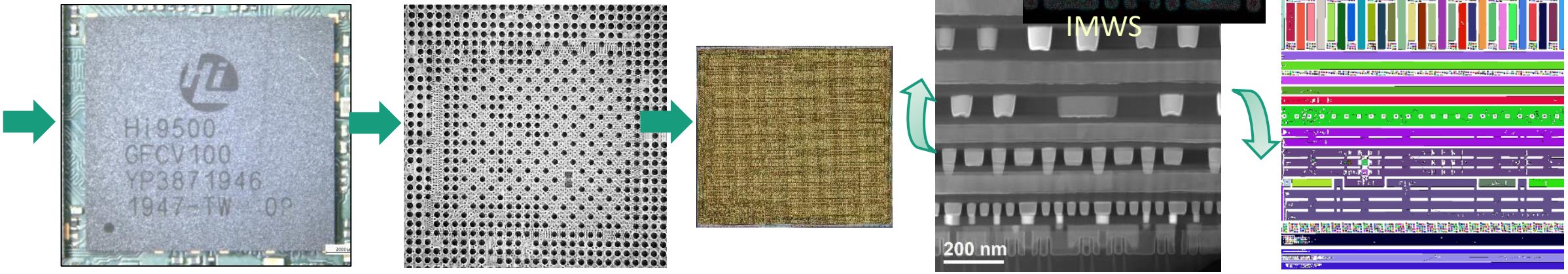
future

Fraunhofer Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Example: Tear Down of a 5G WLAN Router

- Bought from Amazon
- Remove Case and identify 5G-Components
- Demonstrate various Methods for Test and Analysis
- Active – Passive – Destructive
- Analysis of Key Component of Interest
- Technology Characterization – Trust Features
- Scanning & Partial Reconstruction of the Layout

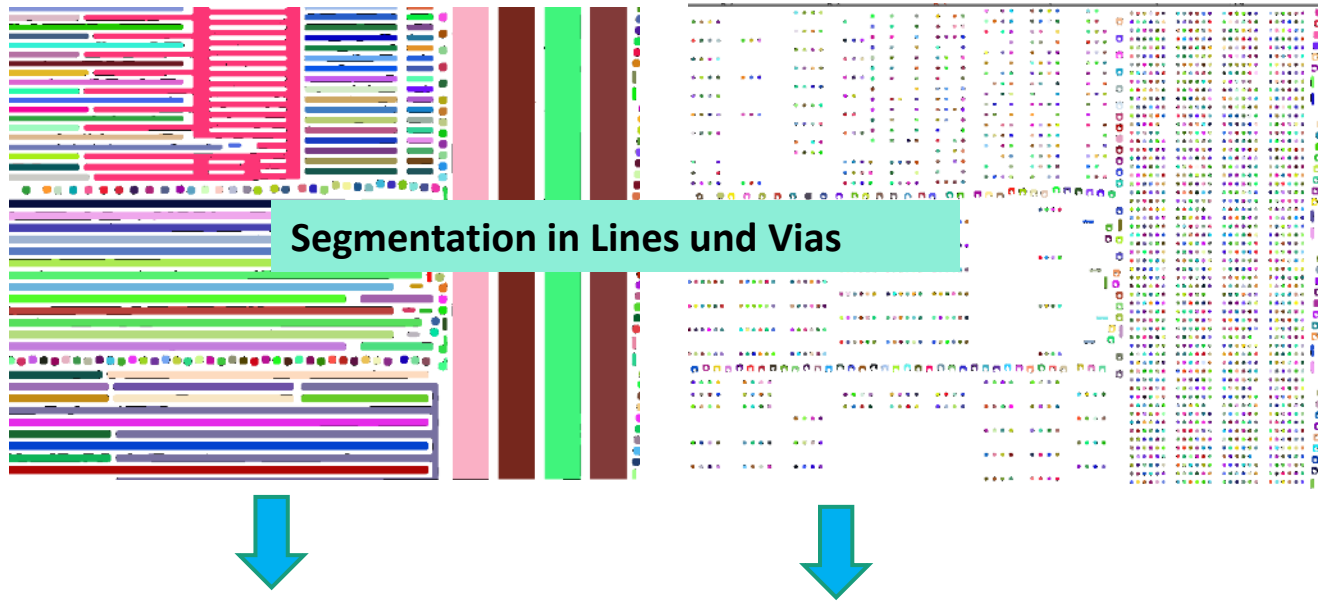




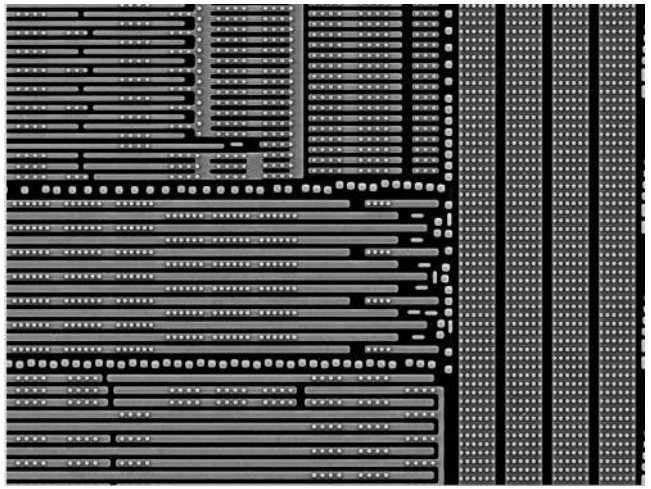
Fraunhofer
Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom
Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

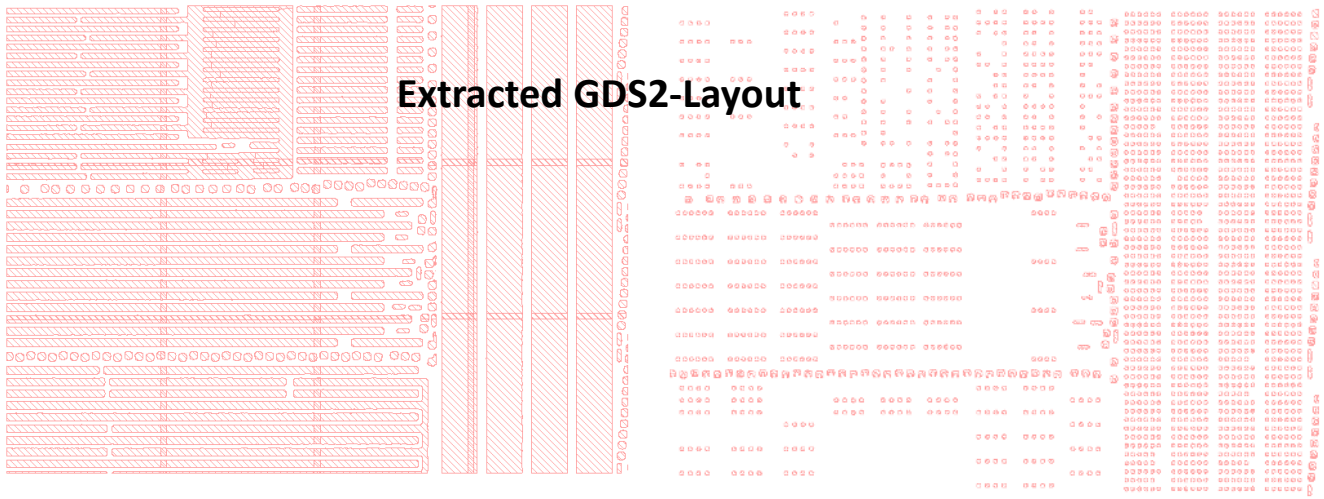
Example Scanning & Layout Reconstruction

- Large Area Scanning Raith 150TWO
- Image Stitching
- Segmentation of Pictures
- GDS2-Extraktion of Layout
- Comparison with Trusted Layout or Golden Device



SEM-
Detailbild
(3x4 Stitch)





Kontakt: Dr. Horst Gieser
Horst.Gieser@emft.fraunhofer.de
Fraunhofer
Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom Bundesministerium für Bildung und Forschung
Fraunhofer EMFT

Bundesministerium für Bildung und Forschung

RESEC Systems und Methods for Analysis and Reconstruction of Highly Integrated Security Circuits

Fraunhofer EMFT

infineon

CC EAL6

Preparation and Analysis Methods
- Delayering with Ion milling
- Chip scanning process
- Layout and circuit extraction

RE Software Platform
- Image processing
- Stitching 2D & 3D
- Analog and digital circuits analysis
- Reference analysis sample

TUM

Chip Scanner Demonstrator
- ultra fast UHR imaging
- low acceleration voltage and WD
- new high speed detectors
- high speed stage and motion platform

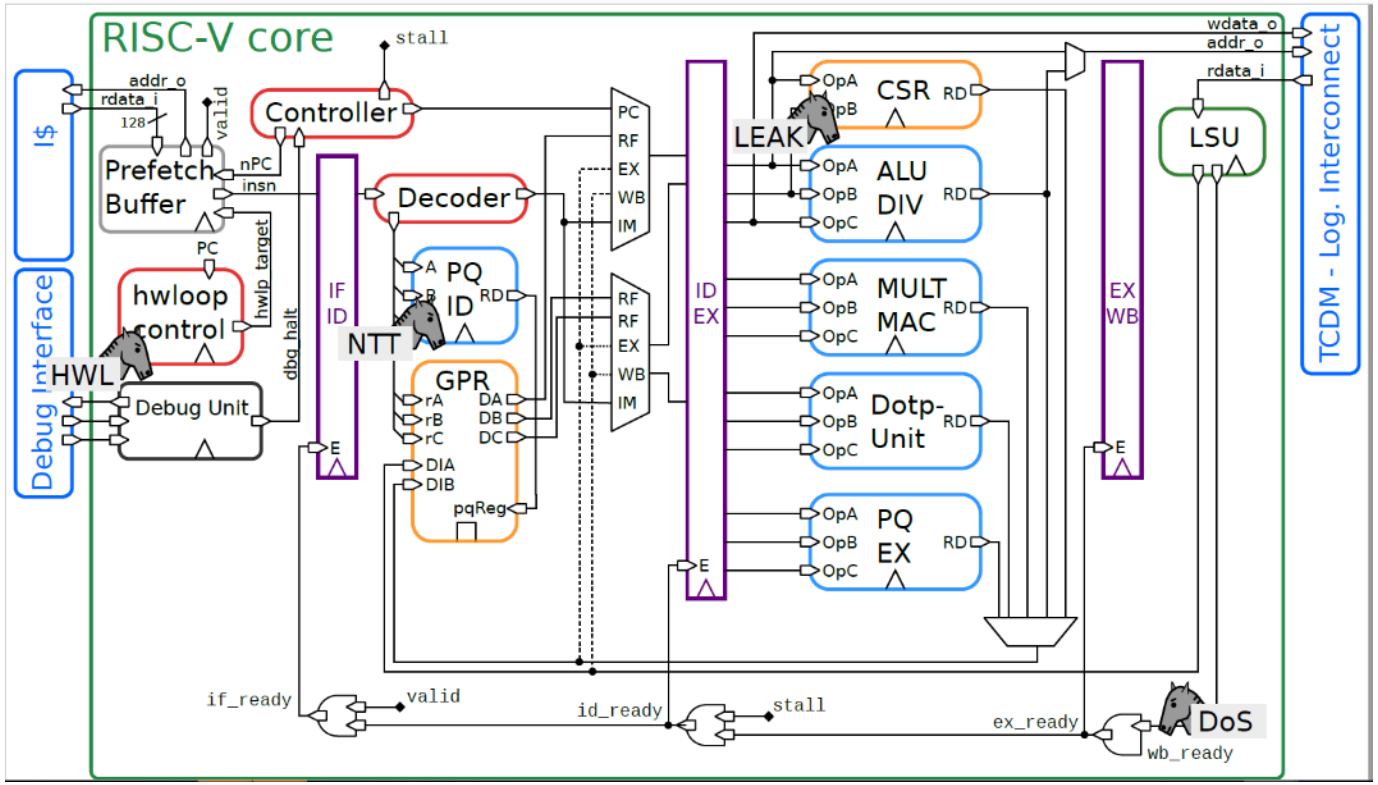
RAITH NANOFABRICATION

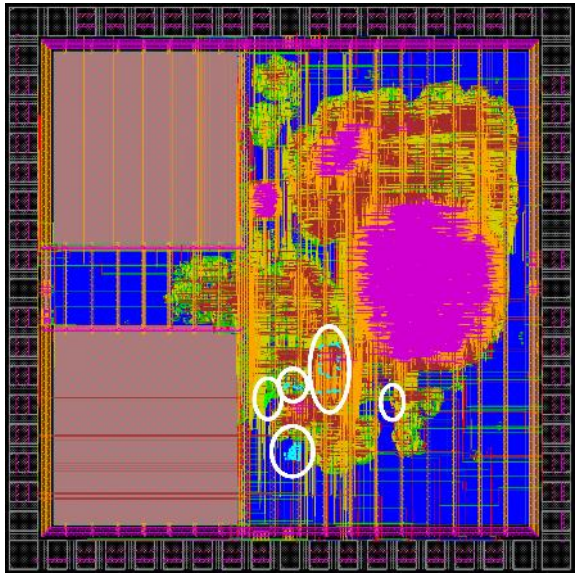
Chip Design with HW Trojans, Circuit Identification
- Design and manufacturing of RISC V with inserted Trojans
- Identification of modifications
- RE and Security assessment

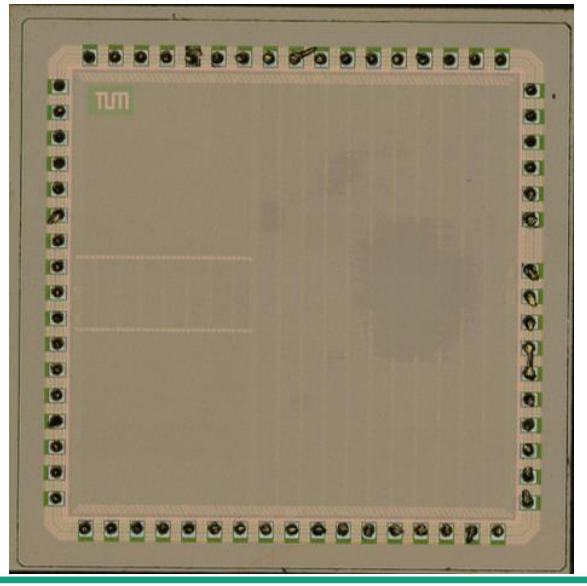
RESEC: Scientific Demonstrator for Integrated HW-Trojans

A.Hepp, G.Sigl ACM 2021

- 1st-Time Right: 4 Trojans with different levels of complexity
- Post-quantum RISC V
- Goal: Identification by Physical Analysis







Alexander Hepp and Georg Sigl. 2021. Tapeout of a RISC-V crypto chip with hardware trojans: a case-study on trojan design and pre-silicon detectability. In Proceedings of the 18th ACM International Conference on Computing Frontiers (CF '21). Association for Computing Machinery, New York, NY, USA, 213–220. DOI:https://doi.org/10.1145/3457388.3458869

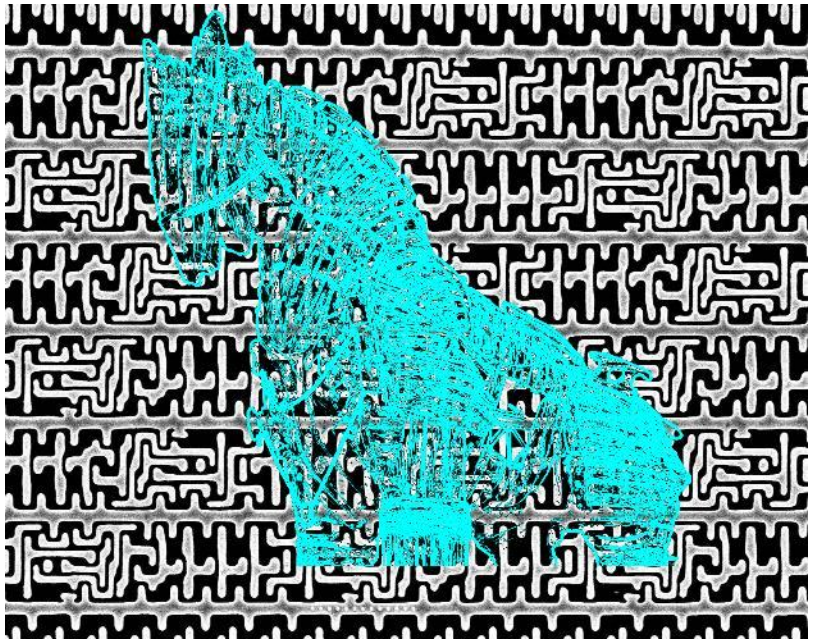
Fraunhofer Forschungsfabrik Mikroelektronik Deutschland

edacentrum

gefördert vom Bundesministerium für Bildung und Forschung

Fraunhofer EMFT

Our Common Charta – Trusted Electronics for a Secure World



Thank you very much for your kind attention

Dr. Horst Gieser horst.gieser@emft.fraunhofer.de

Gratefully acknowledging my Colleagues of Velektronik, TRAICT, RESEC,TREB & for inviting me