Challenges and novel approaches for the development of hardware-related trustworthy electronics

A. Middendorf, M. Böttcher, E. Jung, H. Pötter, I. Ndip, M. Töpper, M. Schneider-Ramelow, W. Steller
Fraunhofer Institute for Reliability and Microintegration (Fraunhofer IZM)
Gustav-Meyer-Allee 25
D-13355 Berlin, Germany
Ph: +49(0)30-46403-135
Email: Andreas.middendorf@izm.fraunhofer.de

Abstract

Emerging and future electronic components and systems must not only meet cost, performance, reliability, miniaturization and environmental requirements, they must also be trustworthy. In the near future, we have to trust even more electronic components and systems in everyday life, such as those used in self-driving cars or service robots.

In this contribution, we present the challenges and novel approaches for the development of hardware-related trustworthy electronics. Our proposed solutions cover all aspects of the value chain starting with the confidentiality of secure production chains, the security against manipulation as well as technological sovereignty. These novel approaches are extensively investigated with partners from academia and industry in R&D projects within the framework of the German Flagship initiative "Trustworthy Electronics". The German Federal Ministry of Education and Research (BMBF) as a contribution to research and innovation for technological sovereignty fund this initiative.

In this paper, we will report on the latest research results of the implementation of our approaches at four key levels, namely wafer, board, system and platform levels.

In the area of wafer level packaging, the focus is on developing solutions for the implementation of trustworthy heterogeneous systems using high-frequency chips in combination with complex signal processing.

At board-level, the goal is to develop a universal electro-optical interposer, particularly taking into account security features (e.g. key generation and encryption / decryption, design of photonic expandable RISC-V peripheral components).

At system-level, we focus on the development of processes and multi-sensor systems that protect important microelectronic circuits from criminal attacks. The entire system has to be protected by hierarchically graded monitoring, by embedded sensors and its corresponding microcontrollers. The development of the packaging and interconnection technology is supplemented by non-destructive testing methods that monitor the integrity of the protective mechanisms. The approach pursued here does not require any modification of the structure of the circuits to be protected and can be combined with all safety-critical application circuits. With this cost-effective solution, small series production is also economically feasible.

Finally, at the platform-level, overreaching issues are investigated within the three pillars, namely design, production and analysis of the microelectronic value chain. The platform concentrates predominantly on contributions to the necessary standardization. This enables companies effectively to support the supply of trustworthy electronics, especially with regard to small series.

Keywords

Chiplet, embedded hardware, hardware-safety, hardware-security, reliability, trustworthy electronics,

I. Introduction

Emerging and future electronic components and systems must not only meet cost, performance, reliability, miniaturization and environmental requirements, they must also be trustworthy. In the near future, we have to trust even more electronic components and systems in everyday life, such as those used in self-driving cars, IoT devices or service robots. With recent events, it is obvious that current reliance on state of the art measures to mitigate security risk are

inadequate. By manipulating not only data streams in transit, but attacking data generating and receiving ends, software based concepts seem to fail against sophisticated attack scenarios. Whether founded or unsubstantiated, the claims reported in [1, 2] depict a scenario, which electronic industry as of today is not well adapted to address. Hardware integrated trustworthy concepts from design, manufacturing and product implementation therefore gain interest in the electronics community.

II. Hardware relevance

While today´s focus w.r.t. "cybersecurity" and "trusted computing" is mostly towards software (i.e. on zero trust concepts, see eg. [3]), the foundation for security features of an electronic system is deeply rooted in hardware. This addresses the initial design process, the supply chain for all components and the manipulation-free assembly and interconnection technology. Only proper consideration of these aspects enables the implementation of further (then software-based) security features. Additionally, building on this, organizational procedures can then ensure a higher level of security to prevent attacks for fraud, ransomware and (state) terrorism (Figure 1).

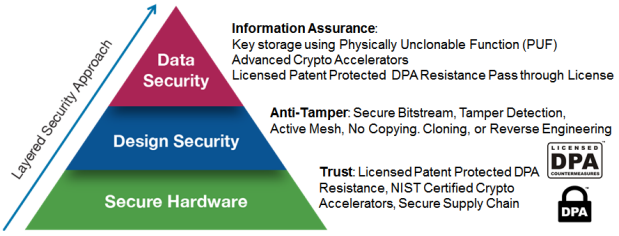

Figure 1: Secure Hardware is the fundament of trustworthy electronics [4], the DPA logo is trademarked by Cryptography Research, Inc.

Trustworthy electronics sub-summarize a wide range of different aspects. Often there is a strong interdependency with software. Furtheron, the hardware related activities have to be embedded in logistic and organizational operations, opening a complex perspective (Figure 2).

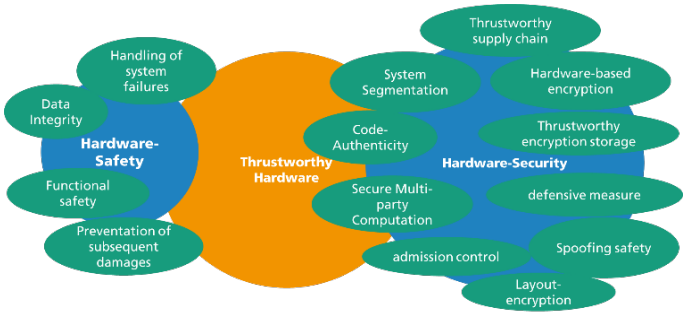

Figure 2: Trustworthy Hardware as multi-level approach

III. Hardware centric means for trusted computing

Starting from the initial concept of a system, strategies for a system level Co-Design can serve as a starting block for trusted platforms (see [5], Figure 3). Here, not only chip functionalities are defined, but also all aspects unto the final system (typically on PCB) are intertwined. In a vertical flow, additional security features can be added referring respectively to the prior or posterior positions in the value chain.

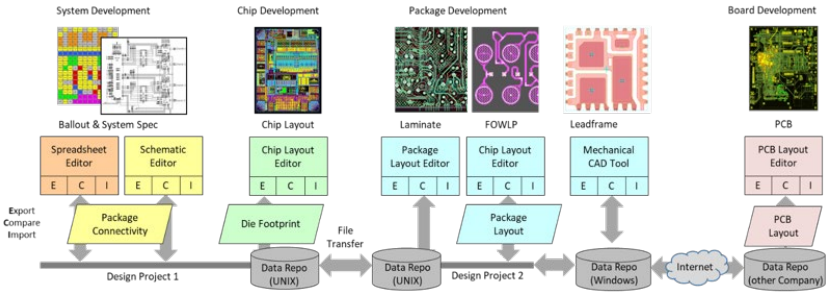

Figure 3: System Co-Design strategy [6]

A critical aspect of modern chip design is the reliance on -until now not intrinsically trustworthy - libraries. This is further complicated by what is dubbed "Fractured Manufacturing" [7], with more and more countries and manufacturers seeking alternative and independent sources for security and safety related chips.

The "new kid on the block", Chiplet Technology [8], adds another layer of complexity, as for the sake of cost, flexibility and performance, different building blocks are sourced - which may ultimately come from different vendors - and merged in a heterogenous system-in-package (SiP). In the case of a heterogenous SoC based chiplet approach, predefined IP blocks are -consequently. integrated in a trusted fab environment.

When combining the chip components in a (sub-) system, today, the vast majority of vendors rely on OSAT or E2MS service providers, trusting that their hardware designs are realized in an unaltered way. At this level, hardware is also merged with software, reaching the next level of trusted computing-to-be.

Clearly, there is an abundance of unchecked interfaces in today´s industry – and even if one part of the value chain is checked and monitored,- there is a large number of angles-of-attack, which are not readily addressable with today´s approaches.

As early as in chip design, handing over the design files to the chip manufacturer opens up the possibility of malicious design alterations, e.g. just adding a kill-switch or a memory access line – for a human review, such alterations will be inivisble and also automated routines are challenged to identify such modifications in larger IC designs. Design-

fingerprints have been suggested to overcome this challenges and wait to be implemented [9]. Additionally, built-in activity supervision may identify unwanted circuitry in the delivered silicon [10].

Similar fingerprinting approaches can be implemented at the OSAT or E2MS level; such approaches have since long time been proposed for quality assurance [11], but lend themselves easily for hardening the PCB manufacturing and assembly process against unwanted modifications.

System co-design concepts, at least spanning over three levels of the value chain, will further enable to place security features communicating from one level to the other to further reduce single-point of injection risks.

Additionally, the finished system should be resilient against post-manufacturing tampering, i.e. changing of code of the embedded software. While the product owner can already take strong measures against some means of attack (i.e. using strong cryptography and embedded crypto-hardware (e.g. 12, 13]) – as soon as the products enters the shipping process the loss of control at various ingress points cannot be denied. Here, data lines connecting to sensors can be tampered with, peripheral chips can be removed/replaced – a number of attack scenarios have been speculated on ([14, 15, 16]), from criminal entities to governmental, highly sophisticated attacks. Here, specific features of a system (i.e. physically unclonable features -PUF-) can again serve as a measure to counteract such malicious intent, allowing the end-user (i.e. providers of critical infrastructure, safety and security organs, …) to doublecheck the integrity of a product prior putting into use. The large number of attach scenarios and similar ways to address these have led to a flurry of concepts and implementations. The paper highlights some of the approaches, as a part of the raising awareness of European and German industry complementing the efforts on the global scale.

IV. Project initiative *VE*lectronic "Trustworthy Electronics and Trusted Value Chains"

The aim of *VElectronic* is to create a platform for the topic of trustworthy electronics. Overarching issues are dealt with in the three pillars of design, production and analysis, research results from consortium partners, research projects of the current funding guidelines and the situation of commercial enterprises are analyzed and brought into a holistic concept for improving technical sovereignty.

The platform aimed at with this project will focus on the technological overview, contributions to the necessary standardization, the network of research and industry, as well as the ultimate expertise in order to counter the increasing need for greater trustworthiness in electronics with specific solutions with solution concepts.

The platform aims to integrate the contributions of all relevant R&D projects and the companies and research institutions important in this area across the entire value chain into a comprehensive concept for trustworthy electronics. In this way, a technological range of services can ultimately be identified and selected and a reliable assessment of the trustworthiness as well as comprehensive and flexible use become possible.

In the *VElectronic* project, the pillars of "production and analytics" are core to the packaging expertise of Fraunhofer IZM and deals with issues relating to the design of industrial electronics, the packaging of electronics at wafer, package and board level, and the reliability of electronic assemblies.

Here, a methodical design at module and board level focusing on systems relying on external sensing is developed. Based on the research findings, a number of systems have been successfully implemented for research and industrial applications, i.e. smart sensor systems, wireless and energy self-sufficient systems and industrial electronics. With the methodology in place and having access to advanced packaging techniques (i.e. embedded chip technology, panel level integration, hybrid bonding), a three tier inclusion of the value chain (design, package, system) could be achieved. In the lab, measurement and testing technology complemented the implementation process flow with attack scenario validation, covering thereby a substantial part of the vulnerable value chain.

As fraudulent components can also have an unwanted reliability impact on critical systems, also the aspects of long term reliability of electronic assemblies is addressed. Here, the change in system performance behaviour can be assessed, i.e. by monitoring the condition of electronic components and assemblies and extracting relevant parameters for fraudulent component detection. This can be achieved eg. by evaluation of supervised stress-induced degradations as well as by artificially induced manipulations.

The methods used include parameter tests as well as imaging methods such as IR thermography. With these measurements, the system models are checked and calibrated, which can describe the material-typical interactions mechanically, electrically, thermally and electro-chemically.

As a result, the effects of degradations and manipulations can be better predicted and specifically influenced, leading to a "digital twin" of the systems under review.

V. Project Intiative Silhouette "Heterogeneous Photonic Electronic Platform Integration"

Most of todays´ security reviews focus on CMOS technology and PCB based system integration. However, modern communication and also military electronics often rely on optical transmission -and respective components- as well.

Thus, *Silhouette* addresses the development, fabrication and validation of methods and technologies to realize an electro/optical system in package (SiP) for trustable data processing.

The system core which needs to be hardened against malicious attacs is a photonic processing unit. In line with a higher degree of (miniature) integration, *Silhouette* endorses a modular concept of a new electro/optical interposer as system carrier, which is hosting all needed components as laser, laser driver, RISC-V processor and the photonic processing unit itself. The concept covers high assembly accuracy and high system performance especially for optical components integration scalable for a future mass production.

The evaluation of this modular electro/optical concept is planned for realization in two different photonic applications. On one hand the function of TNRG (photonic entropy source) and on other hand a cryptographic multi-mode interferometers (MMI).

While this intrinsically seems to seal out a large number of malicious perpetrators, this also is a high value target for e.g. governmental intrusion and is thus thoroughly reviewed with respect to up-front measures to minimize attack scenarios.

Initial R&D activities on E/O-Interposer will target material evaluation regarding influence of processing parameter and processing flow on optical signal and coupling efficiency. A second step will be the simulation and realization of adapted electro/optical test pattern for a first validation of processing, including the assembly concept. The outcome of pre runs will be implemented in a wafer-processing run with final integration of the functional photonic processing unit, readying the manufacturing with "fingerprinting" the 2D representation – the high assembly accuracy will easily flush out post-manufacturing tampering or identify modified components. Additionally, non-functional test patterns will augment the circuit´s security, as physically unclonable features (PUF) can thus be extracted already on the visual (i.e. low threshold) level.

Conceptually, passive-functional patterns, offering delays for phase shift monitoring, can also be implemented, but are prone to false-positives due today´s material property limitations (i.e. TCE mismatches). As such technologies should not be limited to the capabilities of a high-tech laboratory, the processes will be implemented in state-of-the art industry compatible formats (i.e. 300mm wafer substrate line @IZM-ASSID), guaranteeing a fast uptake by industrial partners.

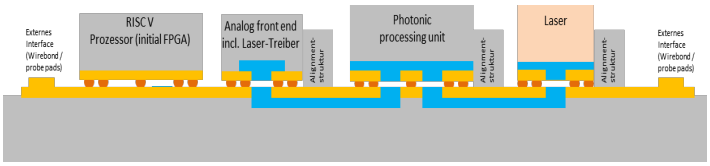

Figure 4: Silhouette *concept - schematic of electro/optical-interposer with photonic processing unit (orange - Cu-RDL & BEOL; blue - photonic wave guides; orange - FC-interconnects; gray - substrate)*

VI. Project Initiative REWAL "Realization of trustable and complex system using fan-out wafer level packaging"

With transistor scaling reaching its limits [e.g. 17], interposer-based integration of dies (chiplets) is gaining traction. As "chiplets" have since several years been suggested to overcome these barriers faced by Moore´s Law paradigm, a number of conceptual approaches for their implementation have arisen. As of such, an interposer-based integration enables finer and tighter interconnect pitch than traditional system-on-packages and offers some key benefits, like reducing design-to-market time by bypassing the time-consuming process of verification and fabrication and reducing the design cost by reusing chiplets.

DARPA, with its CHiP initiative [18] paved the way for a multitude of approaches ([19], [20], [21]), resulting already in first products.

While black-boxing of the slow design stages cuts down the design time, it raises significant security concerns. Thus, most of theses are build in a highly vertical industry setting, foregoing some of the flexibility promises that chiplets hold.

With industry moving towards large-scale System-on-Chip (SoC) and SiP (System-in-Package) designs, where heterogeneous components such as processor cores, DSPs, memory controllers, and accelerator units are bundled via 2.5D integration and obtained from various sources, the integration of many IP modules and hardware components while ensuring security and integrity over this complex value chain is a grand challenge.

So far, no specific focus had been placed on trusted architecture and fabrication. But -obviously- this is changing with further adoption of the technology ([22], 23], [24], [25])

Further to this, malicious software running embedded within a chiplet can pose significant risks as well.

The *REWAL* initiative now studies the security implications of the emerging interposer-based integration methodology. Approaches known from traditional systems-on-chip (SoC) designs are not readily suitable for interposer-based integration. Functionally diverse chiplets with built in "sensing" capabilities to detect and thwart hardware Trojans are combined in *REWAL*, their inherent logic redundancy used to ensure anti-piracy measures. An active interposer as

secure-by-construction, generic root of trust platform for such modern systems results from this concept.

Clearly, impedance matching, controlling wiring length for critical signals, etc, are challenges to be investigated beyond traditional design, simulation and testing concepts.

The new architectural framework where untrusted processing elements, running untrusted code, are integrated on top of such an interposer-based root of trust, allowing us to detect and prevent any form of malicious messages exchanged between the heterogeneous components. Also, the concept has limited design overhead restricted to the design of the active interposer, allowing the heterogeneous components within chiplets to remain untouched. It is expected that such a scheme correctly handles attempted security violations with little impact on system performance, summing up to around 4% performance loss against a non-secured approach.

The expected benefit of the approach is assessed on a demonstrator platform with a MIPS processor, a DCT core, and an AES core using various IPs from the Xilinx CORE GENERATOR IP catalog, on an interposer-based Xilinx FPGA.

Implementation will be done using state of the art advanced packaging technology based on fan-out processes (RDL-first, [26]), offering a platform solution for a multitude of architectures, in the digital, mixed-signal and high-frequency domain. (see. Fig 4). For compatibility with existing industrial manufacturing capabilities, this RF-/HD-FOWLP concept will be implemented in a 300mm BEOL wafer line.

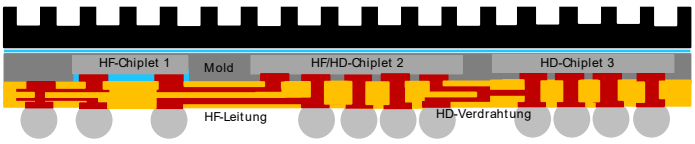

Figure 5:RDL-1st based FOWLP used for REWAL initiative

VII: Project Initiative “VE-SAFE”

Conceptually more complex than the *REWAL* approach described before, which uses an intelligent, active interposer to supervise the “trustworthiness” of the built-on hardware, *VE-Safe* pushes this further on by including specific hardware based anti-tampering measures in an embedded chip package.

Here, the initially mentioned aspect of chip-package-module co-design becomes prominent, as each integration layer may not only contain individual anti-tampering techniques like meshed layer and fusing structures, but adds active sensors to identify angles of attach e.g. by RF injection, optical injection, mechanical (FIB) penetration directly on the hardware anticipating post-manufacturing attac scenarios.

2.5D meshing, co-designed and intertwined on chip/package and package/module level allows also to integrate physically unclonable features (PUF), individual to the system shipped.

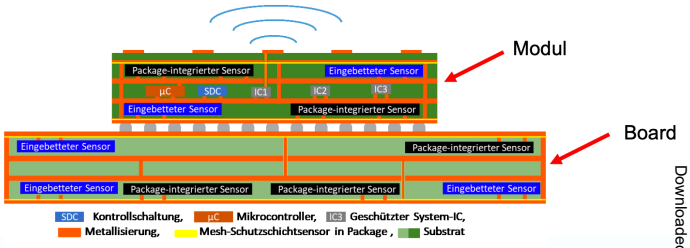

Figure 6: VE-Safe initiative: Concept on package/module

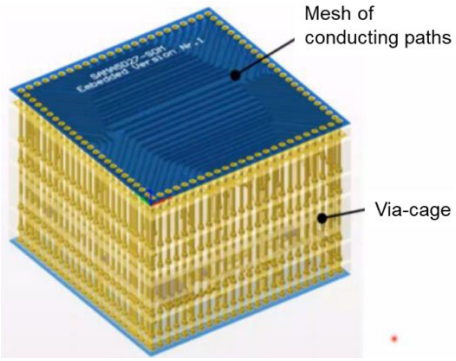

Figure 7: VE-Safe initiative: Concept on chip/package

VE-Safe is currently in an early conceptual state, as it is assessed not only w.r.t. resilience to attack angles, but also w.r.t. manufacturing issues and cost challenges due to the added security features included.

VIII. Conclusion

Trustworthy electronics beyond software, targeting the hardware building blocks and thus thwarting sophisticated angles of attack are becoming more attractive, as critical infastructure and safety/security electronics has since been more and more in the view of malicious attackers. Current approaches, including TPM modules and cryptographically protected memory areas, address only the chip-level security and omit to include attack scenarios on package, module and subsystem level as well as manufacturing itself. Counteracting attacks become in the view of this more difficult, especially as modular architectures (i.e. chiplets) become favourable to address the issue of a slowing Moore´s Law.

The paper offers insight in four intiatives and their conceptual approach to address security issues through out the manufacturing value chain, from chip-design, procurement, integration and module shipment, by including cross-level security measures ranging from passive (eg. Fingerprinting), passive-active (e.g. PUF validation) to fully

active (active monitoring of safety critical details with dedicated sensing circuitry and subsequently actively shutting down module functionality) concepts.

IX. Acknowledgment

The funding enabling the research on hardware based trustworthy computing is provided by German Ministry of Education and Research (BMBF) under various contracts and is gratefully acknowledged. The authors would like to acknowledge the support of the project teams from *VElectronic, Silhouette, Rewal, VE-Safe*, coming from Fraunhofer Institutes and industrial partners

X. References

1 Robertson, Riley, “The Big Hack”, Bloomberg Business Week, Oct. 2018

2 Robertson, Riley, “The Long Hack”, Bloomberg Business Week, Feb. 2021

3 https://www.nccoe.nist.gov/

4 Microsemi webressource: https://www.microsemi.com/product-directory/fpga-soc/1738-security

5 IEEE HIR Roadmap 2019, https://eps.ieee.org/images/files/HIR_2019/HIR1_ch21_sip-module.pdf

6 Brandtner et al., "Chip/Package/Board Co-Design Methodology Applied to Full-Custom Heterogeneous Integration," 70th ECTC 2020, pp. 1718-1727]

7 https://www.eenewseurope.com/news/fragmented-chip-manufacturing-brings-big-risks-says-tsmc-founder

8 https://semiengineering.com/piecing-together-chiplets/

9 Implementation-Based Design Fingerprinting for Robust IC Fraud Detection, DOI:10.1007/s41635-019-00081-x

10 System-on-Chip Platform Security Assurance: Architecture and Validation, DOI: 10.1109/JPROC.2017.2714641

11 An AOI algorithm for PCB based on feature extraction, DOI 10.1109/WCICA.2008.4592931

12 Guajardo et al., “FPGA Intrinsic PUFs and Their Use for IP Protection”. CHES 2007, Lecture Notes in Computer Science, vol. 4727. Springer, Berlin, doi.org/10.1007/978-3-540-74735-2_5

13 Huang et al., “Intellectual property protection for FPGA designs using the public key cryptography”, Advances in Mech. Engr. 4/2019, doi:10.1177/1687814019836838

14https://www.sp.se/sv/index/services/functionalsafety/Documents/Hardware%20safety%20integrity%20guideline%20Process%20version%201.1.pdf

15 Wolf, Gendrullis, “Design, Implementation, and Evaluation of a Vehicular Hardware Security Module”, Report WP11 (public) of EU-FP7 Project EVITA, found at https://evita-project.org/Publications/WG11.pdf

16 Elena Dubrova, Seminar on Hardware Security, https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security__2017_05_08.pdf

17 https://arstechnica.com/gadgets/2021/07/intels-foundry-roadmap-lays-out-the-post-nanometer-angstrom-era/

18 https://www.darpa.mil/program/common-heterogeneous-integration-and-ip-reuse-strategies

19 K. Drucker et al., "The Open Domain-Specific Architecture," 2020 IEEE Symposium on High-Performance Interconnects (HOTI), 2020, pp. 25-32, doi: 10.1109/HOTI51249.2020.00019

20 https://www.intel.de/content/www/de/de/architecture-and-technology/programmable/heterogeneous-integration/overview.html

21 C. Gonzalez et al., "Enabling New System Architectures with 2.5D, 3D, and Chiplets," 2021 IEEE International Solid- State Circuits Conference (ISSCC), 2021, pp. 529-532, doi: 10.1109/ISSCC42613.2021.9365834.,

22 The Importance of Chiplet Security, RAMBUS Whitepaper, obtained: https://go.rambus.com/the-importance-of-chiplet-security

23 M. Nabeel et al., "2.5D Root of Trust: Secure System-Level Integration of Untrusted Chiplets," in IEEE Transactions on Computers, vol. 69, no. 11, pp. 1611-1625, 1 Nov. 2020, doi: 10.1109/TC.2020.3020777.

24 Mandal et al., “Interposer-Based Root of Trust”, arXiv:2105.02917

25 Shayan et al., “Security Assessment of Interposer-based Chiplet Integration”, arXiv:2010.13155

26 Böttcher et al., “Development of High Density RDL Technologies for Panel Level Processing”, Device Packaging, 2019 (DPC): 000284–000313, https://doi.org/10.4071/2380-4491-2019-DPC-Presentation_TP1_041