Physical and Functional Reverse Engineering Challenges for Advanced Semiconductor Solutions

Bernhard Lippmann*, Ann-Christin Bette*, Matthias Ludwig*†, Johannes Mutter*, Johanna Baehr†, Alexander Hepp†, Horst Gieser‡, Nicola Kovač‡, Tobias Zweifel‡, Martin Rasche§, Oliver Kellermann§
*Infineon Technologies AG, Munich, Germany
{bernhard.lippmann, ann-christin.bette, matthias.ludwig, johannes.mutter}@infineon.com
†Technical University of Munich, Department of Electrical and Computer Engineering, Munich, Germany
{johanna.baehr, alex.hepp}@tum.de
‡Fraunhofer EMFT, Munich, Germany
{horst.gieser, nicola.kovac, tobias.zweifel}@emft.fraunhofer.de
§Raith GmbH, Dortmund, Germany
{martin.rasche, oliver.kellermann}@raith.de

***Abstract*—Motivated by the threats of malicious modification and piracy arising from worldwide distributed supply chains, the goal of RESEC is the creation, verification, and optimization of a complete reverse engineering process for integrated circuits manufactured in technology nodes of 40 nm and below. Building upon the presentation of individual reverse engineering process stages, this paper connects analysis efforts and yields with their impact on hardware security, demonstrated on a design with implemented experimental hardware Trojans. We outline the interim stage of our research activities and present our future targets linking chip design and physical verification processes.**

***Index Terms*—Hardware Reverse Engineering, Layout Extraction, SEM Imaging, Image Processing, RISC-V, Hardware Trojans**

I. Introduction

As electronic products are part of daily life, with applications ranging from consumer and entertainment, industrial systems up to autonomous driving and critical infrastructure, many reasons exist to verify the construction, functionality, and security of these products. The search for intellectual property (IP) violations, competitor analysis and benchmarking tasks are typical industrial use cases. In addition, due to globally distributed supply chains for semiconductor design and manufacturing, the physical verification is a major contributor for trust and security through the active search for malicious modification or re-fabrication.

Fig. 1 shows the major stages of a reverse engineering (RE) process with a separation of the physical reverse engineering steps and the electrical function recovery process. Starting from the preparation of samples displaying each physical layer on the chip and the high resolution imaging of these layers using scanning electron microscopy, a first software tool needs to seamlessly stitch the individual tiles together. Only a geometrically undistorted 2D layout of each layer allows the correct 3D alignment of the complete layer set as a first interim result (R1). Using computer vision, the layout images are converted into a vector format (R2). Whereas wires and interconnect structures can be directly converted, semiconductor process, design knowledge, and dedicated methods are needed to extract the digital or analogue devices from the raw layout images. The reconstructed device library and the extracted connectivity between the device instances enables the generation of a flat netlist (R3), using the routing module. Finally, netlist interpretation algorithms are applied to create a humanly comprehensible representation of the electrical design (R4) which is evaluated in the following use cases.

This work was partly funded by the German Ministry of Education and Research in the project RESEC under Grant No.: 16KIS1009.

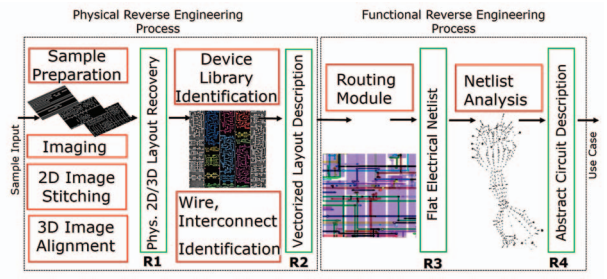


Fig. 1: RE process overview with major interim results R1-R4.

From an industrial viewpoint the total benefits of a reverse engineering activity should clearly exceed the effort of this analysis. This includes cost control, trustworthy project execution time frames, and excellent high valuable technical outcome of this process. Moreover, this process must be applicable to any kind of device and technology node in order not to limit the number of possible analysis projects. Even for a state actor with almost-unlimited resources, clear answers to these challenges must exist. Reviewing the complete process, a list of challenges is presented in table I.

These challenges define strategic requirements and a development roadmap for the future RE process steps. RESEC [1] aims to examine the reverse engineering process in its entirety for the first time, with a focus on sub-40 nm process nodes. By creating and then reverse engineering a chip especially

TABLE I: Challenges for IC Reverse Engineering.

Task	Challenges
1. **Physical** layout recovery	• **Delayering (P1)** maximal uniform layer removal over complete chip size • **Technology (P2)** enable delayering of advanced nodes with ultra-thin and fragile inter-oxide layers, support Al & Cu technology, FinFET • **Chip Scanning (P3)** homogeneous, fast and accurate high resolution imaging over the complete chip area for all layers with minimal placement error • **Image Processing (P4)** precise layout recovery including preparation errors, indication of the error rate
2. **Electrical** function recovery	• **Digital Circuits (E1)** recovery and sense making of large digital circuits based on std. cell designs • **Analogue Circuits (E2)** recovery of circuit functions based on analogue devices with unclear electrical behaviour • **Robustness (E3)** robust to remaining errors coming from the physical layout extraction process
3. Analysis and scoring of **Security** protection mechanisms	• **Chip Individual Features (S1)** hardware security may include chip individual features like physical unclonable functions (PUFs), dedicated protection layers and protection circuits configured with run time keys, logic locking, etc. • **Design for Physical Analysis Protection (S2)** camouflaged cell libraries, timing camouflage • **Error and Effort Estimation (S3)** reliable indications must be shown how strong these measures are under the current analysis options

designed to test the process, not only each single challenge can be addressed, but the effect of challenges in each step on subsequent steps can be investigated. With partners from both industry and academia, RESEC is able to analyse both the technical and the more theoretical aspects of RE.

The paper summarises different RE process stages, with the final goal of measuring the level of hardware security. It is organised as follows: Section II provides an overview of existing approaches for advanced semiconductor reverse engineering and describes the RESEC project set-up and organisation to create a process impact metric. Section III describes the achieved process improvements and their impact on the complete process. In section IV, we present new innovative ideas to address these strategic challenges.

II. State of the Art and RESEC Project Organisation

Complete RE process solutions are available at research institutes, commercial service providers, and chip manufacturers [2]–[6]. These publications cover all stages of the RE process, starting with automated mechanical-chemical deprocessing using plasma FIB delayering on sample sizes of $800\,\mu\mathrm{m} \times 800\,\mu\mathrm{m}$ as an innovative preparation option [7].

Aside from the classical approach of sequential delayering and imaging, computed tomography- and laminography-based reverse engineering analysis has been proposed [8]. A promising approach uses x-ray synchrotron laser interference patterns to retrieve laminographic 3D-images [9]. This removes the requirement for the time-consuming and error-prone delayering process. Nevertheless, this method is not production ready, as only few synchrotron x-ray sources can generate radiation with the required brilliance and coherence. As there is no perspective to overcome these limitations in the near future, delayering-based RE must further improve to keep up with the downscaling of chip production. Partial reverse engineering analysis has also been proposed as a possible method to overcome the challenge of delayering large samples [10].

Furthermore, for all stages of the RE process, machine learning based approaches have become more and more common, whether it be for low level image processing or to gain high-level understanding of the resulting netlist [11].

Extending the analysis scope to sub-$40\,\mathrm{nm}$ process nodes requires dedicated new solutions. The different areas to be addressed by each partner are shown in Fig. 2.

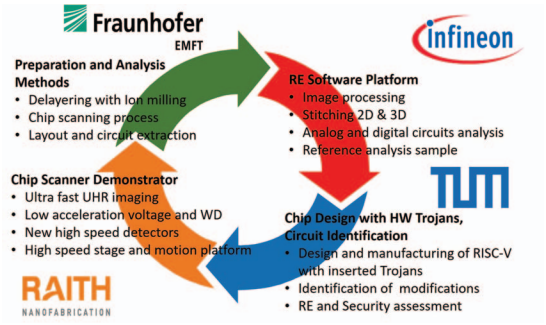


Fig. 2: RESEC partners and contribution.

The work package structure of the RESEC project is grouped in 3 columns: the RE process development (WP3, WP4), software development (WP5, WP6) and the scanning hardware development (WP7) as shown in Fig. 3. Furthermore, in WP1, specification and target settings are defined and in WP2, analysis devices are planned and implemented. Finally, in WP8, the actual analysis projects are executed in order verify the RE process performance.

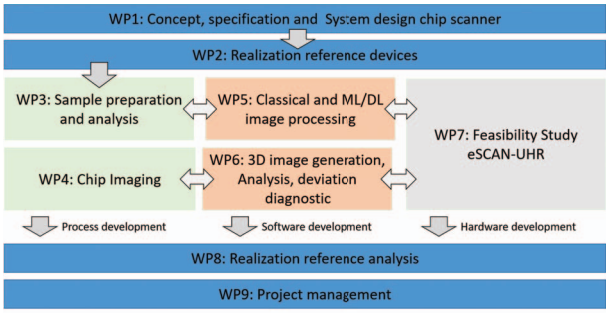


Fig. 3: RESEC project working package structure.

In the earlier SYPASS project, the layout extraction process was evaluated for technology nodes down to $40\,\mathrm{nm}$. The challenges for nodes $\leq 40\,\mathrm{nm}$ using thinner inter oxide layers, analogue devices, and converting the extracted layouts into electrical net list form the scope of the RESEC project. In the connected project, VE-FIDES [12], we will transfer knowledge

to reverse engineer chip-individual features. The implemented physical and electrical verification methods will also form part of the VELEKTRONIK – TRUSTWORTHY ELECTRONICS platform [13].

III. Reverse Engineering Process Steps: Improvements and Impact

A. Sample Preparation

Homogeneous sample preparation techniques of 40 nm product technologies — and even below 40 nm — require intensive reverse engineering knowledge and practical experience in addition to the demand for high-end processing and preparation devices and systems. The delayering processes involves mainly dry chemical etching and mechanical polishing techniques. System and process parameters have been continuously optimised over several years to achieve a homogeneous preparation result. Fig. 4 shows a homogeneous delayering result achieved on chip samples using 40 nm production technology. Fig. 4 (a) shows the sample state with the thick Al top metal still in place, while Fig. 4 (b) shows the same sample after delayering. Here, a fine-pitch Cu layer is visible. The whole layer is prepared homogeneously over the whole sample size and can therefore be used for subsequent layout extraction techniques. When inspecting the colour-uniformity of the whole chip module with optical microscopy techniques, the different colours of the layer are due to different circuit modules and the different layers of the chip.

B. High Speed Chip Scanning

Inspection of small technology nodes requires automatic image acquisition by a dedicated scanning electron microscope (SEM) [14] with a highly accurate laser interferometer stage. Due to the needed resolution, defined by the number of pixels used for imaging the smallest geometrical width, a large amount of undistorted images is required, each with thousands of pixels. Within the SYPASS project, a first demonstrator of a new generation of high speed chip scanning tools was developed, called eSCAN. In its first development stage, eSCAN has addressed the 28 nm to 40 nm node. Major reduction of the scan time is achieved by introduction of a new electron column with a fast deflection system and a 50 MHz scan generator enabling real time distortion, focus and astigmatism corrections. Combined with newly developed fast detectors, chip scanning speed is significantly increased by a factor of 10 – 20.

The excellent image resolution at these low pixel times is displayed in Fig. 5. Below the 40 nm node, scanning metal layer stacks with ultra-thin inter oxide thicknesses requires low acceleration voltages and small working distances, which leads to major adaptions of the e-beam column and detector concept within RESEC. A first column of this new kind is build up and under evaluation.

C. Image Stitching Process

Gradually moving to even smaller technology nodes, showed a significant decrease of stitching accuracy. The conventional Normalised Cross Correlation (NCC) based calculation for optimal 2D local registration proved not to be sufficient any more. As a compensation of larger stage prealignment error in relation to the dimension of the layout patterns, a combination of Feature Extraction (FE), Phase Cross Correlation (PCC), and NCC algorithms has been implemented in the stitching process as shown in Fig. 6. This approach enables successful stitching on samples processed in 22 nm.

Local registration and refinement of outliers is followed by global registration in the stitching workflow. In order to minimise the total error and optimally distribute remaining errors over the image mosaic, the software applies one of the four implemented regression algorithms: Weighted Least Mean Square (W-LMS), Maximum Likelihood Estimation (MLE), Minimum Spanning Tree (MST) or Global Cost Minimisation (GCM). Moreover, this approach is transferable to material science specimens and biological samples, extending the possible applications for the stitching tool [15].

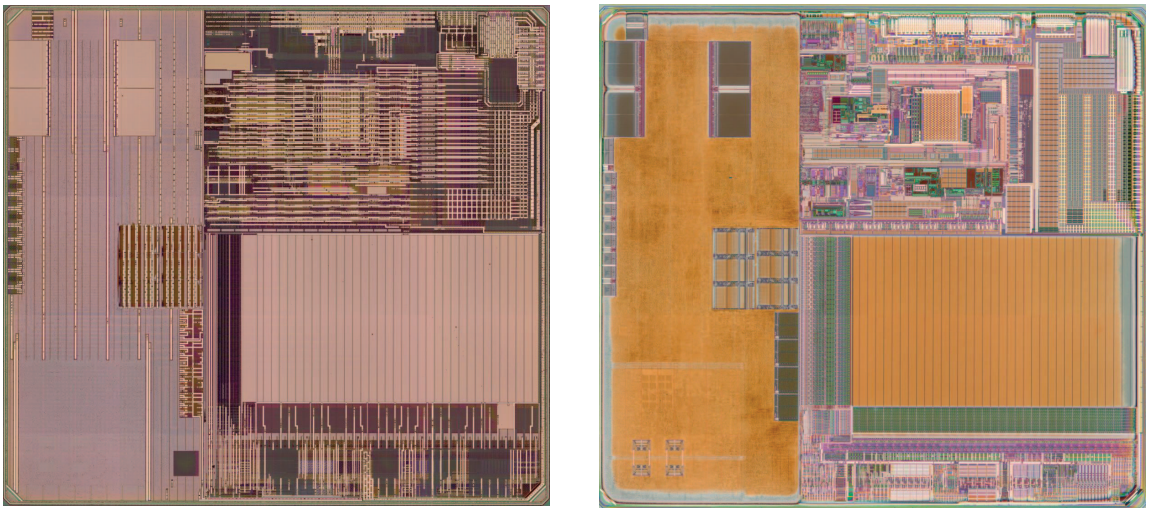
D. Advanced Image Processing

Several publications propose fully automated layout extractions — also deep-learning-based — on the complete chip level [4]–[6]. However, these refer exclusively to technologies larger than 90 nm and do not contain any descriptions of occurring defects. The challenges posed by image defects have only recently been discussed in the research community [11]. The correctness of the extracted layout is essential for the generation of the netlist and the subsequent functional RE. However, due to the ongoing technology shrinking, this prerequisite is severely endangered. Errors in sample preparation are caused by unintentional layer transitions or particles that incorrectly connect individual structures. SEM imaging can be a source of error if the settings are not optimally matched to the properties of the technology to be imaged.

We are convinced that this problem must be addressed early in the RE process flow and not only after or during the layout extraction step. Therefore, we developed the first, standalone defect inspection framework for delayered integrated circuits [16]. The classification of the visible defects in the acquired SEM images triggers two feedback processes: First, conclusions can be drawn about the state of chip preparation. Secondly, the localisation of the defects enables targeted manual correction in the extracted layout. In the long term, defect-specific image processing algorithms could also be created to automatically correct the defect. In a next step, we will extend the feedback to include the scan parameter settings. The aim is to determine the optimal SEM settings based on the given technology and type of preparation.

E. RE Process Accuracy and Layout Integrity Verification

Under assumption of a *malicious foundry* attack model, verification of the layout integrity is a task that can ideally approached via RE. The correctness of recovered designs can be verified for samples where a golden layout is available. This framework for the ***Ver**ification of **T**roj**a**n-free physical **L**ayouts (ViTaL)* is presented in [17]. Besides a layout integrity check,



(a) Thick Aluminium layer

(b) Fine-pitch Copper layer

Fig. 4: Full chip delayering result at 40 nm technology node.

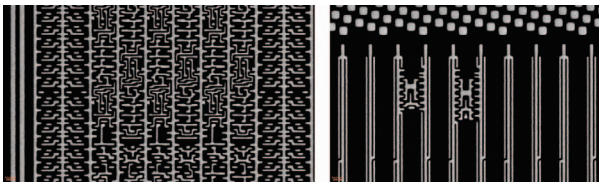


Fig. 5: High speed chip scanning, technology node 40 nm, scan speed: 30 ns/px.

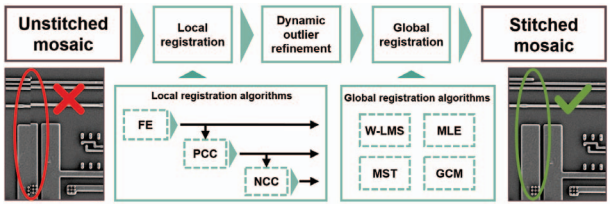


Fig. 6: Improved stitching process for small technology nodes.

the framework also contributes an enabler for RE process performance evaluation. The measurement and classification of different error modes has been evaluated and all physical design and design-for-manufacturabiltity measures (dummy fill patterns, layout post-processing, optical proximity correction) were considered. Furthermore, the total comparison effort for large designs is shown in [18]. The classification of modifications based on their layout foot print [5] leads to a better understanding of the quality of the extracted data and sets the requirements of a successful Trojan identification by utilizing a fully integrated RE process.

F. RISC-V Design with Hardware Trojans

Test and verification of the proposed approach requires a device under test for which specifications at any abstraction level can be shared openly between all partners. This is especially important for the assessment of the complete RE process, because this requires comprehensive and extensive data for evaluation, instead of the limited data a single-step-assessment would require. Hence, TUM designed, implemented and tape-outed a test device, featuring a RISC-V Core with Post-Quantum cryptographic functionality, into which four hardware Trojans were inserted [19]. Each Trojan is placed at a different area of the core, and the functionality ranges from simple (DoS), to complex (side-channel information leakage) Trojans, see Fig. 7. The ASIC allows for a typical red team, blue team scenario, where one team seeks to reverse engineer the chip with no prior knowledge, with the goal to identify the hardware Trojans, and the other team (TUM) is able to verify each step.

G. Vulnerability Assessment of RE-based Attacks

A central aim of RESEC is the security analysis of reverse engineered test samples. Existing certification schemes, e.g. the common criteria evaluation, do not allow a granular assessment of the role of reverse engineering in various attack

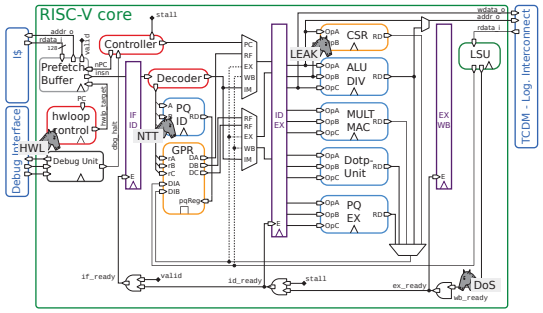


Fig. 7: RISC-V design with inserted hardware Trojans [19].

scenarios. Often, attacks on hardware (logical, observing, semi-invasive, invasive) benefit from results obtained through hardware RE. These range from simple optical device inspection to full net list and functional recovery. However, there is a significant difference in the applied methods complexity and efforts and no framework exists to provide a consistent and coherent classification. To extend the RE classification granularity, we proposed the novel **C**ommon **RE** **S**coring **S**ystem (*CRESS*) [20]. The framework is outlined in Fig. 8.

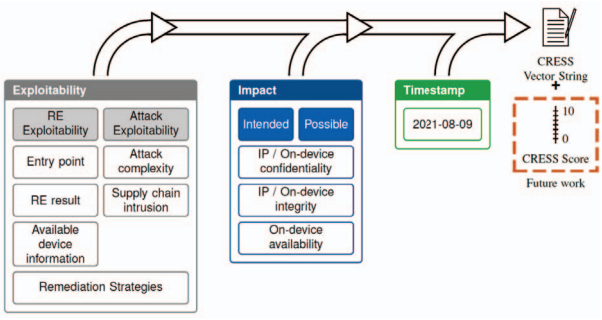


Fig. 8: Vulnerability Assessment of Attack Scenarios using Hardware Reverse Engineering [20].

The introduced *CRESS* vector string is calculated via three metrics: the impact, the exploitability, and a timestamp, as shown in Fig. 8. The first exploitability category **RE** consists of a qualitative assessment of the attributes for entry point, RE result, and available device information. The second exploitability category **Attack** includes the assessment of the attack complexity, where a consistent rating of efforts, costs and limitations is implemented. Remediation Strategies will allow a discussion of protection mechanisms against the attack vectors from a RE point-of-view. With this new way of classifying RE based attacks, a complete and fair security evaluation is possible.

IV. Planned Innovation

A. Readiness for the 10 nm Node

Within the RESEC project new approaches regarding sample preparation in the nanometre scale are researched developed and implemented, in order to become ready for the challenges of the 10 nm node with more than 10 metal layers and fragile low-k dielectrics. While traditional polishing and reactive ion etching is well-established to remove the top metal layers, reactive ion beam milling with a quadrupole mass spectrometer for in-situ process control will be introduced for the lower layers, separated by fragile low-k dielectrics. Starting the deprocessing from the backside should unveil the minimum size structures first, without retaining significant signatures of previously removed larger metal lines. A RAITH VELION dual beam FIB/SEM with a precision laser stage and Bruker EDX will be employed for both local delayering from front side and backside as well as technology analysis. Starting at the 40 nm node, exemplarily smaller areas (50 µm to 200 µm) of 7 nm CMOS samples have already been delayered, scanned and converted successfully in order to explore the challenges.

B. Large Area Scanning Solutions

A new high speed electron column concept including electronics and detectors is developed, combing a 50 MHz scan generator, a high speed deflection system with real time corrections and retarding optics for fast distortion free imaging of ultra-thin layers at low beam energies and various working distances. For further improvements of total chip scanning time and 2D / 3D stitching, a new laser interferometer stage and motion control platform is under development, featuring a new generation of non-magnetic high speed motors and a novel motor controller with high processing power and direct interface to the scan generator.

C. Reverse Engineering Process Simulation

The cost and complexity of RE severely limits the availability of benchmark designs to develop and test new protection methods. Therefore, we plan to introduce a novel tool chain in our project using real chip designs and a simulated physical lab process as shown in Fig. 9. The tool chain re-uses modules from the chip development and conventional RE flow.

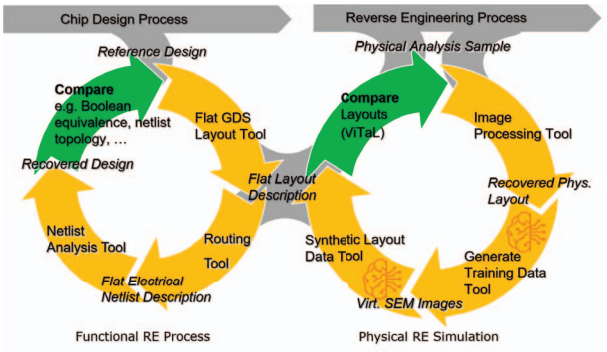


Fig. 9: Reverse Engineering Process Simulation Tool Chain.

The strength of new chip designs against hardware RE analysis can be evaluated by taking this design, converting the netlist into a layout and finally into non-hierarchical flat chip layout description, simulated to mimic images extracted from a real physical RE process [18]. From here we build the flat non-hierarchical netlist and evaluate existing netlist analysis methods. The recovered circuit design is compared against the original design demonstrating the RE process impact.

As the real physical RE process is considered to not be error free, a certain amount of netlist errors will remain during the functional design recovery. Furthermore, protecting measures could be used in the design phase to hinder effective reverse engineering and evaluated with respect to their strength ([21]–[23]). While AI image processing methods can convert a physical layout into vectored data, the inverse direction is also feasible, as we can simulate the chip scanning and delayering process. In addition, dedicated physical reverse engineering

projects on partial areas or special layers are used to improve the quality of the simulated data and verify the applied process.

D. Effective Hardware Trojan Detection

The increasing complexity and size of integrated circuits combined with the improvement of hardware Trojan design will further limit detection techniques relying on sampled randomised verification, e.g. in functional testing. Only very few methods for hardware Trojan detection can be applied without a benign design to compare against. As a consequence, the detection of Trojans (including backdoors) in foreign circuits is almost impossible. RE-based detection, that is analysing a chip for its high-level functionality and identifying unwanted or malicious parts, is an effective solution for this problem. At TUM, we have proven that an approach based on machine learning of Trojan-agnostic features of the circuit structure is efficient, reliable and future-proof, while performing significantly better than competing methods [24]. Using the ASIC developed at TUM, we seek to analyse and improve the capabilities of RE-based detection based on a real-world sample. In addition, we have the unique opportunity to evaluate other existing hardware Trojan detection techniques in a real-world scenario.

V. Conclusion

Within the ongoing RESEC project several innovative process solutions to reverse engineer products with sub-40nm process nodes have been developed. To achieve this, innovative methods must be developed for every step of the process. The customised scanner meets the requirements towards scanning speed and stage accuracy. Large chip area stitching is improved significantly. To the best of our knowledge, we propose the first automatic deep-learning based defect inspection framework that detects and classifies defects caused by preparation and the scanning process. The previous optimisations allow us to minimise manual effort and make our success quantitatively verifiable through the *ViTaL* framework. Accelerated RE for current process nodes paves the way for RE-based hardware Trojan detection. For this, we proposed the first automated detection technique that does not rely on Trojan characteristics. Furthermore, to allow for verification of the complete RE process, an IC with hardware Trojans was designed, and has started undergoing the first RE steps. Finally, the *CRESS* framework serves as a generalization to assess the relation between RE performance and results and counter-strategies.

In the final year of the project, we will focus on the evaluation of future ideas, including the strength of hardware protection mechanisms against RE analysis. The simulation tool chain for the RE process will be further developed. Finally, the complete hardware RE process will be evaluated to successfully reverse engineer the reference samples and identify the included hardware Trojans.

References

[1] Bundesministerium für Bildung und Forschung. (2019–2022). "RESEC, Analyse und Rekonstruktion höchstintegrierter Sicherheitsschaltungen," https : / / www . forschung - it - sicherheit - kommunikationssysteme.de/projekte/resec.

[2] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *48th ACM/EDAC/IEEE Des. Automat. Conf. (DAC)*, Jun. 2011.

[3] *The Role of Cloud Computing in a Modern Reverse Engineering Workflow at the 5nm Node and Beyond*, vol. ISTFA 2021: Conf. Proc. 47th Int. Symp. for Testing and Failure Anal. Oct. 2021.

[4] A. Kimura *et al.*, "A Decomposition Workflow for Integrated Circuit Verification and Validation," *J. Hardw. Syst. Secur.*, vol. 4, Mar. 2020.

[5] B. Lippmann *et al.*, "Verification of physical designs using an integrated reverse engineering flow for nanoscale technologies," *Integration*, vol. 71, Nov. 2019.

[6] R. Quijada *et al.*, "Large-Area Automated Layout Extraction Methodology for Full-IC Reverse Engineering," in *J. Hardw. Syst. Secur.*, vol. 2, Oct. 2018.

[7] E. Principe *et al.*, "Steps Toward Automated Deprocessing of Integrated Circuits," Nov. 2017.

[8] R. Courtland, "3D X-ray tech for easy reverse engineering of ICs [News]," *IEEE Spectrum*, vol. 54, May 2017.

[9] M. Holler *et al.*, "Three-dimensional imaging of integrated circuits with macro- to nanoscale zoom," *Nature Electronics*, vol. 2, no. 10, 2019.

[10] F. Courbon, "Practical Partial Hardware Reverse Engineering Analysis," *J. Hardw. Syst. Secur.*, vol. 4, Mar. 2020.

[11] U. J. Botero *et al.*, "Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives," *ACM J. Emerging Tech. Comp. Syst.*, 2021.

[12] Bundesministerium für Bildung und Forschung. (2021–2024). "FIDES, Know-how-Schutz und Identifizierbarkeit von Elektronikkomponenten für vertrauenswürdige Produktionskette," https : / / www . elektronikforschung.de/projekte/ve-fides.

[13] ——, (2021–2024). "VE-Velektronik Plattform für vertrauenswürdige Elektronik und sichere Wertschöpfungsketten," https : / / www . velektronik.de/en/.

[14] M. Vogel, *Handbook of Charged Particle Optics*, 2nd., J. Orloff, Ed., 4. Contemporary Physics, 2010, vol. 51.

[15] A. Singla, B. Lippmann, and H. Graeb, "Recovery of 2D and 3D Layout Information through an Advanced Image Stitching Algorithm using Scanning Electron Microscope Images," Jan. 2021.

[16] A.-C. Bette *et al.*, "Automated Defect Inspection in Reverse Engineering of Integrated Circuits," in *2022 IEEE/CVF Winter Conf. Appl. of Comput. Vision*, preprint: https : / / www . researchgate . net / publication / 355427265_Automated_Defect_Inspection_in_Reverse_Engineering_of_Integrated_Circuits, 2022, to be published.

[17] M. Ludwig, A.-C. Bette, and B. Lippmann, "ViTaL: Verifying Trojan-Free Physical Layouts through Hardware Reverse Engineering," in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2021, to be published.

[18] A. Singla, B. Lippmann, and H. Graeb, "Verification of Physical Chip Layouts Using GDSII Design Data," Jul. 2019.

[19] A. Hepp and G. Sigl, "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*, May 2021.

[20] M. Ludwig, A. Hepp, M. Brunner, and J. Baehr, "CRESS: Framework for Vulnerability Assessment of Attack Scenarios in Hardware Reverse Engineering," in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, preprint: https : / / doi . org / 10 . 36227 / techrxiv . 16964857, 2021, to be published.

[21] S. Dankowski, T. Gutheit, and B. Lippmann, "Semiconductor package authentication feature," U.S. Patent 11 063 000, Jul. 13, 2021.

[22] T. Kuenemund and B. Lippmann, "Chip and method for manufacturing a chip," U.S. Patent 9 385 726, Oct. 22, 2015.

[23] B. Lippmann and A. Junghanns, "System and method for integrated circuit planar netlist interpretation," U.S. Patent 7 937 678, May 3, 2008.

[24] A. Hepp, J. Baehr, and G. Sigl, "Golden Model-Free Hardware Trojan Detection by Classification of Netlist Module Graphs," in *2022 Des., Automat. & Test in Europe Conf. & Exhib. (DATE)*, 2022, to be published.