





### C. Hardware Trojans

HTs describe any malicious modifications of circuits, breaking the fundamental assumption of hardware serving as root-of-trust for secure data processing. Several studies have demonstrated HTs in real silicon [22]–[24]. By design, HTs are minor in extent but severe in fallout [23], [25], [26]. For example, HTs can undermine the reliability of circuits [27], corrupt computation [23], leak privileged data [28], or cause systems to stop working via glitching or denial-of-service (DoS) attacks [29]. Besides, HTs can be introduced at any point in the supply chain, e.g., at design time through 3rd-party modules, at manufacturing time through mask edits, even post-silicon at the package level [30], etc. Finally, most HTs comprise two distinct parts: trigger and payload. The trigger is an activation mechanism, typically based on rare and specific combinational/sequential conditions. Once activated, the payload performs the HT’s actual malicious operation.

### III. THREAT MODEL

#### A. Scope of EM-based HTs

EM-based HTs aim to decrease the lifetime of interconnects, synonymously defined as mean time to failure (MTTF) in this work. Such HTs realize glitching or DoS attacks that affect the interconnects but ultimately target the whole system [25], [29]. Given the fact that EM predominantly impacts direct current lines, EM-based HTs are most promising for PDNs [27], [31]; we follow the same adversarial approach in this work.

It is important to note that EM-based HTs (i) can be realized at design-time but also via post-silicon modifications of the circuits and/or package itself, e.g., by focused-ion beam (FIB) edits [32]; (ii) only require adversarial edits of the metal layers, rendering them resilient against traditional inspection focused on the active layer [33]; (iii) bypass regular post-silicon circuit testing, as their malicious payload is the delayed but built-in disruption of interconnects; (iv) are trigger-less and zero-gate.

In short, EM-based HTs enable delayed glitching or DoS attacks, while bypassing traditional HT detection.

#### B. Implementation of EM-based HTs

Adversaries can either aim for (i) lowering the critical stress, e.g., by changing the via configuration or removing redundant vias, or (ii) accelerating stress build-up, e.g., by introducing anode reservoirs or locally increasing current density [27], [31]. Note that, for both options, adversaries require detailed technology and design parameters, which can be obtained from technology providers and/or by careful inspection of the circuit design. Which option is more practical also depends on the attack point-in-time, as discussed next.

First, if HTs are implemented at design stage, they will be subject to current-density verification, where modifications to anode reservoirs and via configurations are more promising to remain stealthy. In contrast, implementing modifications at the mask level can be challenging, as this may require significant routing tracks/resources to be available/and or substantial rerouting. The latter may also lead to notable side-effects in power and performance profiles, which could enable detection.

TABLE I: Advanced 2.5D *CoWoS* System: Design Rules

Rule	Value	Rule	Value
Metal layers	4	Metal thickness	1 $\mu\text{m}$
PDN width/spacing	40 $\mu\text{m}$ /100 $\mu\text{m}$	Dielectric thickness	1 $\mu\text{m}$
Micro-bump pitch	40 $\mu\text{m}$	Micro-bump height/width	25 $\mu\text{m}$
Die height	200 $\mu\text{m}$	Interposer height	100 $\mu\text{m}$

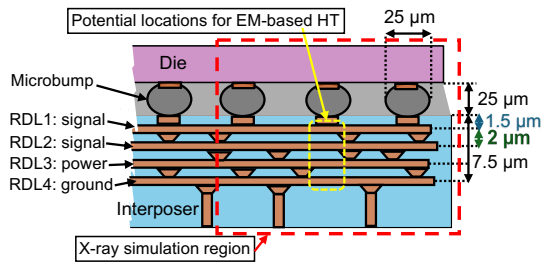


Fig. 3: Region of interest in the 2.5D *CoWoS* system.

Second, if HTs are implemented post-design, it seems promising to narrow down a wire and/or remove redundant vias. Such malicious modifications will increase the maximum current density and, thus, can only be applied in steps following layout verification, e.g., during mask preparation or FIB edits.

### IV. METHODOLOGY FOR EXPERIMENTAL INVESTIGATION

#### A. Setup for Case Study

**Advanced Packaging.** For practical relevance, we consider a SOTA, commercial-grade 2.5D system featuring the well-established *CoWoS* interposer technology [34]. See Tab. I for design rules from [34] and further rules defined for our study.

**Concept for EM-based HT.** Based on Sec. III-B, we devise EM-based HTs that shall locally increase the current density in the PDN, by narrowing down some PDN wire. Such malicious wire modifications can be small and, thus, hard to detect via X-ray inspection, especially when placed strategically under microbumps. We illustrate this key concept of our work in Fig. 3. Importantly, the *CoWoS* system [34] used for our case study utilizes wide power lines that can be easily narrowed down without violating minimal width constraints (0.4  $\mu\text{m}$ ) and carry high currents (upto 12 A in total)—such interconnects become prime targets for EM-based HTs.

Without loss of generality, we consider post-design attacks, and we assume attackers have capabilities for post-silicon, metal-only FIB edits of the interposer RDL, specifically of the PDN. To reflect supply-chain cost/throughput and limit detectability, we bound attackers to a per-device budget of a few localized FIB edits at roughly one device per hour. Furthermore, our evaluation targets for an in-field MTTF of upto  $10^5$  second (i.e., around a day) after inspection.

**Challenges for HT Implementation.** The main mechanism for the proposed EM-based HT is the combination of high current density and the resulting Joule heating, both accelerating EM (Fig. 4). While powerful in general, adversaries have to carefully implement this concept. First, stress has to build up fast enough (to cause wire degradation within some desired MTTF), whereas excessive heating has to be avoided (to ensure functionality during initial testing). Second, the

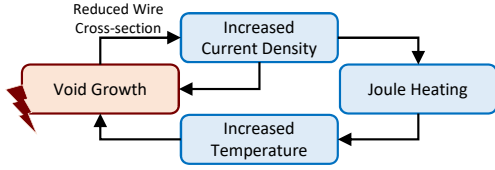


Fig. 4: Self-acceleration of EM-induced void growth [6].

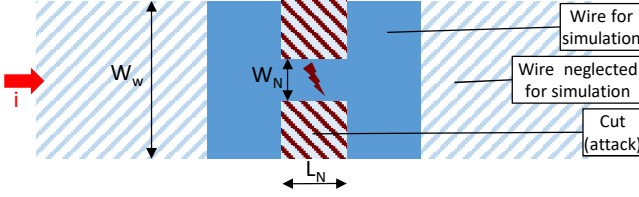


Fig. 5: Geometries for EM-based HTs under FEM simulations.

modifications of the wire should not significantly affect the IR drop and must, thus, be relatively minor. The modifications should also be minor to remain hidden under X-ray inspection. We study all these aspects in depth next.

### B. FEM Simulations for HT Concept and Design

**Model.** To capture stress caused by EM and SM, under Joule heating, we adopt a SOTA coupled structural, thermal, electric, and diffusion simulation model from [15], [17].<sup>2</sup>

**Geometries for HT Design.** Following Fig. 5,<sup>3</sup> we study the following two cases in detail:

- 1) *Baseline, no HT.* We model a long wire (of  $40\mu\text{m}$  width,  $W_w$ ) under a given current load. There is insignificant Joule heating, so MTTF is dictated by EM and SM at a constant temperature. The location of void nucleation is the cathode end of the wire.
- 2) *With HT.* By narrowing down a short portion  $L_N$  of the wire to  $W_N$ , the current density will increase locally and, due to current crowding, that narrow portion is heating up. Any increase in temperature accelerates EM and significant stress will build up around this narrow portion. Accordingly, the location of failure will quickly shift from the cathode to the narrow portion.

**Simulation Parameters.** We consider a typical operating temperature  $T_0 = 60^\circ\text{C}$  for the whole system, including the HT-impacted interconnects. We assume convection from all wire surfaces for heat leakage into the surrounding dielectric/underfill and package [35]. We consider current densities of  $0.125\text{ MA/cm}^2$ ,  $0.25\text{ MA/cm}^2$ , and  $0.5\text{ MA/cm}^2$ , respectively, which are typical values for interposer PDNs and in line with the power supply defined for the *CoWoS* system [34]. Furthermore, we set  $E_a = 0.8\text{ eV}$ .

<sup>2</sup>We consider the moment the critical stress is reached as MTTF. In reality, wires will not fail the very moment a void nucleates; the void has to reach a critical volume first. However, void growth is a fast process compared to the time until critical stress is reached. Also, the process is self-accelerating, as a void further reduces the wire cross-section and, thus, increases current density and Joule heating (Fig. 4).

<sup>3</sup>As shown, we limit the model to a small region of interest. We confirm that regions further away experience only negligible stress build-up.

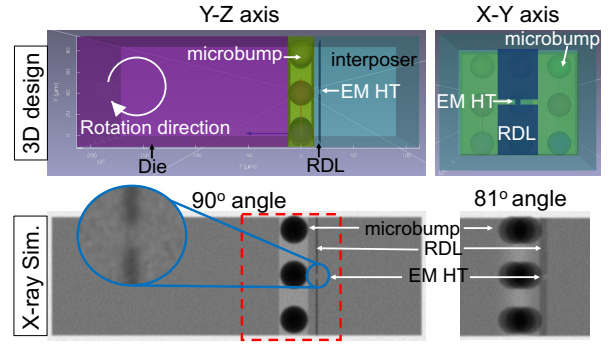


Fig. 6: Simplified *CoWoS* system in 3D design-space and corresponding, exemplary X-ray simulation result.

### C. X-Ray Simulations for HT Inspection

**Simplifications Toward Best-Case Detection.** Following Fig. 3, we simplify the advanced package of the 2.5D *CoWoS* system for X-ray simulations. Doing so enables best-case assessment for HT detection—which is equivalent to worst-case assessment for HT stealthiness—as follows:

- *Exclusion of C4 bumps and packaging structures below.* Large and dense packaging structures like C4 bumps can completely block X-ray beams in significant areas of the interposer. Thus, this simplification mimics scenarios where the interposer is inspected independently, which is not necessarily practical for in-line inspection.
- *Simplification of dies/chiplets.* The die above the region of interest is simplified to a silicon bulk, ignoring thin but dense intra-die metal layers that otherwise contribute to X-ray absorption and scatter.
- *Focus on single RDL.* The interposer is simplified to a silicon bulk except for the RDL with the HT. Doing so eliminates noise and scatter from other RDLs and TSVs.
- *Region of interest at interposer's edge.* Inspecting a region near the edge of the interposer prevents obstruction of view by other microbumps. Furthermore, scatter and attenuation of X-ray beams are less noisy near the edge.

Again, the idea is to limit any X-ray noise and scatter. If EM-based HTs remain hidden even in these conditions, we can conclude they will remain hidden in the full design as well.

**Simulation Setup.** We use Novi-Sim [36], a SOTA commercial software. Imaging parameters are set such that they do not impose limits for inspecting the RDL in detail against EM-based HT. Specifically, we use a field of view (FOV) of  $520\mu\text{m} \times 130\mu\text{m}$ , an exposure time of  $10\text{ s}$ , and a resolution of approximately  $0.97\mu\text{m}$ . We consider 360-degree rotation in the Y-Z plane, i.e., around the X-axis, for thorough profile views of the RDL. The motivation here is the same as above; once in-line imaging constraints apply, inspection becomes more noisy and limited and, thus, HT detection more difficult.

**Geometries for HT Design.** We use the same parameters as in the FEM simulation,  $L_N$  and  $W_N$  (Fig. 5). Furthermore, we model the distance of the RDL to microbumps,  $D_u$ . Figure 6 shows the geometry of the simplified package and examples for X-ray inspection around the X-axis, with the same region





Grounded in practical settings, our work supports further discussion. For example, the HTs' impact on IR-drop is relevant for stealthiness during testing and for attack effectiveness. For a typical PDN segment of  $100\ \mu\text{m}$  length (Tab. I), a HT as in Fig. 8 and with  $W_N = 10\ \mu\text{m}$  and  $L_N = 5\ \mu\text{m}$ , increases the resistance of the segment by 10%. Importantly, the PDN's redundant mesh structure limits the initial increase in IR-drop to only 0.10% on average and 1.02% at most,<sup>4</sup> rendering the HT stealthy. For the same HT and PDN, once the wire under attack fails, the IR-drop increases by 2.15% on average and 19.03% at most, which may well suffice for glitching or DoS attacks [25], [29]. Note that the limited initial increase in IR-drop may also allow adversaries to scale up the number of HT instances and tune their locations as needed for more powerful and/or targeted attacks, while still remaining stealthy.<sup>5</sup>

Our findings underscore that hiding EM-based HTs in an interposer's RDL is alarmingly robust. Consequently, assurance cannot be guaranteed by end-of-line inspection alone, but requires further efforts as follows. *Provision for high-resolution X-ray inspection of the interposer individually.* Doing so would remove the option for HTs to remain "lurking in the shadows" in the first place, but requires an additional inspection step and, more importantly, access to a trusted system integrator. *Explore new DFI approaches.* For example, interposer routing could establish keep-out zones under microbumps in general, or support more sophisticated heuristics to avoid routing of high-current wires "in the shadows" based on X-ray inspection-informed geometry and spacing constraints. Naturally, such DFI-enhanced routing should be easier to inspect and could be applied for regular in-line inspection of the fully integrated system, thereby also providing assurance against malicious system integrators.

#### ACKNOWLEDGMENTS

This work was supported in parts by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Grant No. 525041614, the U.S. National Science Foundation (NSF) under Grant No. 2143591, and the Center for Cybersecurity, New York University Abu Dhabi, UAE. We thank the reviewers for their constructive feedback.

#### REFERENCES

- [1] Y. Li *et al.*, "The applications of simulation and artificial intelligence in advanced packaging," in *IPFA*, 2024, pp. 1–5.
- [2] W. Chein *et al.*, "Advancements in metrology for advanced semiconductor packaging," in *Proc. SPIE*, 2024, p. 129970R.

<sup>4</sup>This is based on first-order SPICE simulations exploring all PDN segments for HT insertion, while assuming the same typical  $T_0 = 60\ \text{C}$ , nominal sheet resistivity, and power sources/sinks as defined and arranged in the CoWoS PDN [34]. Future work should consider full parameter modeling (R, L, G, and C), and also cover various temperature corners, to more thoroughly assess IR-drop and bound the resulting stealthiness and effectiveness of the HTs.

<sup>5</sup>In fact, for two instances of the same HT incorporated, the initial increase in IR-drop is still similar, namely 0.10% on average and 1.68% at most. Once the two attacked wires fail, the IR-drop increases more significantly, namely by 37.27% at most (and by 2.47% on average), confirming the scalability of the HTs. Furthermore, since the HT-induced changes in resistivity impact the current flow in the PDN right away, a detailed study of potentially premature EM-based failures for multiple HTs arranged nearby vs. afar, considering all currents and coupled Joule heating, should be the scope of future work.

- [3] D. Bernard, "X-ray advances in support of advanced packaging – today and tomorrow," *IMAPSource Proc.*, vol. 2018, pp. 409–414, 2018.
- [4] K. Yahyaei *et al.*, "From design to inspection: Can inspection-aware design enhance reliability in advanced packaging?" in *VTS*, 2025.
- [5] J. Xu *et al.*, "An assessment of electromigration in 2.5d packaging," in *ECTC*, 2019, pp. 2150–2155.
- [6] J. Lienig *et al.*, *Fundamentals of Electromigration-Aware Integrated Circuit Design*, 2nd ed. Springer, 2025.
- [7] A. Roy *et al.*, "Applications and challenges of AI in PCB x-ray inspection: A comprehensive study," *JETC*, vol. 21, 2024.
- [8] N. Varshney *et al.*, "Challenges and opportunities in non-destructive characterization of stacked IC packaging: insights from SAM and 3D x-ray analysis," 2024, p. 76.
- [9] S. Lau *et al.*, "Decoupling sub-micron resolution and speed from sample size in 3D x-ray imaging," in *IPFA*, 2022, pp. 1–6.
- [10] B. Peterson *et al.*, "Optimizing x-ray inspection for advanced packaging applications," *Int. Symp. Microelectron.*, vol. 2020, pp. 165–168, 2020.
- [11] M. S. M. Khan *et al.*, "CMx-ray: An x-ray compatibility metric for advanced packages to facilitate design-for-inspection," in *PAINE*, 2023.
- [12] K. Yahyaei *et al.*, "Design guidelines for in-line x-ray inspection in advanced packaging technology: A CoWoS case study," *IMAPS*, 2025.
- [13] —, "X-ADAPT: AI-driven design-based strategy to address x-ray compatibility challenges in advanced packaging metrology," in *SPIE Adv. Litho. + Patterning*, 2025, p. 134264C.
- [14] J. R. Black, "Electromigration – a brief survey and some recent results," *IEEE Trans. Electron Devices*, vol. 16, no. 4, pp. 338–347, 1969.
- [15] S. Rothe *et al.*, "Temperature-aware stress-based migration modeling in IC design: Moving from theory to practice," *AEU*, vol. 200, 2025.
- [16] —, "Stress-based electromigration modeling in IC design: Moving from theory to practice," in *SMACD*, 2024.
- [17] S. Rothe. (2024) Simulation scripts used in this work. [Online]. Available: <https://github.com/IFTE-EDA/EMinPractice>
- [18] L. Peters. (2024) Electromigration concerns grow in advanced packages. Semiconductor Engineering.
- [19] C. Liang *et al.*, "Electromigration reliability of advanced high-density fan-out packaging with fine-pitch 2-/2-um I/s cu redistribution lines," *TCPMT*, vol. 10, no. 9, pp. 1438–1445, 2020.
- [20] Y. Wang *et al.*, "Research on the reliability of advanced packaging under multi-field coupling: A review," *Micromachines*, vol. 15, no. 4, 2024.
- [21] J. Pak *et al.*, "Modeling of electromigration in through-silicon-via based 3d IC," 2011, pp. 1420–1427.
- [22] M. Muehlberghuber *et al.*, "Red team vs. blue team hardware Trojan analysis: Detection of a hardware Trojan on an actual ASIC," in *HASP*.
- [23] K. Yang *et al.*, "A2: Analog malicious hardware," in *SP*, 2016.
- [24] S. Ghandali *et al.*, "Side-channel hardware Trojan for provably-secure SCA-protected implementations," *TVLSI*, vol. 28, no. 6, 2020.
- [25] J. Knechtel, "Hardware security for and beyond CMOS technology," in *ISPD*, 2021.
- [26] J. Knechtel *et al.*, "Trojan insertion versus layout defenses for modern ICs: Red-versus-blue teaming in a competitive community effort," *TCHES*, vol. 2025, no. 1, pp. 37–77, 2024.
- [27] J. Lienig *et al.*, "Toward security closure in the face of reliability effects," in *ICCAD*, 2021, pp. 1–9.
- [28] T. Perez *et al.*, "Side-channel Trojan insertion - a practical foundry-side attack via ECO," in *ISCAS*, 2021, pp. 1–5.
- [29] H. Zhu *et al.*, "PCBench: Benchmarking of board-level hardware attacks and trojans," in *ASP-DAC*, 2021, p. 396–401.
- [30] J. Harrison *et al.*, "On malicious implants in PCBs throughout the supply chain," *Integration*, vol. 79, pp. 12–22, 2021.
- [31] C. Cook *et al.*, "Reliability based hardware trojan design using physics-based electromigration models," *Integration*, vol. 66, pp. 9–15, 2019.
- [32] C. Boit *et al.*, "From IC debug to hardware security risk: The power of backside access and optical interaction," in *IPFA*, 2016.
- [33] E. Puschner *et al.*, "Red team vs. blue team: A real-world hardware Trojan detection case study across four modern CMOS technology generations," in *SP*, 2023, pp. 763–781.
- [34] J. Kim *et al.*, "Chiplet/interposer co-design for power delivery network optimization in heterogeneous 2.5-d ICs," *TCPMT*, vol. 11, no. 12, 2021.
- [35] S. Rothe *et al.*, "Combined modeling of electromigration, thermal and stress migration in AC interconnect lines," in *ISPD*, 2023, p. 107–114.
- [36] D. Neffati *et al.*, "Novi-sim: A fast x-ray tomography simulation software for laboratory and synchrotron systems to generate training databases for deep learning applications," in *iCT*, vol. 28, no. 3, 2023.