Enhancing EU Cyber Defense Through Hardware Trojans Detection Capabilities

Vasile-Florin POPESCU[1], Victor GÂNSAC[2], Olivia COMȘA[3], Cristian ICHIMESCU[4], Dănuț TURCU[5], George BUCĂȚA[6]

[1, 4, 5] "Carol I" National Defence University of Bucharest, Faculty of Security and Defence
popescu.vflorin@unap.ro, ichimescu.cristian@unap.ro

[2, 3] SAFETECH Innovation
victor.gansac@safetech.ro, olivia.comsa@safetech.ro

[6] "Nicolae Bălcescu" Land Forces Academy of Sibiu, Faculty of Military Management

Abstract

Software Trojans and cybersecurity are a concern worldwide. Hardware Trojans are likely to be an issue faced by the Defence Industry of all countries. Information on how defense industry stakeholders deal with HT in Defense Products is by nature scarce or even inaccessible. It is however fair to assume that they adapt and use IC RE methodologies, notably some developed for IP infringement, to search for HTs. With these RE methodologies, checking a chip after its fabrication implies to deconstruct and analyze the whole surface and all the layers of a chip. It is thus hard to know for sure which states has acquired Hardware Trojan detection capabilities. There are however indications that some States could be in the process of acquiring such capabilities.

Index terms: defense industry, hardware Trojans, System-on-Chip, reverse engineering, image acquisition

1. Introduction

Communication technologies, and computing systems are an integral part of today's defense systems. They process security-critical information or perform calculations critical to the success of a defense operation or the safety of the military personnel on the ground. As such, they represent an obvious target for malevolent entities, including nation state adversaries. Software Trojan, virus and malware, are already well known cybersecurity threats, and many countermeasures are available or under continuous development. Hardware Trojan (HT), on the other hand, are becoming a recognized and immediate cybersecurity threat, but no available credible countermeasures are yet available to the European Defense Industry.

As such, they represent an obvious target for malevolent entities, including nation state adversaries. Defense electronics rely on complex System On Chips (SoC) that combine semi-conductors with multiple functions on a single Integrated Circuits (IC).

To reduce cost and time to market, these SoC are designed through a horizontal process and manufactured globally. This implies the intervention of several, potentially untrusted, stakeholders worldwide and comes with an increased security risks. Among these risks, the introduction of Hardware Trojans (HT) that could leak information or alter the functioning of a Defense system, is emerging as an immediate cybersecurity threat.

The European Industry as a whole retains the capacity to design SoC, thereby securing this step of the process. On the manufacturing side however, also called post-Tape Out, the situation is dire.

80% of SoCs are manufactured in Asia and some critical post-Tape Out steps are only provided by non EU suppliers. According to the study carried out by Hepp et al., 2022, demonstrates that the insertion of sophisticated HTs evading all routine tests is possible in less than 24 hours during manufacturing. This highlights the urgent need to rapidly implement large scale solutions to detect HT in SoC manufactured outside of the EU.

The EU's Defense Technological and Industrial Base (EDTIB)'s goal is to build a stronger and more competitive European industry. Communication technologies, and computing systems are ubiquitous both in current Defense products and in Defense technologies in development. Reliability and safety, including safety of information, are major features of defense products. To stay strong and competitive the European Defense Industry must therefore ensure that the Integrated Circuits at the core of communication technologies, and computing systems are safe and reliable. As of today the EDTIB is not autonomous in this as:

- ✓ it does not dispose of an industrially deployable technology allowing to check for HT presence in SoCs, while other Nation states might be developing such capabilities.
- ✓ it is dependent on non EU suppliers for ICs manufacturing. This is particularly obvious since 2020 and the COVID-19 pandemic, and the resulting world shortages coupled with higher prices of semiconductors.

To build a strong and competitive Defense industry, the EDTIB is dependent on demand, supportive political conditions, especially on the European level, but also on reliable and secure supply chains on the European continent as well as globally. There is a strong dependence of the European industry as a whole to foreign IC manufacturer, and the European defense industry is no exception. To be autonomous the EDTIB must rely on a European ICs supply chain. To act on this industrial dependence at the European level, the European Chips Act aims to centralize the production of chips in Europe instead of foreign countries. In February 2022, the European Commission has published a factsheet about the European Chips Act and its goals (Ludwig M, et al., 2022). The plan is split into three period of time. The HARTROID outcomes will support the EDTIB along the three phases of the constitution of a European IC supply chain, thus directly contributing to its autonomy.

The research methodology was represented by specialized literature analysis, corroborated with European directives from EU's Defense Technological and Industrial Base (EDTIB) and European Defense Fund (EDF).

2. Up-to-date analysis of the hardware Trojans identification studies

Considering the huge exposure of security systems vis- a vis hardware Trojans used in chips, R&D initiatives have started at the level of the European Union to come up with a sustainable solution to these threats, as follows:

- ✓ **EPoCH** project (H2020#695022) https://doi.org/10.3030/695022 which has as its primary purpose to develop of an open source software tool able to display and compare circuit netlists extracted from reverse engineering works.Although the extracted netlist is a very reliable way to find a Trojan, extracting the netlist of a high-end, multi-layered integrated circuit is a task that can easily take many months to accomplish.
- ✓ **SAFEST** project (H2020#952252) https://doi.org/10.3030/952252,https://safest.taltech.ee which approaches networking strategy on hardware security focused on testing practices, reverse engineering and hardware-based defenses.
- ✓ **EXFILES** project (H2020#883156) https://doi.org/10.3030/883156; https://exfiles.eu/ which has as its main objective research development of full IC reverse engineering techniques (de-processing, imaging) to get knowledge of encrypted mobile phone SoCs, in order to find

vulnerabilities that can be exploited by LEAs to get access to the stored information.

- ✓ **Codasip** High-end processor IP and high-level design tools for RISC-V (GA: 19010116) https://doi.org/10.3030/190101116
  Codasip offers a unique combination of semiconductor processor IP based on the RISC-V open instruction set architecture (ISA) and high- level EDA tool Codasip Studio providing outstanding flexibility and 5x faster time to market. RISC-V ISA can be used for a wide variety of applications ranging from low power and low gate count embedded cores to advanced high frequency application cores.
- ✓ **EXCEED** project - https://www.exceed-padr.eu/ The EXCEED project aims at creating a European supply chain of reconfigurable, flexible and trustable programmable system-on-a-chip family targeting a number of ruggedized and secure defense applications.
- ✓ **Intelligent Reliability 4.0** project (H2020#876659) https://doi.org/10.3030/876659; https://www.irel40.eu/
  The iRel4.0 project aims to reduce the failure rates of electronic components and systems all along the value chain. Although is a vast project that spans in many fronts, concerning the reliability of IntegratedCircuits they propose AI methods to classify IC SEM images to detect manufacturing defects on them.

3. Solutions to mitigate caveats within cyber defense capabilities

As other electronics, defense electronics rely on Integrated Circuits (IC) of various complexity, including System On Chips (SoC) that combine semi-conductors with multiple functions (memory, logic, MOS micro-components, analog…) on a single IC.

The design of an IC is a highly complex task requiring highly specialized staff, and is subject to short time to market window and cost restriction on the final product. This has led to a horizontal design and a global manufacturing process, which involves several, potentially untrusted, stakeholders worldwide and Third Party Intellectual Property (3PIP). The economic advantages of such design and manufacturing processes thus comes with an increased security risk. The European Industry as a whole retains the capacity to perform the design step thereby limiting the ability of an adversary nation state to tamper with IC design.

From the literature study performed by the authors, only a few academic papers present some elements relative to the discovery of Hardware Trojans within the analog or digital part of an IC (*X. Cao, et al.,2015, Y. Liu, et al., 2017, T. Inoue, et al., 2017, H. Salmani and M. M. Tehranipoor, 2016,* [1] *R. S. Chakraborty, et al., 2008*).

Modern circuits typically integrate several building blocks in the form of 3PIPs. Many proposed solutions tackling the HT issue are therefore focusing on detecting HT insertion during the design phase through unreliable3PIPs. HT implemented as post Tape Out modifications are starting to be discussed and are allegedly the most difficult to detect. To date, the IC design can be done by trusted partners in Europe and it is possible to secure the supply chain all the way totape-out.

But, at some point, at least for the advanced nodes, the masks and/or the actual manufacturing of the chip will be done outside of Europe.

On the manufacturing side however, also called post-TapeOut, the situation is dire. 80% of advanced chips are manufactured in Asia and some critical post-TapeOut steps (Dicing, Packaging), are mostly provided by non EU suppliers. Photomask fabrication is also a very sensitive post-TapeOut operation, that today is mainly provided outside EU. Even EU chip manufacturers could outsource it to foreign sub-contractors.

The testing and qualification of analog modules is more critical and requires dedicated test equipment and methodologies. For instance, RF chips typically need equipment such as high-frequency signal generators, signal analyzers, oscilloscopesetc. During chip qualification, the analog

modules are thoroughly tested with various stimuli. There are typically testing infrastructure embedded in the IC that allows bypassing, probing and stimuli application on areas of the chip that are not available during normal operation. This can, for instance, allow the verification of each segment in a signal chain individually. Sometimes part of this infrastructure is also used for production test and chip calibration. Areas that are considered to be extra sensitive can require a detailed analysis, but this typically only applies on few clearly identified areas.

Reverse Engineering (RE), which corresponds to the deconstruction and imaging of each layer of a manufactured IC for comparison with the initial design, is the only method with the potential to detect advanced HTs inserted during post Tape Out operations. Unfortunately, current RE methodologies can require over a full year of work. They are thus not compatible with the detection of HTs before the defense product harboring the infected SoC is deployed in operations.

The most time consuming parts of current HT detection methods by physical inspection are the delayering (figure 1) and image acquisition process.

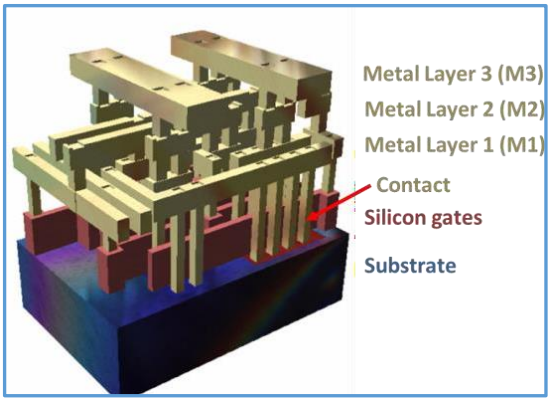

Fig. 1. Illustration of the different layers of a Chip, adapted from Hepp et al., 2022

The delayering process is still done almost in an artisanal way, using process and recipes adjusted to each chip technology (Torrance, *et al.*,2011; Huei Hao Yap and Zhi Jie Lau, 2019; H. B. Kor*, et al, 2020*).

IC with 3 metal layers (insulator removed): The sand-colored structures are metal interconnect. Layers are connected using vias. Contact connect Metal layer 1 to Substrate. The reddish structures are silicon gates. The solid at the bottom is the substrate.

The common and established delayering methods may include:

- ✓ Wet chemical etch: where liquid reactants are in contact with the IC chip creating a reaction with the surface materials. It is very important to precisely know the etching selectivity, i.e. the etching rate differences between construction materials. This process must be done in a standard chemical cabinet with fume extraction.
- ✓ Mechanical polishing: where sample surface material is removed using abrasive discs or cloths with abrasive slurry. Precision planar polishers can be used to perform this task, as well as precise CNC milling machines for local areas. Due to the narrow height of each construction layer, below 100nm for modern technology nodes, it is almost impossible to get a single layer exposed in the whole chip area using only mechanical polishing means.
- ✓ Dry Plasma Etch: Reactive Ion Etchers are specialized semiconductor fabrication equipment that can etch materials in the sample surface using a combination of physical and chemical means. Inert gas ions are accelerated to the sample surface to remove materials by physical sputter, aided by a plasma of gases that selectively reacts with the surface substances.

Regarding the image acquisition, due to the transparent nature of most of the chip's layers, and the narrow dimensions of its components, the visible light imaging is almost discarded. Scanning Electron Microscopy (SEM) can overcome this problem, offering images of sample surface topology up to few nanometers of resolution. To map an entire chip layer, several dozen thousand images are typically needed, and must be acquired in a precise, automated way. High end SEMs or Electron-Beam Lithographers (EBL) are used to perform this task. Given the SEM imaging time, requiring several seconds for each image, and the number of images needed to cover an entire chip layer, HT detection methodologies imaging the whole surface of the layers of the chip are likely to take several months or even exceeding one full year of work before providing any answer. This is particularly true for bigger chips such as the 25mm^2 chip that can be used in targeted applications. Reducing the area to image at high resolution is thus key to keep imaging time under control.

The schematic RE methodologies principle is illustrated in figure no. 2.

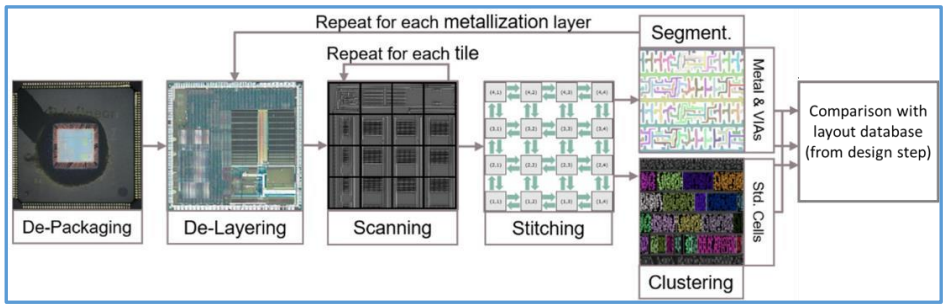

Fig. 2. Schematic illustrating RE methodologies principle. Adapted from Ludwig M, et al., 2021

A scheme for a possible process of identifying the hardware Trojans is presented below in fig. no. 3.

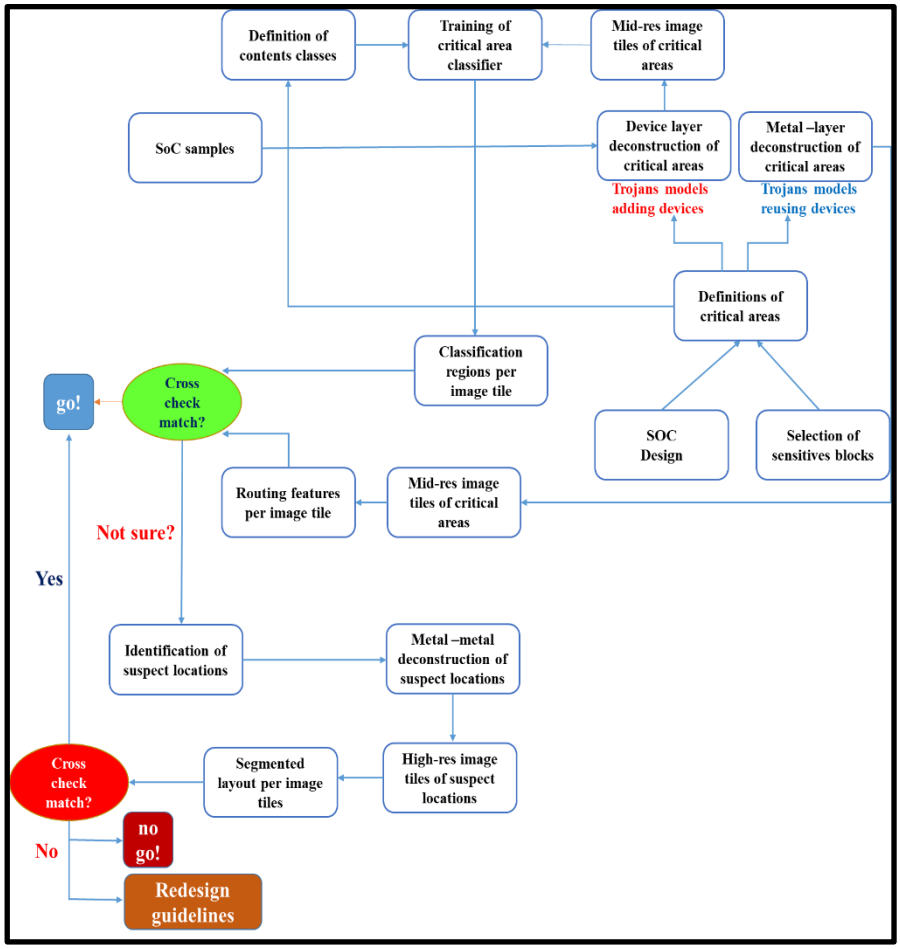

Fig. 3. A possible process of identifying the hardware Trojans

4. Conclusion

Under the Common Foreign and Security Policy (CFSP), and in particular in the context of the Capability Development Plan (CDP), the EU has identified 11 new priorities for capability development. One of these new priorities concerns cross-cutting capabilities that contribute to the EU's ambition. Under this priority, EDA aims to develop the autonomous EU capacity to test and qualify EU-developed defence capabilities prior to deployment in operations and missions, such as:

- *Integration of military capabilities - air security;*
- *Air superiority;*
- *Ground combat capabilities;*
- *Underwater control to contribute to maritime resilience;*
- *Naval maneuverability;*
- *Space-based information and communications services;*
- *Cyber-reactive operations;*
- *Air mobility;*
- *Information superiority;*
- *Improved logistical and medical support capabilities.*

As information technologies and computer systems are ubiquitous in defence products, SoCs are likely to form the basis for the operation of much of the solutions being developed to acquire new defence capabilities. Since Europe does not have control over the entire electronic component supply chain, it is strategically important for the EU to be able to test and qualify as Trojan-free the ICs that are part of solutions being developed to acquire the eleven capabilities defined in the CDP. Failure to do so would expose the newly developed capabilities to the threat of HTs. The consequences of the presence of HT in defence products are far-reaching: HTs can compromise cryptographic functions, leading to a weakening of the secrecy of communications, they can affect the sensitivity of various types of sensors (IR, radar...) or even enable unwanted remote control to switch some devices.

The implementation of large scale HT detection services, will likely come with the discovery of HT in chips destined to Defence products. This will raise the awareness of Defence Product manufacturer and foster cooperation between the latterand their design houses to identify and decrease risks. As a concrete example of potential cooperation between these entities, we could envision the identification of Defence product's function particularly targeted or vulnerable to the insertionof HT. This could lead to an improvement in the Defence product design by limiting or improving these functions, but also in the chip design by focusing design efforts to limit HT insertion risks in EU Defence.

Acknowledgments

This paper was published as part of the project "Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)", Contract No. 270 / 23.06.2020, ID 120436, funded under the Operational Program Competitiveness 2014-2020, Priority Axis: 1. Research, Technological Development and Innovation (RDI) to support economic competitiveness and business development.

References

[1]. Hepp *et al.*, A Pragmatic Methodology for Blind Hardware Trojan Insertion in Finalized Layouts. Arxiv. Aug. 2022. Accessed on 22.02.2023 at the address https://arxiv.org/abs/2208.09235.

[2]. Ludwig M, *et al.*, ViTaL: Verifying Trojan-Free Physical Layouts through Hardware Reverse Engineering. 2021. IEEE. Accessed on 23.02.2023 at the address https://ieeexplore.ieee.org/document/9707702.

[3]. X. Cao, *et al.*, "A hardware Trojan embedded in the Inverse Widlar reference generator," *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2015, pp. 1-4, doi: 10.1109/MWSCAS.2015.7282131.

[4]. Y. Liu, *et al.*, "Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 4, pp. 1506-1519, April 2017, doi: 10.1109/TVLSI.2016.2633348.

[5]. T. Inoue, *et al.*, "Designing hardware trojans and their detection based on a SVM-based approach," *2017 IEEE 12th International Conference on ASIC (ASICON)*, 2017, pp. 811-814, doi: 10.1109/ASICON.2017.8252600.

[6]. H. Salmani and M. M. Tehranipoor, "Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1214-1225, June 2016, doi: 10.1109/TIFS.2016.2520910.

[7]. R. S. Chakraborty, *et al.*, "On-demand transparency for improving hardware Trojan detectability," *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 48-50, doi: 10.1109/HST.2008.4559048.

[8]. Zachariasen M., Fixed Orientation Interconnection Problems: Theory, Algorithms and Applications DOCTORAL DISSERTATION. Department of Computer Science (DIKU) Faculty of Science University of Copenhagen.

[9]. Torrance, *et al.*, “The state-of-the-art in semiconductor reverse engineering” 2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 333-338.

[10]. Huei Hao Yap and Zhi Jie Lau, “Delayering Techniques: Dry/Wet Etch Deprocessing and Mechanical Top-Down Polishing”, Microelectronics Failure Analysis: Desk Reference, 7th ed., Edited By Tejinder Gandhi, ASM International, 2019, p 379–390.

[11]. H. B. Kor*, et al.*, "Sample Preparation for Deprocessing of 3D Multi-Die Stacked Package," 2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), 2020, pp. 1-6.