Proceedings of the 16th International Conference on Manufacturing Research, incorporating the
33rd National Conference on Manufacturing Research, 11-13 September 2018, University of Skövde, Sweden
Advances in Transdisciplinary Engineering: Volume 8: Advances in Manufacturing Technology XXXII pp. 305-310
DOI:10.3233/978-1-61499-902-7-305

Hardware Trojans and Smart Manufacturing – A Hardware Security Perspective

Sohaib ASLAM[1], Mohammad SAMIE and Ian K JENNIONS
School of Aerospace, Transport and Manufacturing (SATM)
Cranfield University, Bedfordshire, UK.

Abstract. Integrated Circuits (ICs) are the cardinal elements of modern electrical, electronic and electro-mechanical systems. Amid global outsourcing of ICs' design and fabrication and their growing applications in smart manufacturing or Industrie 4.0, various hardware security threats and issues of trust have also emerged. IC piracy, counterfeiting, and hardware Trojans (HTs) are some of the key hardware threats that merit the attention of manufacturing community. It is worth noting that the lower abstraction levels (ICs) are falsely assumed to operate securely. The proposition, therefore, is that if an operating system (higher abstraction level) is considered to be secure while operating on a compromised IC (lower abstraction level), would it be prudent to regard this implementation as secure? The purpose of this paper is to highlight IC level threats with an emphasis on hardware Trojans that pose a significant threat to smart manufacturing environment in the wake of Industrial Internet of Things (IIoT).

Keywords. Industrie 4.0, Integrated Circuits, Hardware Trojans, Smart Manufacturing.

1. Introduction

Electronics, conceivably more than any other realm of technology, has undergone an explosive evolution in the last five decades. Sophisticated Integrated Circuits (ICs) like Field Programmable Gate Arrays (FPGAs), Complex Programmable Logic Devices (CPLDs) and Application Specific Integrated Circuits (ASICs) have been seminal in this extraordinary phenomenon of technological growth. These circuits constitute the building blocks of consumer and industrial electronics. They help sustain national and international computer networks, manage transportation and power grids, and warrant the competitiveness of defence systems. The Internet of Things (IoT), autonomous vehicles, artificial intelligence (AI), cyber-physical systems (CPS), and industrie 4.0, all rely on optimised designing and implementation of integrated circuits. Concurrently, their optimisation implies a safe, reliable, and secure deliverance of the designed functionality and intended operation.

Till the last decade, the IC-level (hardware) of processing and computational systems either in System-on-Chip (SoC) or Network-on-Chip (NoC) configuration, was considered highly secure. The main onus had been on the Operating System-level

[1] Corresponding Author. s.aslam@cranfield.ac.uk

(software) for security breaches and malfunctioning of systems. However, with the global outsourcing of IC supply chain (Figure 1), a number of hardware oriented security threats as shown in Figure 2 have emerged, thereby raising issues of trustworthiness. These threats aim at leaking embedded secret keys and sensitive data, disabling vital system functionalities, degrading system performance, and accelerating device ageing process.

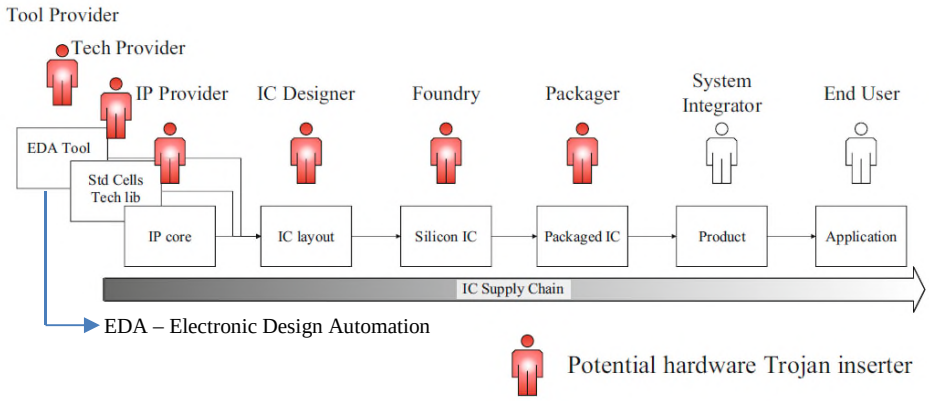

Figure 1. Integrated Circuit Supply Chain and Trustworthiness [4].

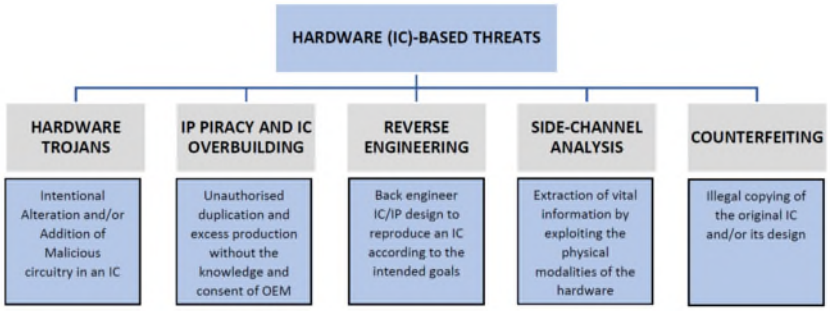

Figure 2. Hardware (Integrated Circuit-based) Threats.

With the industrial domain entering the fourth revolution, called Industrie 4.0 or smart manufacturing, the significance of becoming aware of IC-level security apart from high-level software and cybersecurity has increased manifold. Hardware Trojans, in particular, are being regarded as the major security concern for both the academia and industry [1-2]. In smart manufacturing domain, the focus is more on high-level security including device-security, server data security, and secure gateway [3]. There is no substantial work at the IC-level security, especially in the wake of hardware Trojans.

This paper, therefore, aims to fill this gap and familiarize the manufacturing community with the phenomena of hardware Trojans in integrated circuits - the bedrock of every electronic, electrical, and electro-mechanical system. The rest of the paper is structured as follows. Section 2 illustrates the phenomenon of hardware Trojans. Section

3 provides various hardware Trojan detection techniques and Section 4 draws the conclusion.

2. Hardware Trojans – Phenomenon and Classification

Hardware Trojan is defined as "*a malicious, intentional modification of a circuit design that results in an undesired behaviour when the circuit is deployed* " [2]. Bhunia *et al.* [5] have very aptly described hardware Trojan attack as "*a malicious modification of an IC during design or fabrication in an untrusted design house or foundry, which involves untrusted people, design tools, or components*". Referring back to Greek mythology of 'Trojan Horse', these hardware Trojans exhibit the similar stealthy nature and go undetected until activated by a rare event or condition.

As depicted in Figure 3, a typical hardware Trojan is designed to have 'Trigger' and 'Payload' logic [5]. Hardware Trojan action is initiated once the trigger input is received which, in turn, incites the payload to perform a specific attack. This could be a 'Time Bomb' disabling and damaging the circuit or a 'Backdoor' leaking sensitive data to an adversary.

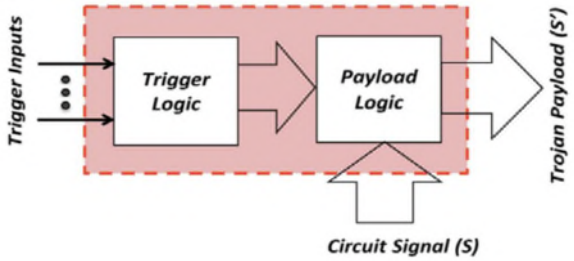

Figure 3. Hardware Trojan – Trigger and Payload [5].

Considering the IC supply chain (Figure 1), there can be a number of ill-intentioned proliferations by an adversary. These could be a modification of any specific line or paragraph of specifications, insertion of an extra line of source code, alteration in CMOS (Complementary Metal Oxide Semiconductor) geometries employed or sub-micron level modification in silicon die during fabrication stage. These Trojans can find their implementation in microprocessors, microcontrollers, Programmable Logic Controllers (PLCs), Field Programmable Gate Arrays (FPGAs), and Application Specific Integrated Circuits (ASICs).

2.1. Hardware Trojan Example

In order to explain the phenomenon of Hardware Trojan, consider the example of a CNC Motion Controller IC on the controller board in Figure 4. This chip or an integrated circuit is a Field Programmable Gate Array (FPGA), which is designed to function as a microcontroller. It sends precise signals to servo drives and amplifiers for controlling position, velocity and acceleration of the load along multiple axes. The feedback signal from an amplifier is analyzed by the microcontroller and error, if any, is corrected and sent back to the amplifier for a desired output. However, if this FPGA is added with the

Trojan gates and wires (indicated in red) that get activated with a specific high operating junction temperature, the error correction will not be generated. Instead, it will result in the malfunction and erratic motion profile of the CNC machine.

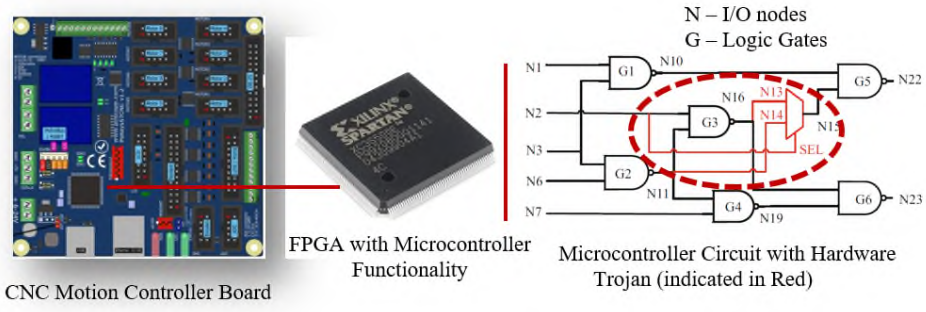

Figure 4. Hardware Trojan Example – Microcontroller on CNC Motion Controller board is inserted with Trojan gates and wires (indicated in red).

2.2. Hardware Trojans' (HTs) Taxonomy

Based upon the 'trigger' and 'payload' circuits' criterion, Wolff et al. [6] proposed the first taxonomy for HTs in 2008 followed by several revisions [7-10]. However, the most comprehensive classification of HTs made till to date is by Tehranipoor *et al.* [11] and Moein *et al.* [12]. Figure 5 represents the current taxonomy of Hardware Trojans. It is based on six hardware Trojan attributes as indicated in the figure below.

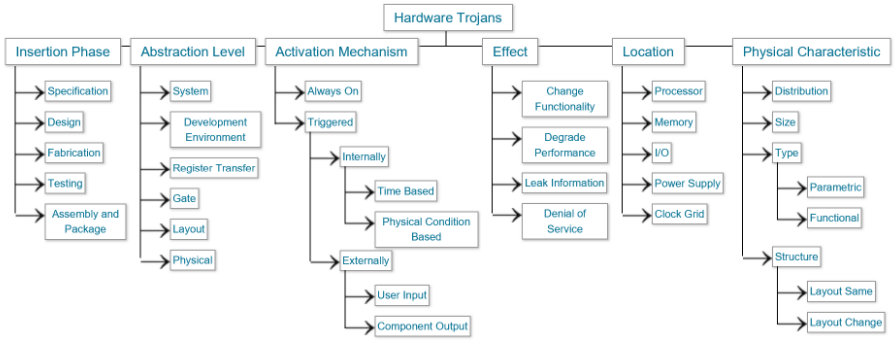

Figure 5. Hardware Trojans Taxonomy based on six attributes [11].

Insertion phase implies adding of extra circuitry or coding to the original IC design during any point of IC supply chain. The level of **Abstraction** indicates the control and flexibility an attacker may exercise on implementing HT. **Activation mechanism** defines the triggering of HT internally or externally or always remaining active. **Effect** determines the payload types of HT which could be changing the function of an IC, reducing its reliability etc. **Location** characterizes the placement of HT in any part of the circuit. **Physical characteristics** determine the alteration effected by HT in the functional or parametric elements, the spatial distribution within the circuit etc. How far these classifications have benefitted HT detection and counter-measuring is yet to be

seen. Salmani *et al.* [11] have critiqued the existing ad hoc nature of metrics and 'home-grown Trojans' along with varying assumptions for comparing various HT detection techniques. Accordingly, they have developed a suite of Trojans and 'Trust Benchmarks' to standardize and organize work on hardware Trojans [11].

3. Hardware Trojans – Detection Techniques

It may be well understood that even for a simple integrated circuit comprising a moderate gate density, the number of HT models with changing activation mechanisms and different effects may be substantial. As a result, devising a universal HT detection method for all HT infested ICs is highly improbable. Nevertheless, relentless efforts are being made to improve hardware security at micro-architectural level, encompassing both the detection and mitigation. The focus of this paper is, however, on HT detection.

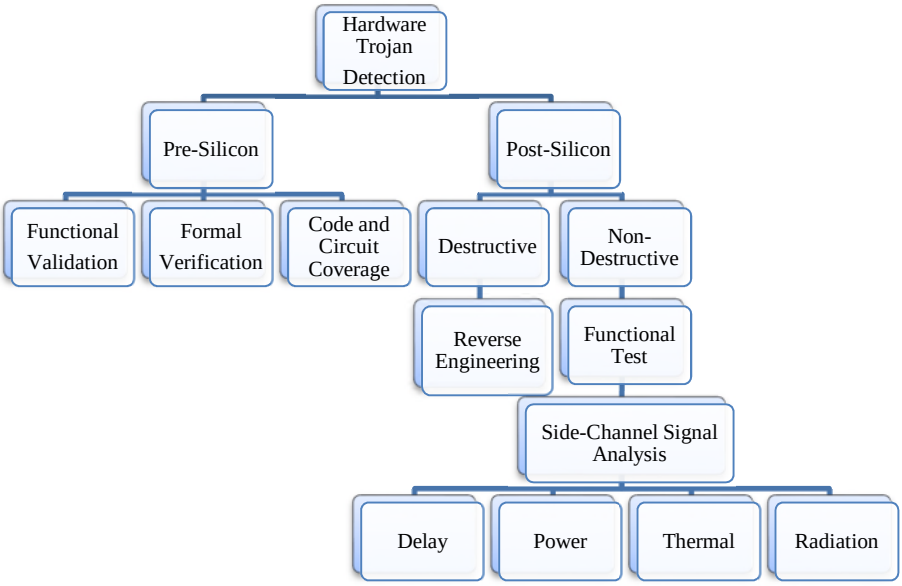

Figure 6. Hardware Trojans Taxonomy based on detection techniques [2].

As can be seen in Figure 6, **Trojan detection** at ***pre-silicon stage*** considers functional validation of IC design by generating different test patterns and carrying out a simulation to detect HTs. It is important to know that intellectual property (IP) cores act as black boxes in the circuit design. It is, therefore, vital to develop IP trust verification methods. A technique called VeriTrust [13] is used to pinpoint suspicious gates that are not driven by any dedicated trigger inputs. It may be noted that such inputs are not sensitized with verification test cases. Manual post-processing is, therefore, sometimes required to further analyse suspicious gates for confirmation, which is one of its main limitations. Formal verification is another viable pre-silicon stage technique that employs an algorithmic-based approach to verify logic if it satisfies the pre-defined security vectors. The recent methods being used for formal verification include

'equivalence checking', 'property checking' [14] and model checking [15]. Similarly, [16] have proposed a method which compares two analogous but untrusted designs for all possible input combination vectors to determine the functional differences between them.

Considering **'Trojan Detection'** at the ***post-silicon stage*** of an IC, both the non-destructive and destructive testing can be undertaken. In case of non-destructive testing, we suggest the analysis of un-programmed blank devices to determine their default output values and verify their electrical characteristics as per the datasheet. At the die-level and wire bound area, X-ray imaging [17] is deemed suitable; however, damaging effects of radiations may be kept in mind. Destructive method, on the other hand, employs IC de-capping and de-packaging. In addition to this, visual inspection and imaging techniques like scanning electron microscopy (SEM) [18] and scanning optical microscopy (SOM) [19] are also used to detect HTs inside the IC die. The downside, however, is the requirement of known-good ICs (golden ICs) for comparison, more time-consumption and complex testing with ever-increasing transistor densities. Moreover, the high cost of detection and IC destruction render destructive testing as unviable.

4. Conclusion

Integrated circuits are the bedrock of the existing state-of-the-art technologies. With enormous applications in industrie 4.0, IIoT, and cyber-physical systems in smart manufacturing environment, sophisticated types of integrated circuits will remain at the root of their optimised operations. The emergence of hardware security threats at the micro-architectural level of digital designs needs to be contemplated holistically in the smart manufacturing environment, in particular. Hardware Trojans, the intentional malicious modifications in integrated circuits, pose a major security concern for the manufacturing community. We, as a part of this community, have attempted to put forth a brief insight into the phenomenon of hardware Trojans in integrated circuits and highlight their debilitating impact on integrated circuit security, which in turn may jeopardise the safe and secure functioning of smart manufacturing systems.

References

[1] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, New York:, 2012.

[2] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: lessons learned after one decade of research," *ACM Trans. Des. Autom. Electron. Syst.*, 22, (2016), 1–23.

[3] C. Schmittner, Z. Ma, T. Ruprechter, and A. Aldrian, "Practical safe, secure and reliable machine-to-machine connectivity for cyber-physical-production systems," *22nd IEEE Int. Conf. Emerg. Technol. Fact. Autom.*, (2017), 1–4.

[4] S. Bhunia and M. Tehranipoor, *The Hardware Trojan War*, Springer, Cham, 2018.

[5] S. Bhunia, M. Banga, Hsiao, M.S., & S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures", in *Proceedings of the IEEE*,102 (2014), 1229-1247.

[6] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards Trojan-free trusted ICs: problem analysis and detection scheme," in *Proc. Des. Auto. Test Europe*, (2008), 1362–65.

[7] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: challenges and solutions," in *Proc. IEEE Int. Workshop Hardware Oriented Security Trust*, (2008), 15–9.

[8] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: threats and emerging solutions," in *Proc. IEEE Int. High Level Design Validation Test Workshop*, (2009), 166–71.

[9] M. Tehranipoor, and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," in *IEEE Trans. Des. Test Comput.*, 27 (2010), 10–25.

[10] J. Rajendran, E. Gavas, J. Jimenez, V. Padman, and R. Karri, "Towards a comprehensive and systematic classification of hardware Trojans," in *Proc. IEEE Int. Symp. Circuits and Systems*, (2010), 1871–74.
[11] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of Hardware Trojans and Maliciously Affected Circuits," *J. Hardw. Syst. Secur.*, (2017).
[12] S. Moein, S. Khan, T. A. Gulliver, F. Gebali and M. W. El-Kharashi, "An attribute based classification of hardware trojans," *2015 Tenth International Conference on Computer Engineering & Systems (ICCES)*, Cairo, (2015), 351-356.
[13] J. Zhang, F. Yuan, L. Wei, Y. Liu, and Q. Xu, "VeriTrust: verification for hardware trust," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 34 (2015), 1148– 61.
[14] E. Love, Y. Jin, and Y. Makris, "Proof-carrying hardware intellectual l property: a pathway to trusted module acquisition," *IEEE Trans. Inf. Forensics Security*, 7 (2012), 25–40.
[15] [34] J. Rajendran, A. Dhandayuthapany, V. Vedula, and R. Karri "Formal security verification of third party intellectual property cores for information leakage," *Proc. 29th Int. Conf. VLSI design*, (2016) 547–552.
[16] T. Reece and W. H. Robinson "Detection of hardware Trojans in third-party intellectual property using untrusted modules," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 35 (2015), 357–66.
[17] "X-ray Nanotomography Imaging for Circuit Integrity," [Online]. Available at: http://www ssrl.slac.stanford.edu/content/science/highlight/2011-09-26/x-ray-nano-tomography-imaging-circuit-integrity, [Accessed: 10 May. 2018].
[18] F. Courbon, P. Loubet-Moundi, J. J. A. Fournier, and A. Tria, "A high efficiency hardware Trojan detection technique based on fast SEM imaging," *Proc. Design Auto. Test Europe*, (2015) 788–93.
[19] B. Zhou et al. "Detecting hardware Trojans using back- side optical imaging of embedded watermarks," *Proc. 52nd ACM/EDAC/IEEE Design Automation Conf.*, (2015), 8– 12.

2018-12-01

Hardware trojans and smart þÿ m a n u f a c t u r i n g a h a r d w a r e s e

Aslam, Sohaib

IOS Press

Proceedings of the 16th International Conference on Manufacturing Research, incorporating the 33rd National Conference on Manufacturing Research, 11-13 September 2018, University of Skövde, Sweden. Advances in Transdisciplinary Engineering: Volume 8: Advances in Manufacturing Technology XXXII, pp. 305-310

https://doi.org/10.3233/978-1-61499-902-7-305