Modern Challenges in Hardware Design

Marek Zmuda
System Security Architect
Intel Technology Poland
marek.zmuda@intel.com

***Abstract*—Over the years, the technology of designing and manufacturing electronic devices has evolved dynamically, introducing new possibilities in the production of integrated circuits, devices, and systems. Despite advancements, significant challenges remain. The presented problems will be supported by examples from real-world projects, including Open Hardware, Chiplets, and security issues such as supply chain attacks, side-channel vulnerabilities, and quantum computing threats. This presentation aims to highlight interesting research directions related to hardware design that are crucial from an industrial perspective.**

***Keywords*—hardware design, design challenges, cybersecurity, supply chain security.**

I. Introduction

Each year, we observe increasingly rapid advancements in technologies related to the design and manufacturing of electronic circuits. These new possibilities often bring new challenges that are entirely different from those we have faced in the past. This presentation highlights attractive research directions related to hardware design that are crucial for industry. By examining recent trends and real-world examples from last years, the challenges related to Open Hardware, Chiplet technology, and critical security issues will be explored. The discussion will provide insights into how these problems impact design and production processes to finally consider strategies to address them.

II. Supply Chain Security Challenges

In today's world, electronic devices have become increasingly complex, with components sourced from numerous manufacturers. Modern integrated circuits often incorporate intellectual property (IP) from multiple suppliers, creating an interconnected system [1]. The design and manufacturing processes involve many subcontractors, each playing a critical role.

The presentation will showcase real-world cases where attacks on advanced supply chains had significant consequences, illustrating system vulnerabilities and the impact of security breaches. It will also discuss current countermeasures to prevent such situations. By examining these cases, we aim to highlight the importance of robust security practices and ongoing efforts to safeguard the integrity of electronic devices.

III. Internet of Things (IoT)

The market for IoT devices is experiencing rapid growth. Despite this swift development, there are no established industry standards for IoT that enable efficient and secure design and deployment of IoT-class devices [2]. This presentation will showcase solutions that offer hope for changing this situation, providing a pathway towards standardized practices that ensure both effectiveness and security in IoT device development.

IV. Side-channel Attacks

In recent years, we have observed a significant increase in both the cost and scope of side-channel attacks [3]. This trend is driven by the substantially decreasing cost of tools required to execute such attacks. The presentation will showcase representative examples of successfully conducted side-channel attacks on real-world devices available in the market. These examples will highlight the vulnerabilities exploited and the impact of these attacks, emphasizing the need for enhanced security measures in hardware design.

V. Quantum Computing

The capabilities of quantum computers are increasing significantly. Currently, widely known implementations of quantum computers do not allow for effective attacks on classical cryptographic algorithms. However, it is anticipated that with the advancement of quantum technology, this will change in the future [4]. The presentation will discuss current strategies to address this increasingly real threat, providing insights into the measures being developed to safeguard against potential quantum computing attacks.

VI. Conclusion

The dynamic evolution of electronic device design and manufacturing presents both opportunities and challenges. By focusing on innovative research directions and addressing critical issues such as supply chain security, IoT standards, side-channel attacks, and quantum computing threats, we can drive the advancement of the electronics industry.

References

[1] S. Maragkou, L. Rappel, H. Dettmer, T. Sauter and A. Jantsch, *The Pains of Hardware Security: An Assessment Model of Real-World Hardware Security Attacks*, IEEE Open Journal of the Industrial Electronics Society, vol. 6, pp. 603-617, 2025

[2] M. S. Sharbaf, *IoT Driving New Business Model, and IoT Security, Privacy, and Awareness Challenges*, 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 2022, pp. 1-4

[3] T. M. Ignatius, T. Birjit Singha and R. Paily Palathinkal *Power Side-Channel Attacks on Crypto-Core Based on RISC-V ISA for High-Security Applications*, in IEEE Access, vol. 12, pp. 150230-150248, 2024

[4] D. Bellizia et al. *Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design*, 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Athens, Greece, 2021, pp. 1-6