QUEEN'S UNIVERSITY BELFAST

SE RESEARCH INSTITUTE FOR SECURE HARDWARE & EMBEDDED SYSTEMS

UF UNIVERSITY of FLORIDA

SECURITY IN THE ERA OF GLOBAL SEMICONDUCTOR INITIATIVES

CHALLENGES AND OPPORTUNITIES

JULY 2024

Funded by

in association with National Cyber Security Centre

EPSRC Pioneering research and skills

CONTENTS

EXECUTIVE SUMMARY

This report outlines a strategic overview of the current challenges and emergent opportunities in semiconductor security, spurred by the insights from a workshop on Security in the Era of Global Semiconductor Initiatives, which was held in November 2023 in Washington DC. This workshop, co-hosted by the Research Institute of Secure Hardware and Embedded Systems (RISE) and Queen's University Belfast, in collaboration with the University of Florida, convened leading experts from the UK and US in academia, industry, and government to address pressing semiconductor security issues.

There are many significant security challenges confronting the semiconductor industry, ranging from the complexity of semiconductor designs and the viability of secure-by-design methodologies, to securing the hardware design lifecycle and mitigating risks associated with chiplets and supply chain vulnerabilities. The report also discusses the threats posed by side-channel attacks and the critical skills shortage in hardware security.

On the opportunities front, the report highlights secure-by-design approaches as essential for building inherently secure systems from the ground up. It advocates for the creation of a hardware vulnerability database to catalogue known hardware vulnerabilities, enhancing supply chain security measures, and leveraging automation and artificial intelligence (AI) to manage design complexity and enhance security. The report also underscores the value of open-source hardware security IP in fostering innovation and security within the semiconductor industry, alongside the necessity for quantifiable assurance through metrics and standards to quantify security assurance of hardware components throughout their lifecycle. Enhanced training and collaboration among industry, academia, and government are emphasized as vital to sharing knowledge and best practices to address semiconductor security challenges effectively.

The key recommendations arising from the report are as follows:

1. Provide Support for Secure-by-Design Initiatives
2. Balance Security with Performance
3. Create a Hardware Vulnerability Database
4. Adopt Security Mechanisms offering Traceability and Provenance
5. Research and Develop AI Enhanced Semiconductor Security Design
6. Adopt Open-Source Hardware Design
7. Establish Industry Standards and Metrics
8. Invest in Education and Training
9. Invest in Collaborative Research and Development

INTRODUCTION

The modern semiconductor supply chain uses overseas foundries, third-party IP and third-party test facilities. However, with so many different untrusted entities, this design and fabrication outsourcing has exposed semiconductor chips to a range of hardware-based security threats such as counterfeiting, IP piracy, reverse engineering and hardware Trojans (HT). Such hardware threats are major security threats for safety-critical and embedded systems applications, for example, in the medical, automotive or transport sectors. Due to the surreptitious nature of this industry, it is very difficult to ascertain the true scale of the problem.

The semiconductor supply chain has suffered severe shortages over the past five years due to material shortages, the Covid-19 pandemic, natural disasters and other major disruptions. This led to acute supply chain issues in a range of sectors, for example, the automotive industry. A small number of foundries in Korea, Japan, Taiwan and China currently dominate the global semiconductor fabrication industry and these nations have plans for further significant investment in this sector to retain their dominance. In addition to this, with high-profile attacks against critical national infrastructure, it is not surprising that both the sovereignty and cyber security of the semiconductor supply chain have become significant concerns for many countries.

The UK National Cyber Strategy 2022 [1] outlines the need to 'ensure that wherever possible the next generation of connected technologies are designed, developed and deployed with security and resilience in mind and … embrace a 'secure by design' approach'. Indeed, one of the 3 pillars of the UK's National Semiconductor Strategy [2], published in May 2023 focusses on ensuring that the 'importance of hardware for cyber security is considered, and more widely prioritised, at the design stage of chips'.

Similarly, the US CHIPS and Science Act [3] introduced in 2022 aims to strengthen the US semiconductor manufacturing ecosystem with significant investment in securing the supply chains for critical industries and ensuring the safety and cyber security of products produced within the US.

More recently, in February 2024, the White House Office of the National Cyber Director (ONCD) published a report [4] discussing approaches needed to reduce memory safety vulnerabilities at scale in order to define cyberspace. It specifically highlights the important role of hardware architectures alongside memory safety programming languages and formal methods in supporting memory protection, and calls out Capability Hardware Enhanced RISC Instructions (CHERI) [5] as an exemplar architecture.

In November 2023, the Research Institute of Secure Hardware and Embedded Systems (RISE) and Queen's University Belfast, in collaboration with the University of Florida, co-hosted a workshop on Security in the Era of Global Semiconductor Initiatives, in Washington DC. This workshop brought together leading UK and US industry, government and academic experts in semiconductor security. The themes discussed during the workshop included: Hardware Security Primitives; RISC-V security; Semiconductor supply chain security; Hardware-based attacks and countermeasures; Formal methods and tools for secure design and verification; System security.

The workshop was chaired by Professor Máire O'Neill, RISE Director, Queen's University Belfast, and Professor Mark Tehranipoor, University of Florida.

This report summarises the outputs of the workshop and outlines the challenges and opportunities in this sector.

In November 2023, the Research Institute of Secure Hardware and Embedded Systems (RISE) and Queen's University Belfast, in collaboration with the University of Florida, co-hosted a workshop on Security in the Era of Global Semiconductor Initiatives, in Washington DC. This workshop brought together leading UK and US industry, government and academic experts in semiconductor security.

ABOUT RISE:
RESEARCH INSTITUTE IN SECURE HARDWARE AND EMBEDDED SYSTEMS

The Research Institute for Secure Hardware and Embedded Systems (RISE: www.ukrise.org), which is hosted at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast, seeks to identify and address key issues that underpin our understanding of Hardware Security. Funded since 2017 by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC), RISE is one of four cyber security institutes in the UK and aims to be a global hub for research and innovation in hardware security.

RISE aims to address the following research challenges in Hardware Security:

1. Understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures.

- State-of-the-art Hardware Security primitives: True Random Number Generators (TRNGs), Physical Unclonable Functions (PUFs).
- Novel Hardware analysis toolsets and techniques.
- Attack-resilient Hardware platforms, Hardware IP building blocks.

2. Maintain confidence in security throughout the development process and product lifecycle.

- Confidence in Developing Secure Hardware devices.
- Supply Chain Confidence.
- Modelling of Hardware Security.

3. Hardware security use cases and consideration of value propositions.

- Novel Authentication, for example, alternatives to passwords.
- Secure document viewers.
- Securing BYOD (Bring Your Own Device) – attestation, roots of trust.

4. Development and pull through.

- Ease of Development and ease of leveraging best security options.
- Understanding Barriers to Adoption.
- Education of Potential User/Developer base.

Funded since 2017 by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC), RISE is one of four cyber security institutes in the UK and aims to be a global hub for research and innovation in hardware security.

UK AND US SEMICONDUCTOR INITIATIVES

In early 2023 the UK Prime Minister established the Department for Science, Innovation, and Technology (DSIT). Led by DSIT, semiconductors, artificial intelligence (AI), engineering biology, future telecoms, and quantum technologies are the five critical technologies that the UK has prioritized for the future, and semiconductors are the common thread that enables all the other four.

Atlantic Declaration, June 2023: The New Atlantic Charter 2021, which reaffirmed the UK and US's commitment to work together to realise a vision for a more peaceful and prosperous future, included a focus on protecting our innovative edge in science and technology to support our shared security and resilience against cyber threats. The Atlantic Declaration issued in June 2023 further built on this, providing a new framework of US/UK economic cooperation that included a commitment to explore collaborative research and development (R&D) in semiconductor technologies.

UK National Semiconductor Strategy

The UK's National Semiconductor Strategy, which was published in May 2023 emerged in response to supply chain disruptions during the COVID-19 pandemic and the risks associated with acquisitions of UK semiconductor companies. It aims to bolster supply chain resilience and safeguard against security risks.

Leveraging the UK's strengths in semiconductor research, design, and intellectual property (IP), the strategy aims to secure world-leading positions in future semiconductor technologies. This includes emphasizing secure semiconductor technologies.

The strategy commits to doubling down on areas of UK strength, particularly in design & IP, compound advanced materials, and research & development. It also outlines the importance of skills and talent development across the sector.

Preparation for high-tech sectors and specific critical sectors is a dual approach to safeguard against supply chain disruptions. The strategy underlines the importance of international cooperation in achieving supply chain resilience and emphasizes building stronger bilateral and multilateral partnerships, notably with the US, Japan, South Korea, and Taiwan.

Protecting UK assets and improving hardware cybersecurity are central to the strategy. It includes implementing regulations to enhance hardware security, promoting Secure by Design standards, and exploring opportunities and challenges with RISC-V architectures.

Digital Security by Design (DSbD) Challenge

As hardware demands become more ubiquitous, it's important that security innovation keeps up with the wider development and technology and that these innovations are adopted widely across society, industry, and government. The UK has therefore supported and are building on the Digital Security by Design (DSbD) challenge [6].

DSbD is a UK-based initiative aimed at fundamentally enhancing the security of digital systems. Funded by the UK government through UK Research and Innovation (UKRI) and in collaboration with industry partners, the challenge seeks to address the pervasive issue of vulnerabilities in digital technologies by rethinking the core design of software and hardware systems. The new design, CHERI (Capability Hardware Enhanced RISC Instructions), developed by the University of Cambridge has been implemented in a prototype by Arm (Morello) and a RISC V variant by LowRISC (Sonata). Research suggests it is possible 70% of ongoing memory safety vulnerabilities could be blocked from exploitation, with more benefits available through other features of the technology.

UK National Cyber Security Centre (NCSC) Hardware Security Problem Book

The NCSC aims to make the UK the safest place to live and work online, and emphasise the importance of cybersecurity across all aspects, including hardware security, to reduce risks to the UK. Hardware security is crucial as it underpins everything, from securing the UK's most sensitive systems to ensuring the integrity of commodity components.

In December 2023, NCSC published its Hardware Security Problem Book [7], which aims to inspire research by outlining challenges that they feel need significant research activity over the next five to ten years. The problems build from the physical properties of an electronic device, through designing devices with security in mind, up to integrating these devices into wider systems.

1. How do our devices physically behave, and how do we secure those behaviours?

Provide Support for Secure-by-Design Initiatives

2. How do we know that we can trust our devices?

It's important to understand the amount of trust we have in a device, and the limits of that trust.

3. What device architectures help us to improve security further up the stack?

To build devices that meet our security goals by design.

4. How do we integrate secure devices, to ensure that the security still holds at the system level?

To make it easy to build a secure system without needing to be an expert in every device used.

Further details on each problem can be found on the NCSC website at: www.ncsc.gov.uk/collection/problem-book/hardware-security

US Semiconductor Research Corporation (SRC) Microelectronics and Advanced Packaging Technologies (MAPT) Roadmap

The US SRC MAPT Roadmap [9] is an industry-wide 3D semiconductor roadmap to guide the future microelectronics revolution. The roadmap outlines the key research challenges that need to be addressed to ensure sustainable growth in the future and allow for next-generation advancements in the context of three fundamental limits of ICT sustainability: 1) energy sustainability; 2) environmental sustainability; and 3) workforce sustainability. It discusses Needs and Drivers, that include Application Drivers & System Requirements, Sustainable and Energy Efficiency and importantly, for this report, Security and Privacy. The report discusses: potential hardware security vulnerabilities in heterogeneous integration; feasible strategies to identify security aspects for Systems-in-a-Package (SiPs) and define fair metrics evaluating the security resilience of implementations; and finally, attack predictions and defence mechanisms in the context of medical devices. A summary of near-term and long-term threats and mitigations is provided, which includes a discussion on areas requiring further research. The key areas identified were: 1) Analysing logic locking, obfuscation, and camouflaging that are considered secure and stable in the context of the new advanced packaging models; 2) Secure placement of chiplets in EDA tools to minimise side-channels in 3D stacks; 3) better resource-constrained crypto algorithms; 4) non-lattice based post-quantum algorithms to improve diversity; 5) standards for inter-chiplet communication security; and 6) standards to support supply chain security.

US CHIPS for America

The US CHIPS for America vision emphasizes enhancing economic and national security by strengthening supply chain security, ensuring the US maintains manufacturing capabilities for advanced technologies, including secure chips for military use, and spurring innovation to ensure long-term US leadership in the semiconductor sector.

The CHIPS for America program involves a significant investment, with $39 billion allocated for manufacturing to attract large-scale investments in advanced technologies and expand manufacturing capacity, and $11 billion dedicated to R&D, focusing on areas such as the National Semiconductor Technology Center (NSTC), National Advanced Packaging Manufacturing Program (NAPMP), Manufacturing USA institute, and advancing measurement science with the National Institute of Standards and Technology (NIST).

US National Semiconductor Technology Center (NSTC): The NSTC aims to lead in next-generation semiconductor technologies, focusing on security and validation of the domestic microelectronics ecosystem, combating counterfeiting, and facilitating the implementation of security standards.

US National Advanced Packaging Manufacturing Program (NAPMP): NAPMP aims to establish US leadership in advanced packaging, addressing challenges in reliability, manufacturability, security, and installation of innovative technologies.

CHIPS Manufacturing USA Institute: The CHIPS Manufacturing USA institute, a first-of-its-kind will be focused on digital twins for the semiconductor industry, specifically focussing on the development, validation, and use of digital twins for semiconductor manufacturing, advanced packaging, assembly, and test processes.

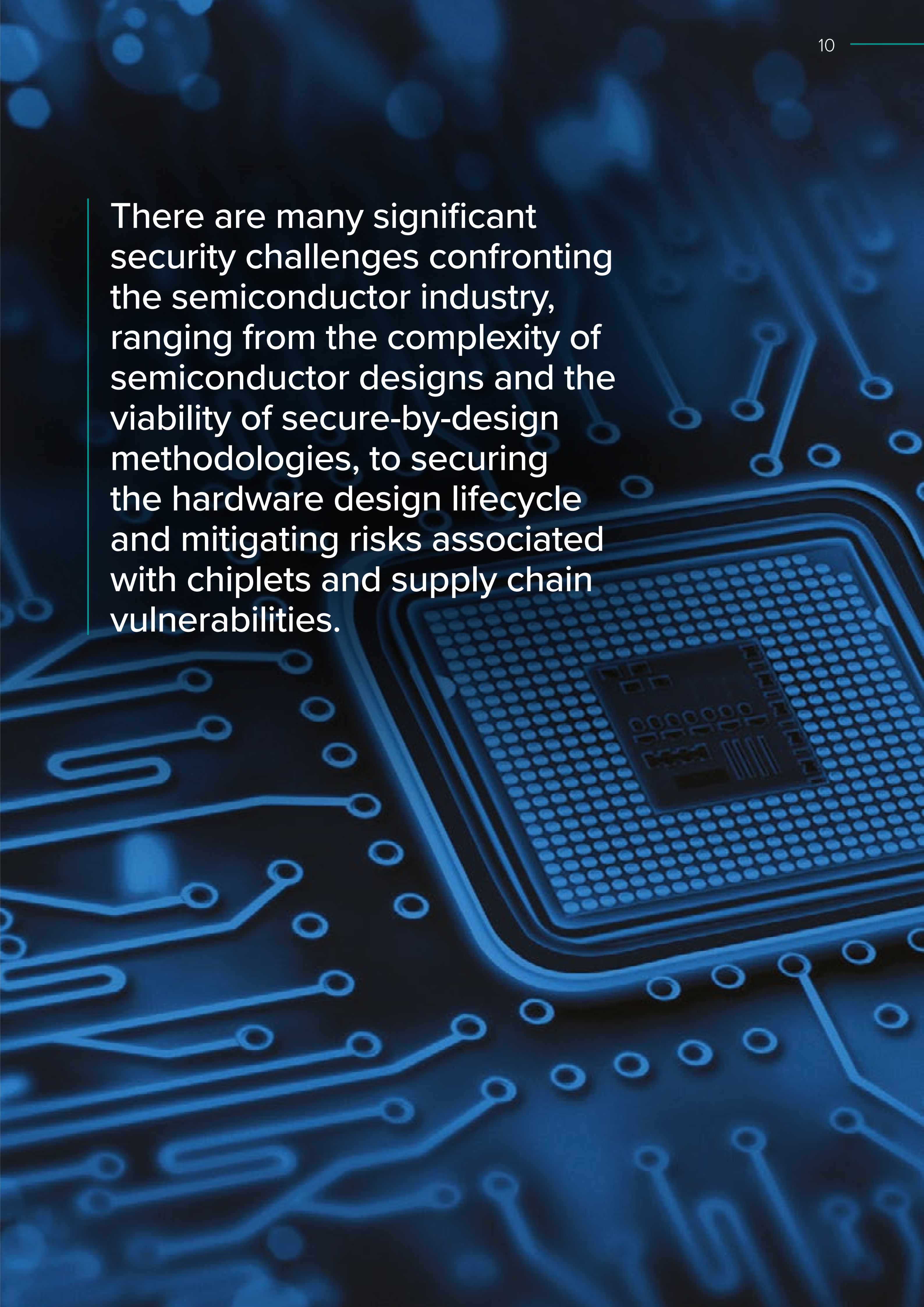
US Metrology Program: The CHIPS R&D Metrology Program, led by NIST, focuses on advancing measurement science for microelectronics, with specific initiatives targeting security challenges in the semiconductor industry.

Security is central to the CHIPS initiative, with efforts to ensure a secure and reliable semiconductor supply chain, especially for critical sectors. The CHIPS Incentives Program focuses on operational security best practices and risk management, covering the entire supply chain from design and fabrication to in-field applications.

International collaboration is emphasised as being critical to advance collective economic and national security and foster a resilient global semiconductor ecosystem.

US Semiconductor Research Corporation (SRC) Decadal Plan for Semiconductors

The US Semiconductor Research Corporation (SRC) Decadal Plan for Semiconductors [8] outlined 5 research grand challenges: 1) analog data deluge; 2) growth of memory and storage demands; 3) communication capacity versus data generation; 4) ICT security challenges; and 5) compute energy versus global energy production, emphasizing the need for breakthroughs in these areas to sustain the industry's growth. In terms of security, it states that breakthroughs in hardware research are needed to address emerging security challenges in highly interconnected systems and AI, with investment needed for privacy and security hardware advances that can keep pace with new technology threats and use cases (for example, trustworthy AI systems, secure hardware platforms, and emerging postquantum and distributed cryptographic algorithms).

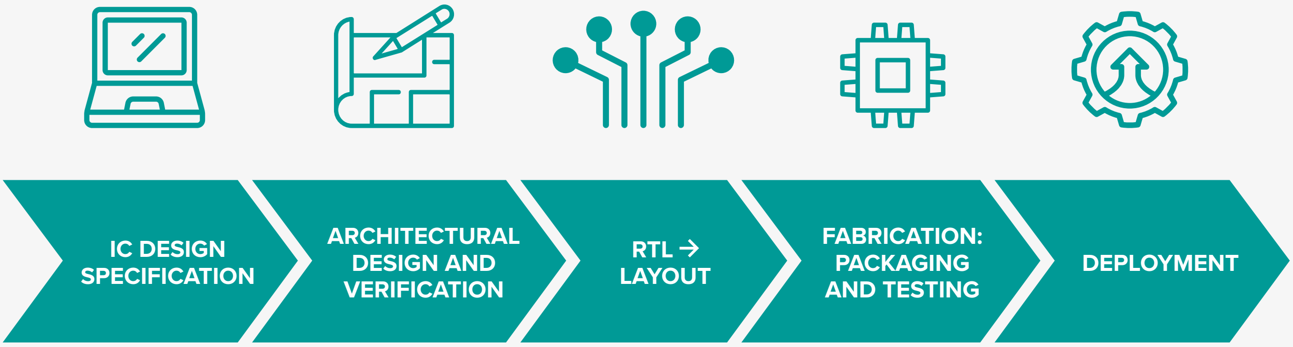


There are many significant security challenges confronting the semiconductor industry, ranging from the complexity of semiconductor designs and the viability of secure-by-design methodologies, to securing the hardware design lifecycle and mitigating risks associated with chiplets and supply chain vulnerabilities.

SEMICONDUCTOR SECURITY CHALLENGES

The semiconductor industry currently faces significant security challenges in an era marked by sophisticated cyber threats and complex geo-politics. This section outlines some of the key challenges facing the industry, from supply chain vulnerabilities to the complexity of securing microelectronic systems across their lifecycle. While the different stages in Integrated Circuit (IC) design and manufacturing are vulnerable to a range of security attacks, vulnerabilities due to unintentional design flaws are more common, some of which lie undiscovered for years. The figure below illustrates the many security threats that may be encountered during the different IC design and manufacturing stages.

Security threats in IC Design and Manufacturing



IC DESIGN SPECIFICATION

ARCHITECTURAL DESIGN AND VERIFICATION

RTL → LAYOUT

FABRICATION: PACKAGING AND TESTING

DEPLOYMENT

Unintentional flaws Unintentional flaws Unintentional flaws Unintentional flaws

Design in Hardware Trojans Tampering Over-production Counterfeiting

Hardware Trojans in IP IP Cloning Cloning Side-channel leakage

Untrustworthy EDA Tools IP Tampering Trojans

Complexity in Semiconductor Designs

The semiconductor industry faces significant challenges in managing increasingly complex designs with chips comprising up to hundreds of billions of transistors, advanced architectural features, and the integration of heterogeneous components. This complexity is driven by the demand for higher performance, lower power consumption, and greater functionality within the same or reduced chip area. However, it poses significant challenges for design, verification, and security.

With the rise in design complexity, traditional verification methods are becoming insufficient. There is a need for advanced verification techniques that can handle the scale and complexity of modern semiconductor designs. This includes the use of automated tools, formal verification methods, and simulation-based approaches to ensure that designs meet both functional and security requirements.

The increasing complexity of semiconductor designs also introduces new vulnerabilities and security risks. Complex designs can have unforeseen interactions between components that may create security loopholes. Ensuring security in such designs requires a comprehensive approach that considers all potential attack vectors, including hardware-based attacks, side-channel attacks, and fault injection attacks.

In addition, all layers of the device architecture (physical, logical, and software) need to be considered to ensure comprehensive security. Inadequate consideration of the interconnectedness of these layers can also result in security vulnerabilities.

A security maturity model is advocated for developing and maintaining system-on-chip (SoC) security assurance best practices, guiding the identification of activities needed to increase security assurance. Ensuring both forensic (reactive) and preventative (proactive) security measures are considered is also important. Such an integrated approach is crucial for understanding and implementing appropriate security measures that protect against a wide range of threats.

The security challenges due to the complexity in semiconductor designs are further compounded by the complexity of the global supply chain, as discussed later.

With the rise in design complexity, traditional verification methods are becoming insufficient. There is a need for advanced verification techniques that can handle the scale and complexity of modern semiconductor designs.

Is Secure-by-Design Achievable?

Addressing the security challenges of complex semiconductor designs requires integrating security considerations early in the design process – a ‘security by design’ approach – where security features and countermeasures are built into a design from the outset. Security needs to be considered as a foundational element of semiconductor design, rather than an afterthought. However, the lack of a clear definition of “secure by design” poses a challenge, as it makes it difficult to set and achieve concrete security goals. Secure by design should involve hardware actively protecting against vulnerabilities higher up in the stack. Securing hardware is critical as it underpins critical national infrastructure, such as telecommunications networks.

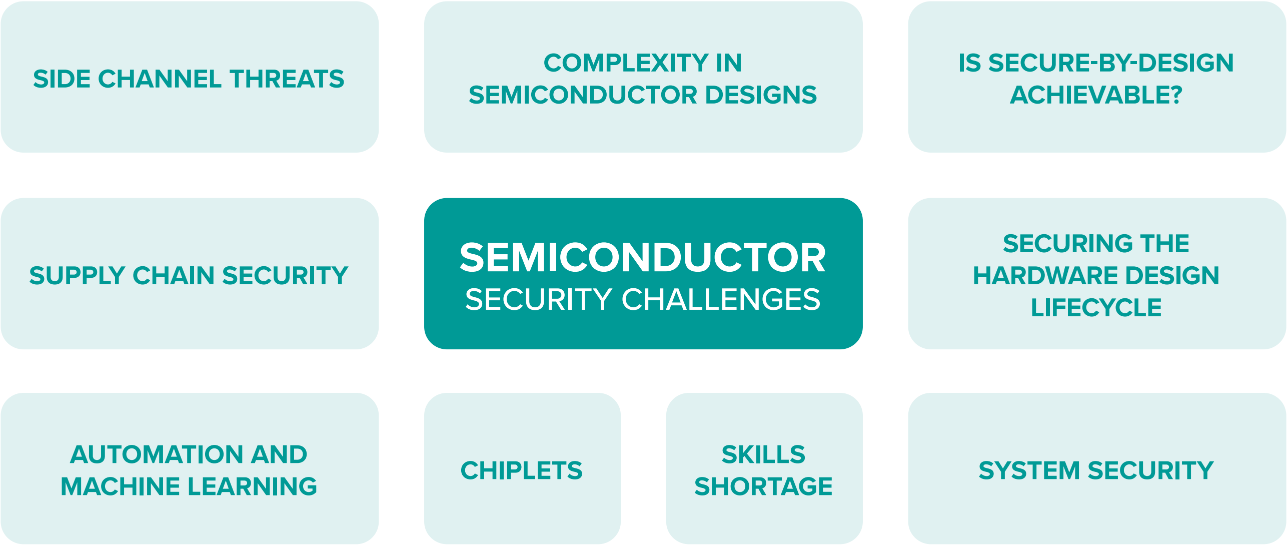
Secure by Design approaches include hardware-based roots of trust, encryption modules, secure boot mechanisms, and physical unclonable functions (PUFs), which provide a foundation for building secure systems and protection against unauthorized access and tampering.

Further approaches include designing hardware that reduces the attack surface and utilizing special programming techniques to ensure that the potential for vulnerabilities can be minimized and designing architectures that mimic air gaps for improved isolation. Enclaves, memory protection, and encrypting memories can help in preventing severe impacts from software mistakes.

The Digital Security by Design Programme (DSbD), detailed previously, aims to radically update the foundation of today’s insecure digital computing infrastructure, by demonstrating that mainstream processor technology (for example, from Arm) and software can be updated to include new secure-by-design technologies based on the CHERI Architecture, along with accompanying innovations across system software, runtime environments, formal verification, and tools.

It is also important that semiconductor products can be verified and validated for security post-manufacture. This includes creating mechanisms for attestation, secure updates, and recovery, thereby enabling trust and assurance throughout the product’s lifecycle.

A major challenge to achieving secure-by-design hardware is also the global shortage of skilled professionals capable of contributing to the secure design of future systems.


SIDE CHANNEL THREATS

COMPLEXITY IN SEMICONDUCTOR DESIGNS

IS SECURE-BY-DESIGN ACHIEVABLE?

SUPPLY CHAIN SECURITY

SEMICONDUCTOR SECURITY CHALLENGES

SECURING THE HARDWARE DESIGN LIFECYCLE

AUTOMATION AND MACHINE LEARNING

CHIPLETS

SKILLS SHORTAGE

SYSTEM SECURITY

System Security and Securing the Hardware Design Lifecycle

It is critical to integrate security considerations throughout the entire lifecycle of a hardware design, from pre-silicon to post-silicon stages, and that span from silicon to software and systems, taking a proactive approach to security rather than reactive measures.

There are major challenges to achieving system security. As discussed previously, the complexity of modern semiconductor systems makes it challenging to identify all potential security vulnerabilities and to implement comprehensive security measures that cover every aspect of the system and its design lifecycle. The security of the underlying components and processes do not imply system-level security. Many semiconductor products incorporate third-party IP and components. Verifying the security of these external elements can be difficult, especially when detailed implementation information is proprietary or unavailable. Implementing a true zero-trust architecture requires a comprehensive and strategic approach that goes beyond traditional security measures. Architecting for true zero trust involves a holistic approach that incorporates strict access controls, continuous verification, and data protection strategies. While trust can be composable, it requires standardised, interoperable claims and vigilant management to ensure that the overall security posture accurately reflects the collective trust level of all components.

There is also a lack of standardization in security practices across the semiconductor industry. This lack of uniformity can lead to inconsistencies in security implementations, making it harder to achieve a comprehensive and holistic security approach.

Achieving a balance between system performance, cost, and security is a recurring challenge. Adding security features can lead to increased complexity, higher costs, and potential impacts on performance. Organizations must carefully evaluate trade-offs to ensure that security enhancements do not unduly compromise other critical system attributes. In addition, it is necessary to future proof systems for future potential threats and attacks. The threat landscape is continuously evolving, with attackers developing new techniques and tools. Staying ahead of these threats to protect semiconductor systems requires ongoing vigilance, research, and investment in securityImplementing a holistic security strategy requires specialized knowledge and skills. However, there is often a gap in security expertise within organizations, combined with resource constraints that limit the ability to focus on security. This challenge is exacerbated by the current competitive demand for skilled cybersecurity professionals.

Chiplets

Chiplets are a novel approach to semiconductor design and manufacturing, where a single, larger chip is constructed from multiple smaller, modular pieces, or “chiplets.” This method deviates from the traditional monolithic design, where all components of a chip are fabricated on a single silicon die. Chiplets allow for greater flexibility, scalability, and efficiency in the design and production of ICs. The use of chiplets in semiconductor design introduces several security challenges that stem from their modular nature, diverse sourcing, and integration complexities.

Chiplets are often sourced from different suppliers, which complicates the tracking and verification of the security integrity of each component. Ensuring that all chiplets come from trusted sources and are not tampered with during transit is a significant challenge. The firmware and software running on chiplets must also be secure and free from vulnerabilities. However, the distributed nature of chiplet-based systems can complicate the deployment of updates and patches, increasing the risk of exploits. The compact nature of chiplet-based systems can also make them more susceptible to physical attacks, such as side-channel attacks. The interfaces and interconnects that facilitate communication between chiplets within a package also open up new potential attack vectors. Different chiplets may also adhere to different security standards and therefore integration into a system while maintaining a uniform security posture is also challenging.

Supply Chain Security

The global and interconnected nature of semiconductor supply chains introduces multiple points of vulnerability. Supply chain security in the semiconductor industry is a multifaceted issue, encompassing the integrity of components, the reliability of suppliers, and the mitigation of risks associated with the sourcing and integration of materials and technologies from a global network. This includes managing risks related to counterfeit components, malicious insertions, and other supply chain attacks.

There is currently a dependence on international suppliers for critical components and technologies. This reliance poses risks related to geopolitical tensions, trade restrictions, and the potential for supply chain disruptions that can impact the security and availability of semiconductor products. To mitigate risks associated with over-reliance on specific suppliers or regions, it is important to diversify supply sources. This will enhance resilience against disruptions and reduce vulnerabilities by broadening the supplier base.

As previously discussed, the use of third-party IP, components and chiplets within semiconductor designs is a security risk and ensuring the integrity and security of these external elements requires rigorous vetting processes and security audits.

Automation and Machine Learning

The growing complexity of semiconductor designs, coupled with the escalating number of security threats, necessitates the automation of security verification processes. Manual verification methods are becoming increasingly untenable due to the scale and intricacy of modern hardware systems.

Despite the clear need, the development and implementation of automated security verification tools face significant challenges. These include the creation of comprehensive security property sets for automated checking, the development of sophisticated algorithms capable of understanding complex hardware designs, and the integration of these tools into existing design and verification workflows.

Developing comprehensive sets of security properties that automated tools can check is challenging. These properties must encompass a wide range of potential vulnerabilities and attack vectors, requiring deep security expertise and continuous updates as new threats emerge.

In addition, automated tools may struggle to ensure security compliance and best practices are followed in highly complex, distributed, and heterogeneous systems, particularly if components are sourced from multiple vendors and include legacy parts.

Side Channel Threats

Side channels potentially exist at all levels of the design stack:

- Application: cryptanalysis of application data
- Software: control-flow side channels
- Memory: memory access side channels
- Architecture: timing side channels
- Circuits: physical measurement channels

Side-channel attacks, which are a significant concern in cryptographic hardware design, can also be applied to AI/ML hardware. These attacks can exploit data-dependent correlations, such as power or timing, to steal sensitive information such as trained machine learning models, disrupt operations, or cause critical misclassifications.

Many modern processors contain a Performance Monitor Unit (PMU), which allows the recording of architectural and microarchitectural events for profiling purposes. However, it has been identified as a potential side channel that could be exploited to reverse engineer microarchitectures, infer encryption keys, or implement attacks like Spectre [10] and Meltdown [11]. This highlights the need to carefully consider design aspects through a security lens, as components intended for performance enhancement may inadvertently introduce vulnerabilities.

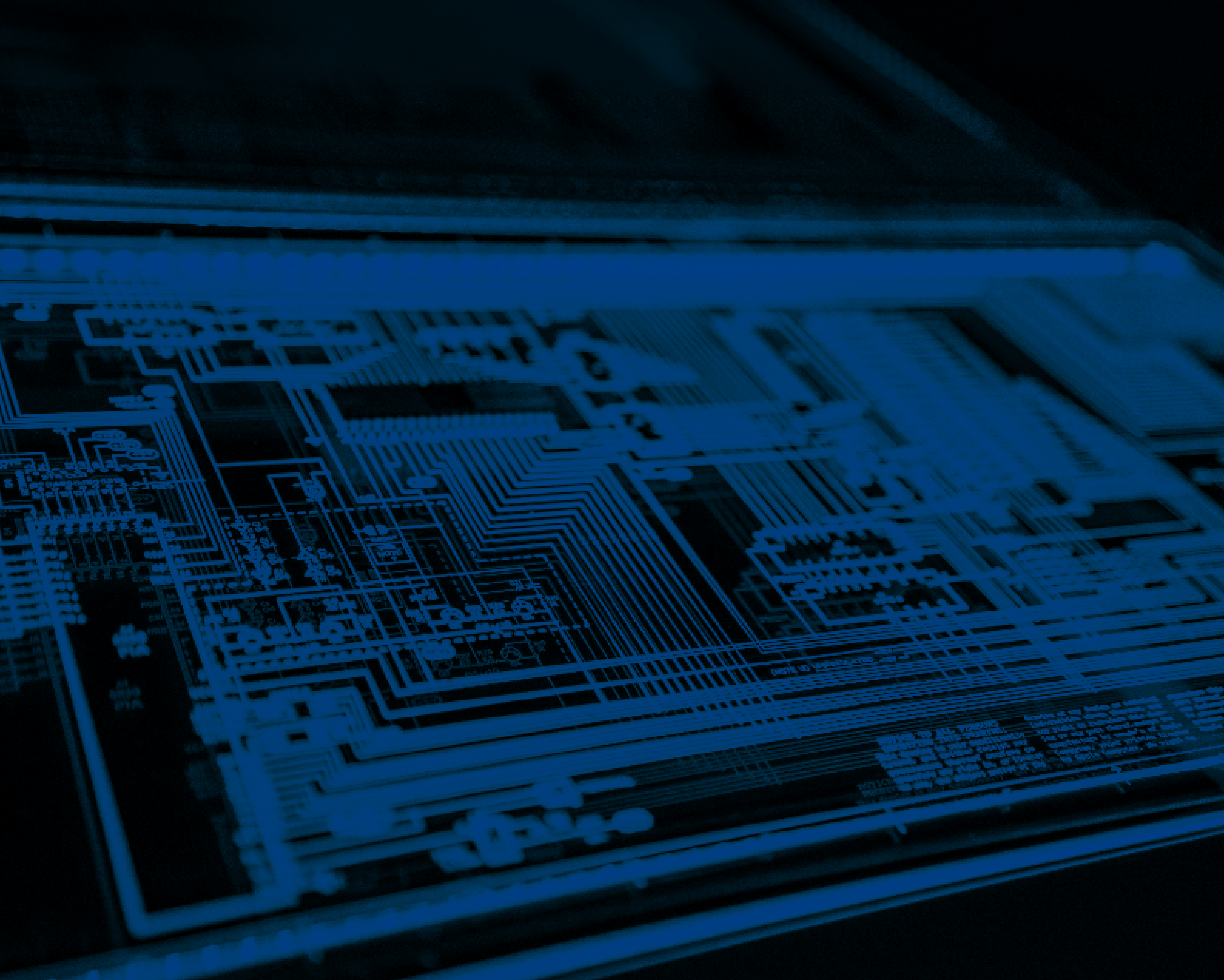
Skills Shortage

The skills shortage in cyber security is a critical issue globally. Initiatives to address this skills shortage rarely include hardware security. Hence, there is a pressing need to fill the significant gap in the skilled workforce required for the future security and design of systems. In the context of both the US and UK's strategic approach to semiconductor sector growth, interventions around skills and talent are pivotal. The respective efforts to support innovation throughout the lifecycle of semiconductor development, from early-stage research to scale-up are underpinned by initiatives focused on addressing the skills and talent needs voiced by the industry.

Diversity and inclusion are essential in addressing the skills shortage and there is a need for a broader talent pool beyond PhDs – a broader base of skilled individuals is essential for future growth and innovation.

SEMICONDUCTOR SECURITY OPPORTUNITIES AND RECOMMENDATIONS

The numerous security challenges facing the semiconductor industry outlined previously also bring significant opportunities for new research, innovation and economic impact. Innovations in hardware design, such as the shift towards open-source security IP and leveraging advances in AI for improved security verification, present promising avenues for strengthening the entire semiconductor ecosystem. The advent of advanced technologies and collaborative research and innovation between academia, industry and government has begun to pave the way for more robust, transparent, and resilient semiconductor architectures.



Secure-by-Design Approaches

Secure-by-design approaches in semiconductor development are becoming increasingly imperative, serving as a foundational element for creating inherently secure systems. It is essential to have early and consistent integration of security measures at the onset of hardware design, with security woven into the very fabric of semiconductor architectures.

Workshop discussions highlighted a need for a clear and comprehensive definition of what constitutes secure-by-design hardware. This clarity would aid in the creation of a common language and understanding, fostering industry-wide adoption of best practices. Establishing such standards is not just about prescribing measures but also about creating benchmarks that facilitate consistent evaluation and improvement of security postures across different hardware platforms.

Balancing security with performance is a challenging endeavour, particularly as the drive for higher efficiency and greater capability accelerates. Here, the goal is to ensure that security mechanisms do not unduly hinder the performance that users expect from their devices. Achieving this balance requires not only innovative design but also the optimization of existing technologies to create security measures that are both robust and unobtrusive.

Recommendation 1 – Provide Support for Secure-by-Design Initiatives

Governments and industry leaders should provide support and funding for initiatives aimed at advancing secure-by-design hardware, including research projects and the development of new technologies.

Recommendation 2 – Balance Security with Performance

Research and develop technologies that enhance security without significantly impacting performance, ensuring that secure-by-design hardware is practical for widespread use.

Hardware Vulnerability Database

In order to address the complex challenges and vulnerabilities within the global microelectronic supply chain a database to catalogue hardware vulnerabilities could be utilised, or a system CVE (Common Vulnerabilities and Exposures), drawing parallels to existing software vulnerability databases, and serving as a centralized repository for documenting known hardware vulnerabilities. This would facilitate the sharing of information about vulnerabilities, aiding in the quicker identification and mitigation of security risks associated with hardware components.

Recommendation 3 — Create a Hardware Vulnerability Database

Create a dedicated centralised database to catalogue hardware vulnerabilities, drawing parallels to existing software vulnerability databases.

> Balancing security with performance is a challenging endeavour, particularly as the drive for higher efficiency and greater capability accelerates. Here, the goal is to ensure that security mechanisms do not unduly hinder the performance that users expect from their devices.

Supply Chain Security Measures

To ensure supply chain security requires the development and implementation of measures that provide security and integrity assurances, including the verification of third-party IP and components, the adoption of transparent security practices and effective security and lifecycle management.

Implementing mechanisms for greater transparency and traceability throughout the supply chain is a crucial strategy, for example, privacy-preserving verification without revealing black box IP. This also includes adopting standards and technologies that enable the tracking of components from their origin through to integration into final products, ensuring their authenticity and security.

Strengthening collaboration among industry stakeholders, including manufacturers, suppliers, and regulatory bodies, is important for identifying and mitigating supply chain risks. Information sharing mechanisms that do not compromise proprietary or sensitive information are essential for a unified approach to supply chain security.

Secure manufacturing practices and the establishment of trusted foundries are also key components of a robust supply chain security strategy. This includes the implementation of security measures at the manufacturing level to prevent tampering and ensure the integrity of semiconductor devices.

Recommendation 4 — Adopt Security Mechanisms offering Traceability and Provenance

Adopt semiconductor security mechanisms with hardware traceability and provenance functionality.

Leverage Automation and AI

A recurring theme throughout the workshop was the need to invest in automation and AI technologies to manage the complexity of semiconductor designs and to enhance security through better documentation, traceability, and vulnerability assessment.

Machine learning (ML) and deep learning (DL) techniques were highlighted as promising tools for automating the generation of security properties. By analyzing existing designs and known vulnerabilities, ML algorithms can help identify potential security flaws in hardware designs and suggest relevant security properties for verification.

ML and DL models were also discussed as an effective means for detecting anomalies in hardware behaviour that may indicate security vulnerabilities. These models can be trained on vast datasets of normal hardware operations to identify deviations that could signal an attempt to exploit a design flaw or a previously unidentified vulnerability.

Further research and innovation is needed in the fields of automation and AI to address the security challenges faced by the semiconductor industry. This includes developing new methodologies for automating security verification, creating more accurate and efficient ML models for security analysis, and integrating these technologies into the hardware design lifecycle.

Recommendation 5 – Research and Develop AI Enhanced Semiconductor Security Design

Research and develop AI tools and methodologies for security verification and validation to manage the complexity of modern semiconductor designs effectively.

Open-Source Hardware Security IP

Open-source IP has an important role to play in fostering innovation, education, and security within the semiconductor industry.

The RISC-V architecture [12], which is being developed as an open standard, is an excellent example of the move towards open hardware to improve transparency and trustworthiness of devices. Open-source silicon roots of trusts include Caliptra [13] from the Open Compute Project (OCP) and OpenTitan [14].

Caliptra is targeted at data-centre focussed server-class ASICs and serves as a root-of-trust for both measurement and identity of a system-on-chip. OpenTitan is an open-source ecosystem, which produces both silicon IP and top-level designs capable of supporting numerous applications. It is supported by a consortium of companies, led by the non-profit lowRISC group. The OpenTitan IP set can now support quantum-resilient capabilities, specifically Sphincs+ and Crystals Kyber, which were selected by the US NIST as part of their post-quantum cryptography standardisation initiative. This highlights the proactive stance of open-source projects in addressing future security challenges, such as those posed by quantum computing.

Despite the benefits, there is a risk of fragmentation within open hardware standards and projects. The RISC-V ecosystem, including initiatives like Caliptra and OpenTitan, may be prone to fragmentation, and there is a need to maintain cohesion and compatibility across open-source projects.

Recommendation 6 – Adopt Open-Source Hardware Design

Adopt open-source hardware design approaches to improve transparency and trustworthiness. .

Quantifiable Assurance

There is a need for metrics and standards to quantify the security assurance of hardware components throughout their lifecycle.

The use of metrics and standards serves to delineate the security features and certifications adhered to by hardware components. This approach facilitates trust transfer, allowing industry to assure customers of the security of their products through third-party evaluations and certification.

The development of reliable methods for the verification of security assurance aspects of hardware parts is needed. This includes focusing on manufacturing issues, die identification and tamper detection. Quantifiable security assurance needs to span the entire lifecycle of semiconductor parts, from design, through to manufacturing to end-of-life. Another perspective involves the concept of a security maturity model, guiding the identification of activities necessary to enhance security assurance. This model advocates for methods that quantify and improve the performance of security measures, with a need for early identification of potential threats to make security efforts more cost-effective.

The sector should work towards establishing clear industry-wide security standards and best practices for the industry and ensure adherence to these standards to improve security outcomes across devices and systems.

PSA Certified [15] is an example of a global partnership providing independent evaluation to demonstrate commitment to IoT security. It offers a framework for securing connected devices, from analysis to security assessment and certification. It promotes a secure-by-design culture with a requirement that security is implemented at the beginning of product development.

Recommendation 7 – Establish Industry Standards and Metrics

Work towards establishing standardised security practices and metrics that can guide and assess the security efforts of hardware developers.

Enhanced Training and Collaboration

A common thread throughout the workshop was the need to promote enhanced training and collaboration between industry, academia, and government to share knowledge and best practices to drive innovation in semiconductor security, focusing on areas like secure system design, hardware/software interfaces, and AI applications in security . Global partnerships and initiatives focused on semiconductor security are vital to help embed a culture of security-by-design within organizations and ensure delivery of trusted and resilient products and ecosystems.

It is recognised that while there is some degree of skills development and training available, this is on a very small scale and is not sufficient to meet the industry's current or future needs. Hence, dedicated training programs on semiconductor security need to be expanded to a much larger scale to fulfil the demand for skilled professionals in both the industry and government sectors, with a focus on diversity and inclusion to foster a more varied and innovative workforce.

Recommendation 8 – Invest in Education and Training

Address the skills shortage by investing in education and training programs in semiconductor and hardware security design, ensuring a diverse and inclusive scholar pipeline.

Recommendation 9 – Invest in Collaborative Research and Development

Invest in collaborative partnerships, in particular, trusted international partnerships between academia and industry to drive innovation in semiconductor security and address the unique challenges of semiconductor technologies.

> A common thread throughout the workshop was the need to promote enhanced training and collaboration between industry, academia, and government to share knowledge and best practices to drive innovation in semiconductor security.

WORKSHOP CHAIRS

Máire O'Neill, FREng, FIAE, MRIA, is Regius Professor in Electronics and Computer Engineering and Director of the Centre for Secure Information Technologies (CSIT) at Queens University Belfast, Northern Ireland. She is also Director of the UK-wide Research Institute in Secure Hardware and Embedded Systems and serves on the Responsible AI UK leadership team.

She is internationally recognised for her research in the areas of hardware security and applied cryptography. She previously held a UK EPSRC Leadership Fellowship (2008–2014), was a former holder of a UK Royal Academy of Engineering research fellowship (2003–2008) and led the €3.8M EU H2020 SAFEcrypto (Secure architectures for Future Emerging Cryptography) project (2014–2018).

She has received numerous awards which include a 2024 Royal Irish Academy Gold Medal, a Blavatnik Engineering and Physical Sciences medal, 2019, and a Royal Academy of Engineering Silver Medal, 2014. She is a Fellow of the Royal Academy of Engineering, a member of the Royal Irish Academy and Fellow of the Irish Academy of Engineering.

Mark M. Tehranipoor is currently the Intel Charles E. Young Preeminence Endowed Chair in Cybersecurity and the Chair of the Department of Electrical and Computer Engineering (ECE) at the University of Florida. He served as the founding Director for Florida Institute for Cybersecurity (FICS) Research from 2015–2022, and is currently serving as Director for Edaptive Computing Inc. Transition Center (ECI-TC), Co-director for the AFOSR/AFRL Center of Excellence on Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN), and Co-Director for the National Microelectronic Security Training Center (MEST).

He has published numerous journal articles and refereed conference papers and has delivered 220+ invited talks and keynote addresses. In addition, he has 18 patents issued, 23 pending invention disclosures, and has published 16 books of which two are textbooks. His projects have been sponsored by 50+ companies and Government agencies.

Professor Tehranipoor is a Fellow of IEEE, a Fellow of ACM, a Golden Core Member of IEEE Computer Society, and a Member of ACM SIGDA. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and co-founded IEEE Asian-HOST and the IEEE International Conference of Physical Assurance and Inspection of Electronics (PAINE). Further, he co-founded the Journal on Hardware and Systems Security (HaSS) and currently serving as EIC for HaSS. He is also led development of Trust-Hub sponsored by the National Science Foundation (NSF).

WORKSHOP CONTRIBUTORS

Government Representatives

UK Department of Science, Innovation and Technology (DSIT)
UK Defence Science and Technology Laboratory (DSTL)
UK National Cyber Security Centre (NCSC)
US CHIPS Program Office
US Department of Homeland Security
US National Institute of Standards and Technology (NIST)
US Defense Advanced Research Projects Agency (DARPA)

Industry Representatives

Dan O'Loughlin, VP Engineering, Qualcomm
Adam Cron, Distinguished Architect, Synopsys
John Oakley, Semiconductor Research Corporation (SRC), US
Angela Dalton, Director, AMD Research & Advanced Development, AMD
Doug Gardner, Chief Technologist, Analog Devices
David Maidment, Arm
Shawn Fetterolf, Intel
Sid Allman, Senior Technical Director, Marvell Technologies
Manuel Offenberg, CTO/Chief Architect, Seagate Federal
Patrik Ekdahl, Manager Platform Security, Ericsson

Academic Representatives

John Goodenough, University of Sheffield
John Goodacre, University of Manchester
Simon Moore, University of Cambridge
Dan Page, University of Bristol
Ahmed Atamli, University of Southampton
Waleed Khalil, Ohio State University
Farinaz Koushanfar, University of California San Diego
Shreyas Sen, Purdue University
Aydin Aysu, North Carolina State University
Ramesh Karri, New York University
Gang Qu, University of Maryland
Farimah Farahmandi, University of Florida

REFERENCES

[1] UK National Cyber Strategy 2022, available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022.

[2] UK National Semiconductor Strategy 2023, available at: https://www.gov.uk/government/publications/national-semiconductor-strategy.

[3] US CHIPS and Science Act 2022, available at: https://www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf

[4] White House Office of the National Cyber Director (ONCD), "Back to the Building Blocks: A Path Toward Secure and Measurable Software", available at: https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf, February 2024.

[5] R N.M. Watson, S. W. Moore, P. Sewell, P. G. Neumann, An Introduction to CHERI, Technical Report Number 941, University of Cambridge, September 2019, available at: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-941.pdf.

[6] UKRI funded project – Digital Security by Design (DSbD) Challenge – https://www.dsbd.tech/

[7] The NCSC Research Problem Book, available at: https://www.ncsc.gov.uk/collection/problem-book.

[8] Decadal Plan for Semiconductors – Full Report, Semiconductor Research Corporation (SRC), January 2021, available at: https://www.src.org/about/decadal-plan/

[9] Microelectronics and Advanced Packaging Technologies (MAPT) Roadmap, 2023, available at: https://srcmapt.org/

[10]P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom, Spectre Attacks: Exploiting Speculative Execution, 40th IEEE Symposium on Security and Privacy, 2019.

[11] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A, Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, Meltdown: Reading Kernel Memory from User Space, 27th USENIX Security Symposium, 2018.

[12]RISC-V Open Standard Instruction Set Architecture – https://riscv.org/

[13]Caliptra Silicon RoT Services, Open Compute Project – https://github.com/chipsalliance/Caliptra

[14]OpenTitan Silcon RoT Project – https://opentitan.org/

[15]IoT Security Framework and Certification – PSA Certified: https://www.psacertified.org/

RISE

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: info@ukrise.org.uk
T: +44 (0) 28 9097 1771
𝕏 @UK_RISE
in UK RISE