RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

QUEEN'S UNIVERSITY BELFAST

FUTURE RESEARCH TRENDS IN SECURITY HARDWARE AND EMBEDDED SYSTEMS

2025 ISAB REPORT

Funded by

in association with National Cyber Security Centre

EPSRC Pioneering research and skills

CONTENTS

SUMMARY AND RECOMMENDATIONS

SUMMARY AND RECOMMENDATIONS

This report outlines projected future trends for the Research Institute for Secure Hardware and Embedded Systems (RISE) and identifies the underlying hardware and embedded systems security research likely to be required over the next five to twelve years to support industry needs. Our previous report was published in 2022.

This update draws on contributions from non-academic industry experts to highlight priority research areas. While the findings represent our best current assessment, they should be viewed as informed predictions rather than certainties.

Role of the RISE Industry and Stakeholder Advisory Board (ISAB)
RISE operates through three main elements:
- Academic research teams
- The **Industry and Stakeholder Advisory Board (ISAB)**
- The institute management team

The ISAB enables member companies and other stakeholders to engage directly with researchers, ensuring that funding calls are informed by real-world challenges.

Key ISAB functions include:
- Identifying results that advance the **state of the art (SOTA)** and could be transitioned into commercial products or services
- Providing pathways to impact (e.g., licensing opportunities, support for spin-out companies)
- Highlighting shifts in technology or market demand with relevance to RISE's mission
- Advising on future RISE research proposal calls
- Helping to develop a national hardware security community
- Supporting the growth of the UK's science, technology, engineering and mathematics (STEM) talent base in digital security and related disciplines

Further information on RISE's work can be found at: https://www.ukrise.org

CONTEXT OF FUTURE TRENDS

Social Context

The broader global and societal drivers for hardware security identified in our previous report remain relevant. These include:
- Geo-political tensions
- The global reach and democratisation of technology
- Increasing complexity of socio-technical systems and networks
- Supply chain vulnerabilities
- Climate change considerations
- Growing demand for energy efficiency

Legislation

Recent legislative and regulatory developments continue to shape hardware security priorities, and these have described below, including:
- The UK Cyber Security and Resilience Bill and NCSC Annual Review 2024
- International cybersecurity standards driving hardware-focused research
- The Cybersecurity Act
- The Network and Information Systems (NIS) Directive
- Emerging artificial intelligence (AI) legislation and governance frameworks

Cyber Security Sectoral and Threat Landscape – 2025

United Kingdom

The UK's 2025 Cyber Security Sectoral Analysis found that 43% of businesses and 30% of charities experienced a cyber breach or attack in the past year — affecting around 612,000 businesses and 61,000 charities. The NCSC identifies the increase from other States and to Commercial and Business, in particular to vulnerabilities which improved hardware security can address.

The UK shows particular strengths in software security capabilities, notably in:
- Application security testing
- Secure development lifecycle practices
- Software vulnerability assessments
- **Development, Security and Operations (DevSecOps)** integration
- Code and **application programming interface (API)** security
- Container security and supply chain security
- The UK's National Semiconductor Strategy (which is a £1 billion, 20-year plan launched in May 2023 to establish the UK as a world leader in future semiconductor technologies).

European Union – ENISA Reports (2024–2025)

The **European Union Agency for Cybersecurity (ENISA)** has identified several significant hardware-related attack trends:
1. Exploitation of edge devices (e.g., FortiGate, Cisco, Ivanti) through firmware tampering and persistent backdoors
2. Targeting of virtualisation platforms and hypervisors as high-value compromise points
3. Compromise of firmware and bootloaders, including malicious router updates
4. Supply chain and build system compromises, targeting maintainers and update processes
5. Use of trusted sites and legitimate tools for stealth persistence
6. Credential and identity attacks, such as brute-forcing hardware administrator accounts
7. Increased state-linked activity from some foreign State Actors targeting networked devices and critical infrastructure

"43% of businesses and 30% of charities experienced a cyber breach or attack in the past year"

Sector impacts include:

- **Digital infrastructure** – 8% of observed events, primarily targeting servers and network equipment
- **Manufacturing** – ransomware and data theft affecting industrial control systems
- **Energy** – exploitation of firmware in critical infrastructure
- **Public administration and transport** – distributed denial-of-service (DDoS) attacks against hardware-dependent services

Key hardware security challenges:

- Patch latency
- Supply chain trust and verification
- Persistence through malicious implants
- Increased exposure of **Internet of Things (IoT)** and edge devices

International – CIS and ETSI Reports

The **Center for Internet Security (CIS**) and the **European Telecommunications Standards Institute (ETSI)** highlight global hardware security developments:

- **Network and endpoint defence** – over 1,142 monitoring sensors deployed; average incident response time under five minutes; 25.1 billion malicious domain name system (DNS) requests blocked
- **Protective DNS** – Malware Domain Blocking and Reporting (MDBR) and MDBR+ services blocking malicious domains, including those accessed by off-network devices
- **Secure hardware configuration** – more than 115 new CIS benchmarks; hardened operating system and cloud images used for over 1.2 billion hours
- **Hardware-adjacent threat intelligence** – 158% increase in reported threats against election infrastructure
- **Incident response and recovery** – 119 incidents resolved in 2024, including cases requiring hardware isolation or replacement

Global Implications for Hardware Security:

- Continuous monitoring and rapid response are now essential for detecting hardware-focused attacks
- Supply chain security which is an increasing requirement from many Governments and Standards Organisations,
- Hardened images and secure configurations form a baseline defence
- Mobile devices are now fully integrated into enterprise security strategies
- Cloud-to-edge security integration is critical for protecting both physical and virtual environments

FUTURE TRENDS

FUTURE TRENDS

The following are our considered opinions and predictions for major trends in hardware and embedded systems security over the coming decade.

1. Post-Quantum Cryptographic Integration

- **Trend:** Migration to p**ost-quantum cryptography (PQC)** for embedded systems, particularly in **Internet of Things (IoT)** and critical infrastructure.
- **Drivers:** Standardisation of PQC algorithms by the **National Institute of Standards and Technology (NIST)**; concerns about "harvest now, decrypt later" attacks. The requirement that devices must have lifetimes of up to 30 years.
- **Research need:** Development of lightweight, low-power PQC implementations suitable for resource-constrained devices.

2. Hardware-Assisted Security Primitives

- **Trend:** Increasing use of hardware-based roots of trust **(RoT)**, **physical unclonable functions (PUFs)**, and **trusted execution environments (TEEs)**.
- **Drivers:** Demand for tamper resistance, secure boot, remote attestation, and secure key storage.
- **Research need:** Scalable, physical and side-channel resilient with hardware and adaptable primitives.

3. Side-Channel and Fault Attack Mitigations

- **Trend:** Ongoing development of defences against power analysis, electromagnetic (EM) attacks, speculative execution, Rowhammer, and fault injection.
- **Drivers:** Availability of low-cost attack tools to the public.
- **Research need:** Low-overhead countermeasures that do not significantly reduce performance or increase energy consumption.

4. Machine Learning and AI Model Protection on Embedded Devices

- **Trend:** Securing AI models deployed on edge devices from inversion, extraction, and poisoning attacks.
- **Drivers:** Growth in AI-enabled embedded systems such as smart cameras and autonomous vehicles.
- **Research need:** Secure model deployment and inference methods for constrained environments.

5. Supply Chain and Lifecycle Security

- **Trend:** Ensuring verifiable provenance and integrity from semiconductor manufacturing through to end-of-life.
- **Drivers:** Risks of counterfeiting, hardware Trojans and malicious intellectual property **(IP)** insertion.
- **Research need:** Component based tracking, digital watermarking, and secure firmware update protocols, with provenance, and automated analysis tools for pre and post silicon design stage.

6. Security for Networked Embedded Systems (IoT, IIoT, CPS)

- **Trend:** Embedded devices increasingly integrated into **industrial Internet of Things (IIoT)** and **cyber-physical systems (CPS)**.
- **Drivers:** Expansion of smart grids, smart homes, and autonomous manufacturing.
- **Research need:** Lightweight, Secure-by-design for edge/deployed devices, and scalable distributed trust protocols.

7. Formal Verification and Hardware–Software Co-Design

- **Trend:** Application of formal verification to prove security properties from **register-transfer level (RTL)** design through to firmware.
- **Drivers:** Vulnerabilities such as Spectre and Meltdown showing the risks at hardware–software boundaries.
- **Research need:** Automated, efficient verification tools spanning the entire system stack. Secure by design and memory safety techniques (such as those provided by CHERI (Capability Hardware Enhanced RISC Instructions)), with a broader focus on compartmentalisation and design patterns for large-scale software across abstraction layers, rather than being confined to hardware–software interfaces alone.

8. Wireless and RF Security for Embedded Systems

- **Trend:** Securing radio frequency **(RF)** communication stacks such as Zigbee, Bluetooth, and ultra-wideband **(UWB).**
- **Drivers:** Increasing threats from RF replay, jamming, and spoofing attacks.
- **Research need:** Physical-layer authentication and low-latency cryptographic techniques. Techniques to support post-quantum cryptography (PQC) requirements to make implementations quantum safe.

9. Fault Tolerant Hardware

- **Trend:** Hardware and embedded systems need to be more fault tolerant.
- **Drivers:** Increasing need of these requirements from, for example, critical infrastructure and the space sector
- **Research need:** Techniques and methods to meet these requirements for fault tolerance and recovery.

10. Education, Skills, and Upskilling (Horizontal Activity)

Skills shortages represent the most urgent barrier to progress. Universities adapt too slowly to industry needs, and reliance on government and market mechanisms risks creating systemic paralysis. RISE should play a leadership role in building new training pipelines through degree programmes, student competitions, and integration into Level 6 and Level 7 qualifications.

Incentives, internships, and sponsorships will be critical for recruitment. This horizontal activity underpins every phase of the roadmap – without a trained workforce, advances in secure hardware and embedded systems cannot be fully realised.

PRIORITIES

PRIORITIES

An overall priority should be the Education, Skills, and Upskilling as a Horizontal Activity.

Phase 1:
Foundation and Immediate Challenges
(2025–2026)

Goals:
- Strengthen existing embedded security foundations
- Prepare for quantum-era and next-generation attack methods

Key focus areas:
1. Side-channel attack mitigation (e.g., differential power analysis, fault and timing attacks)
2. Low-overhead cryptographic primitives for embedded devices
3. Secure firmware update and boot mechanisms
4. Threat modelling and risk assessment for embedded devices

Global activity:
- NIST and European Telecommunications Standards Institute (ETSI) initiatives promoting PQC deployment
- Academic–industry collaborations to standardise secure embedded platforms
- Ongoing disclosures of vulnerabilities in consumer embedded devices (e.g., automotive, medical)

Phase 2:
Post-Quantum and Lifecycle Integration
(2026–2028)

Goals:
- Prepare for transition to PQC algorithms
- Integrate security throughout the device lifecycle

Key focus areas:
1. PQC implementations for embedded systems
2. Secure design and verification tools from RTL to field-programmable gate array (FPGA)/application-specific integrated circuit (ASIC)
3. Hardware–software co-design for security using methods such as CHERI, and defence against speculative execution attacks.
4. Trustworthy supply chain frameworks and anti-counterfeiting measures
5. Secure decommissioning and data sanitisation protocols

Global activity:
- PQC adoption becomes important for critical embedded systems (e.g., defence, finance, energy)
- Stronger partnerships between original equipment manufacturers (OEMs) and suppliers to ensure IP integrity
- Cross-disciplinary initiatives (e.g., electrical engineering, computer science, and legal) to build supply chain trust

Phase 3:
AI and Edge Security Domination
(2028–2030)

Goals:
- Protect AI and machine learning (ML) assets at the edge
- Secure the entire lifecycle of intelligent embedded systems

Key focus areas:
1. Resilience against adversarial attacks in ML models on embedded/edge devices
2. Secure inference and federated learning for embedded AI
3. On-device model watermarking and IP protection
4. Security for autonomous systems (e.g., drones, autonomous vehicles, industrial robots)
5. Energy-efficient security for AI hardware (e.g., neuromorphic chips, edge tensor processing units (TPUs))

Global activity:
- Governments mandate transparency and trust in edge AI devices
- National security concerns drive protections for autonomous vehicles, drones, and IIoT infrastructure
- Industry-wide push towards zero-trust architectures for AI-enabled embedded devices

Phase 4:
Formal Methods and Resilient Architectures (2030–2032)

Goals:
- Achieve mathematically proven hardware security
- Deploy self-healing and self-monitoring embedded systems
- Explainable AI (XAI), that can provide human-understandable explanations for their decisions and outputs, making complex “black box” models more transparent, trustworthy, and reliable

Key focus areas:
1. Formal verification of security properties from transistor level to firmware
2. Runtime monitoring and adaptive security architectures
3. Secure and composable microarchitecture design
4. Autonomous embedded systems with built-in threat detection
5. Global certification frameworks for secure hardware
6. Fault tolerance for hardware and embedded systems.

Global activity:
- Standardised certification schemes across regions (e.g., United States, European Union, Asia)
- Government and academic consortia supporting large-scale formal verification projects
- Critical infrastructure increasingly demands provable trustworthiness in embedded devices

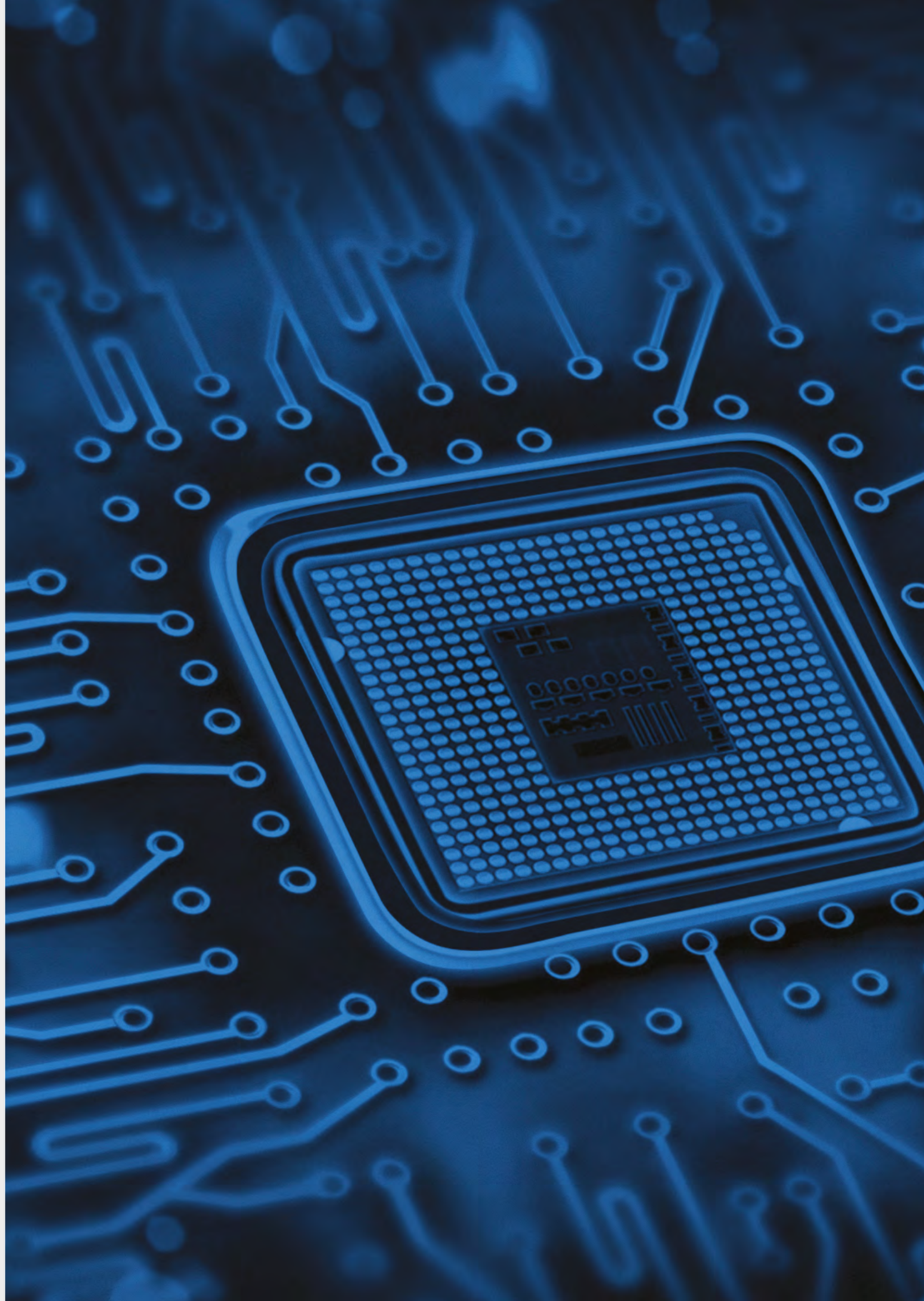
“An overall priority should be the Education, Skills, and Upskilling as a Horizontal Activity”

Cross-Phase Supporting Trends

Education, Skills, and Upskilling are regarded as critical.

Trend	Description
Open-source silicon security	Concerns about insecure third-party IP are driving the demand for verified secure open hardware designs.
Hardware security education	A global push is underway for interdisciplinary curricula combining computer science, electrical engineering, AI, and security.
Digital sovereignty	Nations are investing in domestic secure chip design to reduce foreign dependency.
Quantum threat awareness	Global infrastructure upgrades are accelerating in preparation for the post-quantum era.

“Education, Skills, and Upskilling are regarded as critical”



ACKNOWLEDGEMENTS

Acknowledgement is made to the individual RISE ISAB Board members who helped provide input into this report.

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: info@ukrise.org

ukrise