RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

RISE ANNUAL REPORT

2025–2026

Funded by

in association with National Cyber Security Centre

EPSRC Pioneering research and skills

Hosted by

QUEEN'S UNIVERSITY BELFAST

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES



CONTENTS

FOREWORD 3

INTRODUCTION 4

RISE OBJECTIVES 5

RISE AFFILIATED PROJECTS 6

- TruDetect: Trustworthy Deep-Learning Hardware Trojan Detection 7
- IOTEE: Securing and Analysing Trusted Execution Beyond the CPU 9
- SECCOM: Securing Composable Hardware Platforms 12

RISE ANNUAL CONFERENCE 2025 14

UK-US SEMICONDUCTOR SECURITY SYMPOSIUM 18

- Summary Report on Key Research Challenges 22

NATIONAL SEMICONDUCTOR STRATEGY & COLLABORATIVE RESEARCH 24

- Collaborative Research Seed Funding Call 24

COLLABORATIVE RESEARCH SHOWCASE & SPRING SCHOOL 2026 25

FUTURE RESEARCH TRENDS REPORT 30

RISE IMPACT COMPETITION FUND 31

- Impact Competition 2026 – Call 2 31

RISE-FUNDED WORKSHOPS 32

- ConfAd 2026: The 1st Workshop on Advances in Confidential Computing 33
- Building Supply Chain Confidence in Secure Hardware Systems 33



Professor Máire O’Neill
RISE Director
Queen’s University Belfast

FOREWORD

The past year has been a busy and rewarding one for the Research Institute for Secure Hardware and Embedded Systems (RISE), as we continued to strengthen our role as a national focal point for hardware and embedded systems security.

In September 2025 we held the RISE Annual Conference in London, where our keynote speaker, Prof Daniel Gruss, discussed how greater security can in fact lead to better performance. A real highlight of the day was the Lightning Talk session from early career researchers and academics. It was fantastic to see such a strong pipeline of talented researchers emerging in this field.

In October, with the support of the UK Department for Science, Innovation and Technology (DSIT), we hosted the second UK–US Semiconductor Security Symposium at the Royal Society, London, bringing together leading experts from industry, academia and government. The summary report, which RISE published after the event concluded that semiconductor security is a strategic, systemic and transnational priority. Participants agreed that security must be embedded across the full lifecycle, supported by measurable robustness and trustworthy AI-enabled tools. They also agreed that ecosystem cohesion, including open-source hardware platforms, shared verification practices and common metrics, is needed to build trust and support skills development.

This year’s report outlines the progress made in our three EPSRC-funded affiliated research projects, which have now either finished or are drawing to a close. TruDetect has delivered hardware Trojan detection that needs no golden reference, exposed weaknesses in existing machine-learning detection approaches, and produced explainable detection integrated into an open-source design toolchain. IOTEE has shown that confidential computing can be undermined well beyond the CPU, through memory interfaces, accelerator protocols and previously unknown leakage mechanisms, with findings reported to industry and leading to vendor mitigations. SECCOM, which completed in August 2026, has built open emulation and verification tools for securing composable hardware platforms.

RISE has continued to build international collaborative links. We were delighted to work with DSIT and EPSRC to issue a US–UK and Germany–UK Collaborative Research call for seed funding in semiconductor security. The funded projects attracted early-career academics from a breadth of UK universities, helping to grow our research community. The programme culminated in a Research Showcase in London in March 2026, held alongside the RISE Spring School, attracting a full house at the Royal Academy of Engineering. We had two excellent keynote speakers at the event: Simon Johnson, Intel Fellow and Strategic Lead for Confidential Computing, Intel, US, and Professor Georg Sigl, Technical University of Munich and Director of Fraunhofer AISEC, Germany.

I would like to thank Charles Brookson, independent Chair of the RISE Industrial and Stakeholder Advisory Board (ISAB), for his work with industry partners on the 2025 Future Trends report. It outlines the hardware and embedded systems security research likely to be needed over the next five to twelve years to support industry needs. Further details can be found in this report and on the RISE webpage.

We were also pleased to launch our second Impact Competition to accelerate the translation of research in secure hardware and embedded systems, and we look forward to seeing the practical tools and technologies that emerge from the three funded projects. For the first time this year we also offered funding for academics in the RISE community to host workshops and events in emerging areas of hardware security research. We were delighted to support two workshops, at the Universities of Oxford and Southampton, and look forward to funding further events over the coming year.

Hardware is the foundation of every digital system we rely on, from critical national infrastructure, healthcare and communications to transport and artificial intelligence. Vulnerabilities at this level are difficult to detect, costly to fix once devices are deployed, and can undermine every layer of protection built on top. As supply chains grow more complex, AI workloads move onto shared and heterogeneous hardware, and the threat landscape evolves, security must be designed in from the outset rather than added later. This is why sustained investment in research, skills and international collaboration in this area matters, for national resilience as well as for economic competitiveness and trust in future technologies.

Professor Máire O’Neill
RISE Director
Queen’s University Belfast

INTRODUCTION

The Research Institute for Secure Hardware and Embedded Systems (RISE: www.ukrise.org) is hosted at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast and has been funded since 2017 by the National Cyber Security Centre (NCSC), with the support of the Engineering and Physical Sciences Research Council (EPSRC). RISE is one of four cyber security institutes in the UK and aims to be a global hub for research and innovation in hardware and embedded systems security.



RISE OBJECTIVES

- Conduct and support **research in hardware and embedded systems** that addresses security throughout a device's lifecycle, from the initial design and manufacture through to its operational environment.
- Grow the UK hardware and embedded systems community by bringing academia and industry together and **facilitating networking opportunities**.
- Grow the UK's **skills** in hardware and embedded systems security.
- Support **development and pull-through** of hardware and embedded systems technologies.
- Build a strong network of national and international research and innovation **collaborative partnerships**.
- Support **policy issues** and **standards activity** relevant to RISE.



RISE AFFILIATED PROJECTS – UPDATES

TRUDETECT: TRUSTWORTHY DEEP-LEARNING HARDWARE TROJAN DETECTION

Prof Máire O'Neill
Dr Ihsen Alouani
Dr Niall McLaughlin

QUEEN'S UNIVERSITY BELFAST

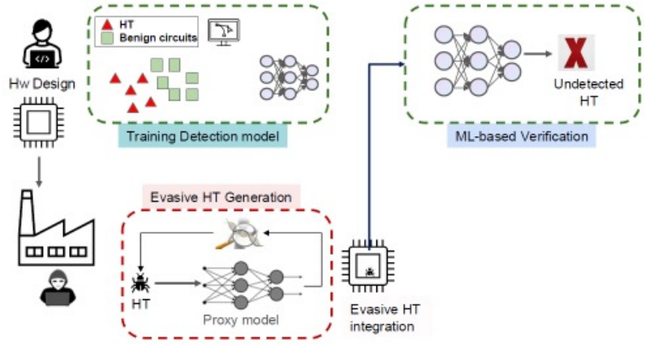
The TruDetect project aims to deliver a trustworthy deep learning–based system for detecting hardware Trojans (HTs) in digital circuits, capable of integration into electronic design automation (EDA) toolflows. Progress to date spans three core technical work packages, with significant advances in detection capability, robustness analysis and explainability.

Advanced Deep Learning–Based Trojan Detection

A scalable, golden-reference-free hardware Trojan detection framework has been developed for gate-level netlists through a Trojan-agnostic, unsupervised one-class classification approach, named TAGDet. Unlike supervised methods that require examples of Trojan-infected circuitry during training, TAGDet is trained exclusively on benign nodes, allowing previously unseen Trojan behaviour to be identified as anomalous. The pipeline converts gate-level netlists into directed graphs, extracts structural, graph-centrality and gate-level features, and applies principal component analysis to reduce dimensionality before node-level classification using Autoencoder and One-Class SVM models. A graph-aware post-prediction refinement stage uses neighbourhood information to suppress isolated false positives and improve localisation of suspicious components. Evaluation on Trust-Hub benchmarks (https://trust-hub.org/), achieves strong detection performance and scalability, demonstrating a practical detection approach where labelled Trojan examples are scarce or unavailable.

Trustworthiness and Adversarial Robustness

The project has also involved a systematic study of adversarially evasive hardware Trojans, introducing a ***novel black box gate approximation attack*** that can evade existing ML–based detection approaches while preserving circuit functionality. Extensive evaluation across multiple benchmarks and detection models shows that even state of the art techniques are vulnerable to such evasive attacks, highlighting a critical gap in current defences. The work establishes a rigorous threat model and provides a foundation for strengthening HT detection via adversarial training. This research has been published at AsianHOST 2025.



Overview of the Approximate Black Box Attack

A complementary strand of work strengthens trustworthiness by making the detector self-interpretable rather than relying on explanations generated only after classification. The proposed gate-level GNN routes each prediction through a compact, saliency-selected subgraph and jointly trains classification and explanation using sufficiency and necessity constraints: the selected circuitry should preserve the verdict, while removing it should alter the prediction. On TrustHUB benchmarks under circuit-family-disjoint evaluation, the framework reports average true-positive and true-negative rates of 97% and 96%, respectively, with near-zero average sufficiency error for most circuits. Integrated Gradients then converts model attributions into structural rules that identify both where suspicious logic occurs and why it merits inspection, providing actionable evidence for human-in-the-loop verification while also exposing limitations for unusually distributed trigger structures. This research work was published at VLSI-SoC 2026.

Explainable and Interpretable HT Detection

Significant progress has been made towards improving the transparency and trustworthiness of GNN-based hardware Trojan detection. Analysis of leading GNN-based detection approaches revealed that existing models can rely predominantly on node-level features, such as gate properties, rather than fully exploiting circuit topology. To address this limitation, TruDetect has developed MaskLearner, a self-supervised framework that uses learned node masking to encourage greater structural awareness while identifying Trojan-critical regions without requiring explicit node-level supervision. By combining classification with consistency and sparsity objectives, MaskLearner learns compact node-importance maps that highlight the circuit regions most influential to detection decisions. Experimental evaluation across Trust-Hub, ISCAS and OpenCore benchmarks demonstrates improved structural awareness and Trojan localisation while maintaining strong detection performance, providing more interpretable evidence to support analysis of potentially malicious circuit modifications.

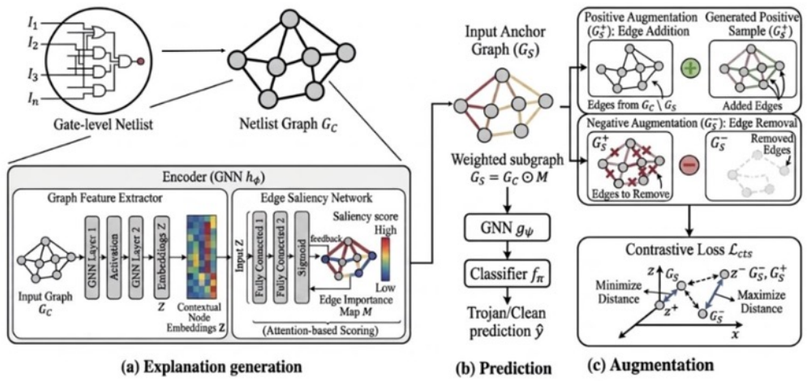
Next Steps

The final phase of the project integrates the outputs of the work completed to date into a unified, trustworthy detection design with the goal of embedding TruDetect capabilities within EDA toolflows. A demonstrator illustrating the outputs integrated into the OpenRoad open-source digital design toolchain has been developed. This will help enable practical adoption of robust, explainable HT detection in real world semiconductor design and verification processes.

Publications

Publications to date include the following papers, with a further two papers currently under review:

- M. Dhiaf, H. Bouzidi, and I. Alouani, “Adversarially evasive hardware trojans through approximate designs,” in *Proc. 2025 Asian Hardware Oriented Security and Trust Symp. (AsianHOST)*, Nanjing, China, Dec. 2025.
- M. Dhiaf and I. Alouani, “Self-interpretable hardware Trojan detection on gate-level netlists with sufficient and necessary GNN explanations,” in *Proc. IFIP/IEEE 34th Int. Conf. Very Large Scale Integration (VLSI-SoC)*, Limassol, Cyprus, Oct. 2026.



Overview of Proposed Self-Interpretable Hardware Trojan Detection Framework

IOTEE: SECURING AND ANALYSING TRUSTED EXECUTION BEYOND THE CPU

Prof David Oswald

Durham University

Prof Mark Ryan

UNIVERSITY OF BIRMINGHAM

Dr Ahmad Atamli
Prof Vladi Sassone

University of Southampton

The IOTEE project addresses the security of confidential computing and Trusted Execution Environments (TEEs) across the modern heterogeneous hardware stack, spanning CPUs, GPUs, NICs, external memory interfaces, and cross-accelerator communication protocols. This report combines the work carried out at Durham University and at the University of Southampton, together with related work previously undertaken at the University of Birmingham.

Cross-Accelerator Protocol Security (SPDM)

Confidential computing is moving beyond the CPU towards heterogeneous CPU–GPU and accelerator systems. In such environments, the Security Protocol and Data Model (SPDM) is a core protocol for establishing trust, authenticating components, and supporting secure communication between devices. Because production-grade SPDM implementations remain scarce and are only expected to become widely available over the next few years, the project consortium carried out a theoretical analysis of the protocol-level fault-injection (FI) attack surface of SPDM rather than an attack on a specific deployed stack. The work systematically analysed how fault injection could affect security-critical SPDM operations and demonstrated how faults introduced at selected stages of the protocol could undermine expected security guarantees. The study also considered potential countermeasures for improving the resilience of SPDM implementations against such attacks. The Durham team’s broader view in this area is also captured in a survey of confidential computing on heterogeneous CPU–GPU systems.

- P. Sun, Q. Wang, D. Oswald, M. Dermot, V. Sassone, A. Atamli. *FaultSpy: On the Insecurity of SPDM Protocols under Fault Injection*. IEEE TrustCom 2025. https://doi.org/10.1109/Trustcom66490.2025.00252 — repository record: https://durham-repository.worktribe.com/output/4830928
- Q. Wang, D. Oswald. *Confidential Computing on Heterogeneous CPU–GPU Systems: Survey and Future Directions.* ACM Computing Surveys, 58(9), Article 230, 2026. https://doi.org/10.1145/3793532

Formal Analysis of PCIE Security Mechanisms

A major project theme at Southampton has focused on the formal analysis of PCIe mechanisms relevant to confidential computing, particularly TDISP, IDE, and ATS. These mechanisms are increasingly important for confidential computing systems in which accelerators and other PCIe devices must interact securely with protected workloads and memory. TLA+ has been used to construct formal models of the relevant protocols, including their state transitions, security-sensitive behaviours, and interactions. The models capture key aspects such as device assignment, secure communication, memory access, configuration changes, and protocol state management. The formal analysis has identified multiple potential vulnerabilities and protocol weaknesses in TDISP and related PCIe security mechanisms. These findings have been reported to Intel and NVIDIA for further discussion and validation. The team is currently working on a research paper presenting these findings and the corresponding TLA+-based formal analysis.

The next stage of this work will focus on incorporating industrial feedback, further validating the identified weaknesses, and preparing and submitting a research paper based on the formal analysis of TDISP, IDE, and ATS.

Security of ML Workloads in Confidential Computing

A confidential computing platform is only as trustworthy as the workloads it protects, and ML inference is now a major confidential-computing workload. The project has shown that the ML models themselves, not just the surrounding infrastructure, can be attacked through both fault injection and side channels. For fault injection, *BarkBeetle* demonstrates that fault injection can be used to extract the internal structure of decision-tree models. For the side-channel attacks, two results show that TEE-protected ML inference leaks: *Activation Functions Considered Harmful* recovers neural-network weights and biases from within an SGX enclave, while *TrEEStealer* extracts decision trees via enclave side channels. Together, these results establish that model confidentiality inside TEEs cannot be assumed and motivate defences.

- Q. Wang, J. Sander, M. Jiang, T. Eisenbarth, D. Oswald. BarkBeetle: Stealing Decision Tree Models with Fault Injection. ACM ASIA CCS 2026, pp. 343–357. https://doi.org/10.1145/3779208.3785372
- J. Spielman, D. Oswald, M. Ryan, J. Van Bulck. Activation Functions Considered Harmful: Recovering Neural Network Weights through Controlled Channels. RAID 2025. https://doi.org/10.1109/RAID67961.2025.00062
- J. Sander, A. Rabich, N. Mahling, F. Maurer, J. Heller, Q. Wang, T. Eisenbarth, D. Oswald. TrEEStealer: Stealing Decision Trees via Enclave Side Channels. Preprint, 2026. https://arxiv.org/abs/2604.18716

External Interface Security: Breaking Confidential Computing via Memory

A major project theme is that confidential computing can be broken by attacking components beyond the CPU even where the CPU-internal protections are sound. This line of work builds on *BadRAM*, which showed that reprogramming memory configuration data defeats memory-integrity protections in TEEs. This foundation has been extended along several dimensions: *Battering RAM* develops a low-cost DDR4 interposer that introduces aliases dynamically at runtime, bypassing Intel's and AMD's boot-time alias-checking mitigations. It achieves the first breach of Intel Scalable SGX's single-key encryption domain and re-enables a full attestation breach on up-to-date AMD SEV-SNP.

The IOTEE project has also demonstrated the breadth of the memory attack surface across operating systems, architectures, and memory generations:

Download More RAM shows, for the first time, that memory aliasing can be induced purely from software, breaking Windows Virtualisation-Based Security. Microsoft assigned CVE-2026-23670 and issued a mitigation through Windows Update.

DisARMed extends memory aliasing to ARM systems, demonstrating the first end-to-end aliasing attack that escalates from unprivileged userspace to compromise both the Linux kernel and ARM TrustZone, together with a low-overhead boot-time detection mitigation. Finally, the Battering RAM interposer work has been extended to DDR5, with a paper to appear at ACM CCS 2026.

- J. De Meulemeester, D. Oswald, I. Verbauwhede, J. Van Bulck. Battering RAM: Low-Cost Interposer Attacks on Confidential Computing via Dynamic Memory Aliasing. IEEE S&P 2026. https://doi.org/10.1109/SP63933.2026.00052 — https://batteringram.eu/
- J. De Meulemeester, L. Wilke, D. Oswald, T. Eisenbarth, I. Verbauwhede, J. Van Bulck. BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments. IEEE S&P 2025. https://doi.org/10.1109/sp61157.2025.00104
- S. Collins, T. Chothia, W. Burgess, M. Muench, D. Oswald. Download More RAM: Dismantling Windows Operating System Defences with Mischievous Memory. USENIX Security 2026. https://www.usenix.org/conference/usenixsecurity26/presentation/collins (CVE-2026-23670)
- J. Henes, M. Bowden, M. Ordean, D. Oswald. DisARMed: Attacking ARM TrustZone from Userspace with Memory Aliasing. USENIX WOOT 2026. https://www.usenix.org/conference/woot26/presentation/henes

Novel Physical Leakage Mechanisms

Beyond memory-interface attacks, the project has identified a previously undocumented leakage mode relevant to embedded and confidential-computing platforms. *Racing against the clock* shows that memory and peripherals operating in a different (asynchronous) clock domain to a target processor can act as an indirect, data-dependent proxy for power consumption. This enables power-style side-channel attacks to be mounted purely from software, using only a cycle counter

- M. Thompson, D. Oswald. Racing against the clock: side-channel leakage from crossing asynchronous clock domains. IACR TCHES 2026(2), 28–50. https://doi.org/10.46586/tches.v2026.i2.28-50

Summary and Next Steps

Across 2025–2026, IOTEE has established that confidential computing faces threats at every layer beyond the CPU core: at the cross-accelerator protocol layer, at the workload layer, at the external memory interface, and through new physical leakage mechanisms. The consistent finding is that current TEE and confidential-computing designs place implicit trust in components — DRAM, clock domains, cross-accelerator protocols, and workload implementations — which a realistic adversary can subvert.

The SPDM work demonstrated how fault injection can undermine security-critical protocol operations and resulted in the publication of *FaultSpy: On the Insecurity of SPDM Protocols under Fault Injection* at IEEE TrustCom 2025. In parallel, the Southampton team developed TLA+ models of TDISP, IDE, and ATS and used them to systematically analyse their security properties and interactions, leading to the identification of multiple potential vulnerabilities and protocol weaknesses that have been reported to Intel and NVIDIA.

The next phase will consider low-level firmware attack surface, GPU architecture, as well as strong protections for heterogeneous confidential computing with a focus on AI applications. It will also focus on validating the PCIe findings with industry partners and completing and submitting the associated research paper. Looking ahead, the project will also explore AI-assisted security verification, including the use of AI to support vulnerability discovery, formal modelling, security-property generation, and automated analysis of complex hardware–software systems.

SECCOM: SECURING COMPOSABLE HARDWARE PLATFORMS

Prof John Goodacre
Dr Bernardo Magri
Prof Lucas Cordeiro

The University of Manchester

The SECCOM project set out to investigate the security exposure of composable hardware platforms, in which memory and accelerator resources are attached to, detached from and shared between hosts at runtime. Taking the Compute eXpress Link (CXL) interconnect as its primary vehicle, the project built a representative QEMU/Linux platform, developed the attack and security models needed to reason about a zero-trust composable system, and delivered a verification framework that turns security properties into checkable obligations discharged against the real software managing the platform. The project completed in August 2026.

A Composable Platform for Security Research

Composability in CXL comes from switching and fabric management layered on the base protocols, and this is precisely where open tooling was thinnest. SECCOM found that switching, dynamic capacity and multi-host sharing were unimplemented or only nominally supported in QEMU and the Linux kernel, with no working open-source Fabric Manager available at all. Building the emulation platform therefore became a substantial engineering contribution in its own right.

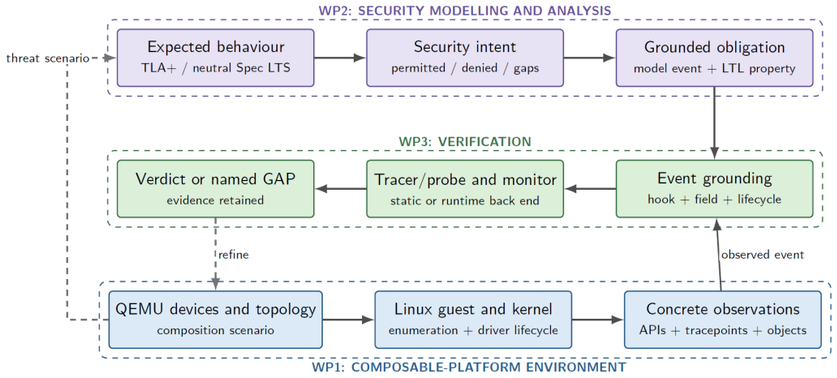
The project developed the **cxl-vcs-switch** object for QEMU, providing Virtual CXL Switch support and the FM-API commands for switch enumeration and vPPB bind/unbind, released as an RFC patchset to the linux-cxl mailing list with upstream acceptance in mind. This was extended to multi-guest operation, allowing one QEMU instance to act as a Fabric Manager and compose the CXL topologies of separate compute nodes at runtime over shared memory backends. Alongside this, SECCOM contributed four fixes for CXL hotplug defects in QEMU, two upstreamed fixes to Samsung's **libcxlmi** management library, and the **uom-cxl-tools** repository, which gives a complete reproducible multi-guest CXL development and emulation environment. The work was presented to the community at the UK RISE 2025 Conference.

A boot-time attack using malicious PCI Option ROMs was demonstrated on the emulated platform, with arbitrary code executing in the pre-OS environment. Analysis of the Linux and firmware paths established that this class of attack cannot reach runtime composability, since Option ROMs are consumed only as passive data once the kernel has control — a negative result that redirected the project's attention to the composability mechanisms themselves.

Modelling Attacks and Subversion-Resilient Security

SECCOM developed an attack model and a security model for composable hardware systems, identifying adversarial parties, goals and capabilities, and mapping security objectives onto the mechanisms required to defend them against each capability class.

Two case studies instantiate the models. The first shows that supply-chain-subverted device firmware can establish covert communication through the random-looking values in authentication and key-establishment transcripts, and that this channel survives a monitor performing perfect system-level safety verification, holding all parties' secret keys and possessing quantum computational capability. The second answers it with the first post-quantum reverse firewall in the literature: a trusted sanitising interface re-randomises the key-establishment transcript so that a subverted implementation cannot use it as a subliminal leakage channel, instantiated in an X3DH-style setting with unique signatures closing the authentication path. Both studies have been submitted to leading cryptography conferences.



From Specification to Verified Runtime Enforcement

The verification work turned these properties into obligations discharged against the real software managing composable PCIe/CXL platforms. ESBMC was extended to parse unmodified Linux 7.1.5 kernel driver source, with the kernel-C frontend fixes and an overflow-check correction contributed upstream to the ESBMC project. A CXL verification suite of 98 tests over an operational driver model, together with harnesses verifying four functions of the real **drivers/cxl/core/pci.c**, exercised the defect classes the threat model targets.

The emphasis then moved to runtime verification against the running system, using the Linux kernel's Runtime Verification subsystem with eBPF probes supplying events for driver paths that carry no tracepoint. In the flagship case study, a CXL mailbox doorbell property was carried into a live instrumented kernel: the correct driver produced four clean transitions, while a driver with the doorbell wait removed was caught on its second command with the RV reactor firing, a fault invisible to the userspace caller and to any test checking return codes. A PCIe multi-function-device class-exclusion property demonstrated the same chain on the eBPF route, detecting a keyboard-class function injected into a device already presenting a network interface.

A late result unified the two halves of this work. Because a runtime monitor's obligation is a safety property, a single automaton can drive an unbounded consistency check, a bounded check over driver code, and the running kernel; across four CXL automata all 67 transition pairs agreed across all three back ends. A separate strand produced the first contract-based regression-verification tool, using LLM-inferred partial contracts that are certified by the verifier and never trusted on their own, and which never certified a non-equivalent program pair as equivalent across the 272 pairs of the EqBench-C benchmark.

Assurance Boundaries and Legacy

A recurring finding is that automatically generated verification artefacts must be validated against the real system before they can be trusted. Generated kernel attach points proved to be unverified suggestions: of 25 tracepoint names proposed by an early cross-specification model, none attached to the evaluated kernel. SECCOM's response was to make evidence gaps explicit — where an obligation cannot be observed, the framework records a named observability, runtime or attestation gap and declines to interpret missing evidence as compliance. This discipline matters most in exactly the setting CXL creates, where device identity is unattested, fabric-manager operations may never traverse the host's driver stack, and the specification's own confidential-computing mechanism is currently out of scope for the switching and sharing features that make a system composable.

The project's results have been submitted to VLSID 2026, DVCon Europe 2026 and ASP-DAC 2027, with further submissions to ICSE and FMCAD, and an integrated account, *INVAR: Intent Verification from Natural-Language Specifications to Grounded Kernel Enforcement,* submitted to ACM Transactions on Embedded Computing Systems.

Follow-on work is to automate the concretisation and probe-generation step that currently stands between a specification and a running monitor, to validate device identity using attested evidence, to measure monitor overhead against a userspace baseline, and to extend the observation model so that fabric-manager actions are authenticated and visible across hosts. The open QEMU, kernel and tooling artefacts produced by SECCOM are the precondition for that work being possible outside the small number of hyperscale operators currently able to build CXL fabric-management stacks in-house.

RISE ANNUAL CONFERENCE 2025



Prince Philip House, Royal Academy of Engineering – venue for the RISE 2025 Annual Conference

The 2025 RISE annual conference was held at Prince Philip House, the Royal Academy of Engineering, London on 11th September 2025.

The one-day programme opened with a keynote from Prof. Daniel Gruss of Graz University of Technology, followed by updates from the RISE affiliated projects. Lunch provided an opportunity for networking, alongside a poster session giving PhD students and early career researchers the opportunity to showcase their work.

After lunch, Prof. John Goodacre, Challenge Director, Digital Security by Design, UKRI, gave an update on government security and resilience activities. This was followed by a series of 10 short lightning talks giving early-career researchers the opportunity to highlight their work and share recent results. Louise Cushnahan, Head of Innovation at RISE, introduced the Impact Competition projects, who each provided an update on their work.

The day concluded with a RISE Industrial and Stakeholder Advisory Board (ISAB) meeting, chaired by Charles Brookson OBE, where the board reviewed a draft of the ISAB Future Research Trends report and provided feedback on the project updates presented earlier in the day.

A summary of the agenda and contributors is as follows.

Rise Annual Conference, 11th September 2025, Prince Philip House, London	
09:00 – 10:00	**Registration & Tea/Coffee/Refreshments**
10:00 – 10:10	**Opening Remarks & Welcome** Prof Máire O'Neill
10:10 – 11:10	**Keynote: Breaking Confidentiality and Integrity Through the Microarchitecture and Finding Free Lunch Down There** Prof Daniel Gruss, Graz University of Technology
11:10 – 11:30	**Break**
	RISE Project Updates
11:30 – 11:45	BlueGuard: Accelerated Host and Guest Introspection Using DPUs Dr Ahmad Atamli, University of Southampton
11:45 – 12:00	SECCOM: CXL and QEMU – setup for research on composable systems Dr Joshua Lant, University of Manchester
12:00 – 12:15	BadRAM: Breaching Processor Security via Rogue Memory Modules Prof David Oswald, University of Birmingham
12:15 – 12:30	TruDetect: Trustworthy Deep-Learning based Hardware Trojan Detection Dr Ihsen Alouani, Dr Niall McLaughlin, Queen's University Belfast
12:30 – 13:30	**Lunch & Networking (Poster Session)**
13:30 – 13:45	Update on Government Security and Resilience Activities Prof John Goodacre, Challenge Director, DSbD, UKRI
13:45 – 14:40	**Early Career Academic & Researcher Lightning Talks (5 min each)** Audio-based shared secret generation method – Vinod Khandkar, University of Surrey Cheri-Cap-Lib – A hardware library for CHERI capability implementations – Jon Woodruff, University of Cambridge Chosen-ciphertext Attack on SCA-resistant Lattice-based PQC Implementation and Protection – Anh Tuan Hoang, Queen's University Belfast Transient-execution attacks in CHERI and how to mitigate them – Franz Fuchs, University of Cambridge Side-Channel Leakage Assessment in the Pre-Silicon World – Yusuf Hegazy, University of Birmingham Spectre Hunting with Extended Formal Specifications – Daniel Wright, University of Surrey E2EdgeGenAI: Energy-Efficient Edge Generative AI for Secure Embedded Robotics and Hardware – Tinoosh Mohsenin, Johns Hopkins University Securing UAV Vision: Hardware Threats and the Defensive Road Ahead – Selma Dilek, University of Bristol Fault Injection in SPDM – Peiyao Sun, University of Southampton Understanding threat actors as users – how much can we anticipate? – Andrew Peck, Loughborough University
14:40 – 14:55	**Break**
	RISE Impact Competition Projects
14:55 – 15:00	Impact Competition Introduction Louise Cushnahan, Head of Innovation at RISE
15:00 – 15:15	SHIELD: A New Layer of Defense with Intelligent Hardware Monitoring for Safer Embedded Systems Dr Sangeet Saha, University of Essex
15:15 – 15:30	PaRtial Execution oF EncRypted dAta using reconfiguraBle hardware (PREFERABLE) Prof Gareth Howells, University of Essex
15:30 – 15:45	Combating fake media with edit-tolerant authentication Daniel Fentham, Prof David Oswald, Prof Mark Ryan, Dr Xiao Yang, University of Birmingham
15:45 – 16:00	**Closing Remarks**
16:00 – 17:00	**RISE ISAB Meeting (closed session)**



Prof. Daniel Gruss, Graz University of Technology, Austria



Best Lightning Talk Winner: Daniel Wright, University of Surrey



Prof. John Goodacre, Challenge Director, DSbD, UKRI



Dr Ihsen Alouani, Queen's University Belfast



Dr Selma Dilek, University of Bristol



Prof. Gareth Howells, University of Essex

UK–US SEMICONDUCTOR SECURITY SYMPOSIUM

The 2025 UK–US Semiconductor Security Symposium was held at the Royal Society, London on 8th–9th October 2025. Supported by the UK Department for Science, Innovation and Technology (DSIT), the symposium brought together leading UK and US experts from industry, government and academia to explore the challenges and opportunities in semiconductor security, and to identify priority research challenges that lay the groundwork for collaborative research between UK and US organisations.

The symposium was co-chaired by **Prof. Máire O'Neill FREng**, Director of RISE, Queen's University Belfast, and **Prof. Mark Tehranipoor**, Chair of the Department of Electrical and Computer Engineering, University of Florida.

It was the second in a series of collaborative UK–US semiconductor security events. The first, a workshop on Security in the Era of Global Semiconductor Initiatives, took place in Washington DC in November 2023 and culminated in a RISE report published in July 2024 setting out a strategic overview of the challenges and emerging opportunities in semiconductor security.

The two-day programme included an update from Richard Duffy, Head of Innovation Policy, Semiconductors at DSIT, on implementation of the UK National Semiconductor Strategy, alongside industry talks from Marvell, Thales e-Security, Cisco, Codasip, Ericsson, Intel, Qualcomm and Graf Research, and contributions from NCSC and UKRI. Two emerging research sessions featured short talks from leading UK and US universities, and a panel chaired by Sarah Munro (DSIT) discussed industry, academic and government perspectives on building a semiconductor security workforce.

Round-table breakout sessions explored four themes in depth, with the aim of moving forward with recommendations:

- Secure-by-Design Hardware Foundations
- AI-Enabled Security Design and Verification
- Supply Chain Integrity and Hardware Vulnerability Intelligence
- Open-Source Security IP and Ecosystem Cohesion



Panel discussion on Semiconductor Security Skills, chaired by Sarah Munro, DSIT.



Prof. Waleed Khalil, Ohio State University



Sid Allman, Marvell Technologies



Richard Duffy, DSIT



Dr. Patrik Ekdahl, Ericsson



Prof. David Oswald, Durham University



Prof. Farimah Farahmandi, University of Florida



Carl Shaw, Codasip



Dr. Alieeldin Mady, Qualcomm

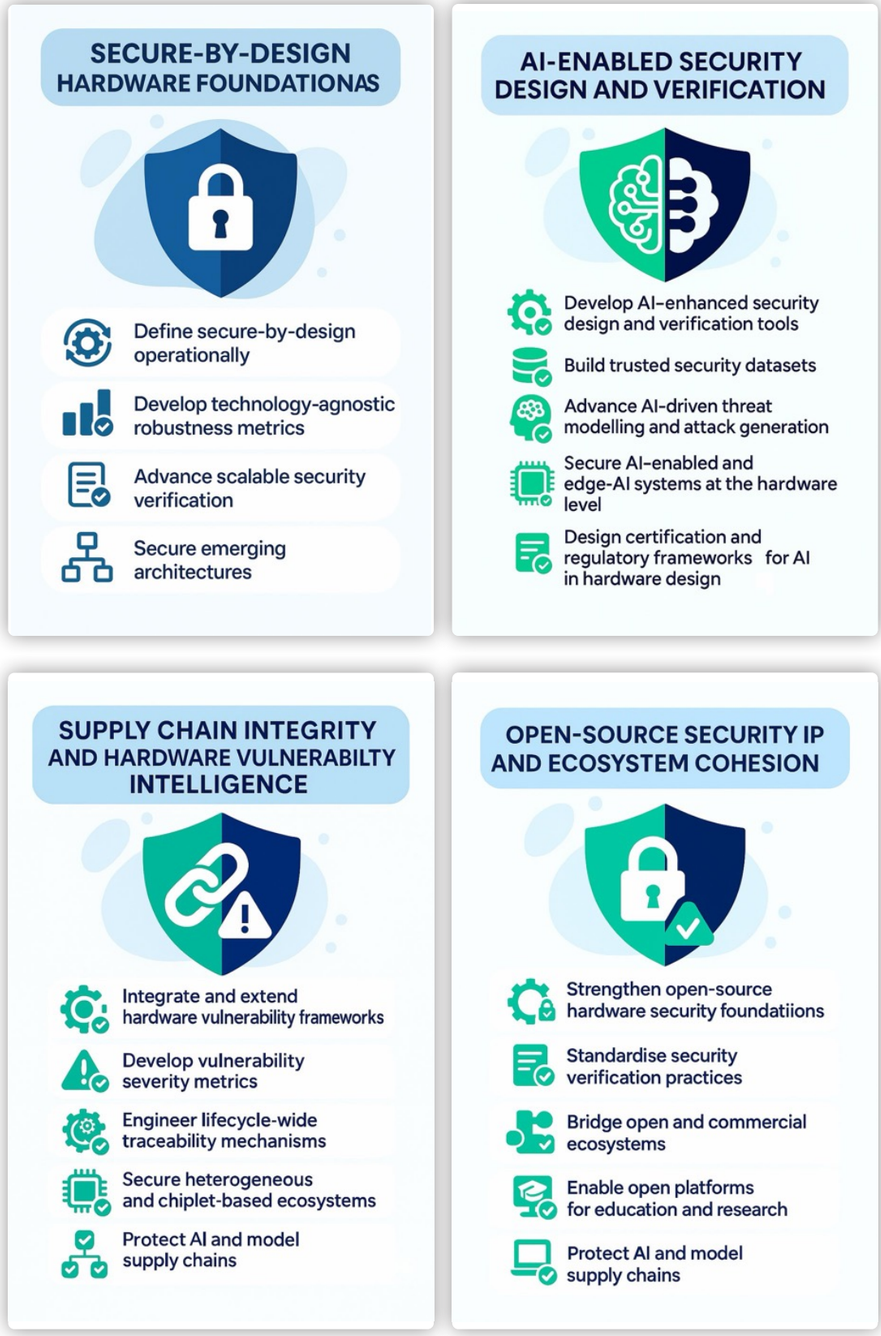
SUMMARY REPORT ON KEY RESEARCH CHALLENGES

Following the symposium, RISE published a summary report capturing the discussions and the key research challenges identified under each theme. Participants agreed that semiconductor security is now a strategic, systemic and transnational priority that must be embedded across the full lifecycle, supported by measurable robustness, trustworthy AI-enabled tools and coherent ecosystem governance.

A key insight was that the challenges are not solely technical: progress must be matched by stronger incentives, standards, procurement practices and regulatory alignment, with security treated as a first-order design parameter. The report also provided a structured agenda for long-term UK–US collaboration.

The full report is available on the RISE website:





Key research challenges identified for each of the four symposium themes

NATIONAL SEMICONDUCTOR STRATEGY & COLLABORATIVE RESEARCH

One of the three pillars of the UK's National Semiconductor Strategy, published in May 2023, focuses on ensuring that the importance of hardware for cyber security is considered, and more widely prioritised, at the design stage of chips. RISE has continued to support DSIT's Semiconductor Security Team in the delivery of this security pillar with collaborative discussions with the US and Germany.

COLLABORATIVE RESEARCH SEED FUNDING CALL

These discussions resulted in RISE partnering with DSIT and EPSRC to issue a US–UK and Germany–UK Collaborative Research call for seed funding in Semiconductor Security, which opened on 3 July 2025 and closed on 31 July 2025.

Applicants could request up to £100k for short-term visits or short-term projects, to be completed by 31 March 2026. Proposals were required to address the RISE technical research challenges. Applications from early career researchers were encouraged, and post-doctoral researchers were eligible to apply as a researcher co-lead with a suitable project lead as mentor. The funding aimed to support:

- short-term visits (up to 3 months) to the US or Germany to foster collaborative linkages or facilitate knowledge exchange, or
- short-term projects that advance research in semiconductor security.

RISE promoted the call to the wider RISE community through social media and mailing lists.



Collateral promoting the EPSRC collaborative research call in semiconductor security

The resulting projects – 11 UK–US and 8 UK–Germany collaborations – involved UK partners including the Universities of Sheffield, Liverpool, Oxford, Southampton, Swansea, Cardiff, Bristol, Essex and Loughborough, Queen's University Belfast, Imperial College London and Digital Catapult. The projects were showcased at the 2026 RISE Collaborative Research Showcase & Spring School.

COLLABORATIVE RESEARCH SHOWCASE & SPRING SCHOOL 2026



The 2026 RISE Collaborative Research Showcase & Spring School was held at Prince Philip House, the Royal Academy of Engineering, London on 5th–6th March 2026, supported by the UK Department for Science, Innovation and Technology (DSIT).

The event showcased the EPSRC UK–US and UK–Germany Collaborative Research Projects in Semiconductor Security, with project teams presenting their work alongside their international partners across five themed sessions:

- Hardware Security Vulnerabilities & Mitigations
- Hardware Security Primitives & Physical Unclonable Functions (PUFs)
- Hardware-Rooted Security in RF, Photonic and Semiconductor Systems
- AI & Hardware Security
- RISE Impact Competition Winners

The programme was chaired by Prof. Máire O'Neill and featured two keynote speakers:

- **Simon Johnson**, Intel Fellow and Strategic Lead for Confidential Computing within Intel's Office of the CTO, US
- **Prof. Dr.-Ing. Georg Sigl**, Technical University of Munich and Director of the Fraunhofer Research Institute for Applied and Integrated Security (AISEC), Germany – Design and Validation of RISC-V based Secure Microcontroller Chips

The event also included a presentation from the National Cyber Security Centre (NCSC), demo and poster sessions, a drinks reception and buffet at The Admiralty, Trafalgar Square, and an update on RISE activities and future opportunities. A limited number of bursaries were available to UK-based PhD students and post-doctoral researchers to cover travel and accommodation.

A summary of the agenda for day 1 and contributors is as follows.

Day 1 – Thursday 5th March 2026	
09:00 – 10:00	**Registration – Tea / Coffee / Refreshments**
10:00 – 10:15	**Opening Remarks / Welcome** Prof Máire O'Neill, RISE Director
10:15 – 11:00	**Keynote** Simon Johnson, Intel Fellow & Confidential Compute Technical Director
	Session 1: Hardware Security Vulnerabilities & Mitigations Chair: Dr Patrik Ekdahl, Ericsson
11:00 – 11:20	Foundations of Configurable Hardware Tracing for Monitoring Safety-Critical Systems Dr Martin Berger, University of Sussex; Prof Martin Leucker, University of Lübeck; Dr Alexander Weiss, Accemic
11:20 – 11:50	**Break & Networking**
11:50 – 12:10	Secure Start and Execution with Electronics Having Hardware Security Vulnerabilities Dr Amit Kumar Singh, University of Essex; Prof Prabhat Mishra, University of Florida
12:10 – 12:30	Side-Channel Analysis (SCA) and Countermeasure Implementation of Post-Quantum HQC on FPGA and ASIC Dr Anh Tuan Hoang, Queen's University Belfast; Prof Samuel Pagliarini, Carnegie Mellon University
	Session 2: Hardware Security Primitives & PUFs Chair: Dr Chongyan Gu, CSIT, Queen's University Belfast
12:30 – 12:50	Secure-by-Design Photonic Identification Using Inhomogeneously Broadened Quantum Dot PUFs (QD-PUFs) Dr Craig Allford, Cardiff University (with Prof Peter Smowton, Cardiff University; Prof John Bowers, UC Santa Barbara)
12:50 – 13:10	NeuroSecure – Building Trustworthy PUFs for Neuromorphic Chips Dr Xiaoyao Song, Prof Merlyne De Souza, University of Sheffield; Dr Stefan Wiefels, Forschungszentrum Jülich
13:10 – 14:20	**Lunch, Poster Session & Networking**
14:20 – 14:40	Hardware Root of Trust Reconsidered – A Distributed Security Architecture to Protect Vulnerable Devices in the Semiconductor Supply Chain Dr Prosanta Gope, University of Sheffield; Dr Owen Millwood & Dr Witali Bartsch, Wiznet, Germany
14:40 – 15:00	Multi-Parameter Physically Unclonable Functions with Thin-Film Multimodal Transistors (MULTI-TRUST) Dr Radu Sporea, University of Surrey; Dr Hans Kleemann, TU Dresden
	Session 3: RISE Impact Competition Winners Chair: Dr Louise Cushnahan, CSIT, Queen's University Belfast
15:00 – 15:20	SHIELD: A New Layer of Defense with Intelligent Hardware Monitoring for Safer Embedded Systems Dr Sangeet Saha, University of Essex
15:20 – 15:50	**Break & Networking**
15:50 – 16:10	PaRtial Execution oF EncRypted dAta using reconfiguraBle hardware (PREFERABLE) Prof Gareth Howells, University of Essex
16:10 – 16:30	Combating fake media with edit-tolerant authentication Daniel Fentham, Prof Mark Ryan, Dr Xiao Yang, University of Birmingham
16:30	**Day 1 Closing Remarks**
19:00	**Drinks Reception & Buffet** **The Admiralty, 66 Trafalgar Square, London**



Presentations at the 2026 RISE Collaborative Research Showcase & Spring School



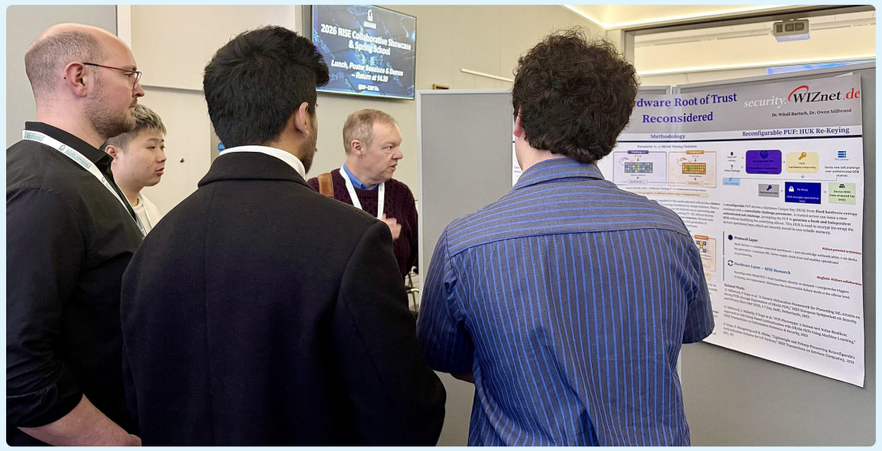
Keynote Presentation: Prof Georg Sigl, Director, Frauhofer AISEC



Dr Chongyan Gu, Queen's University Belfast



Demo session



Poster session



Networking during the demo and poster sessions

A summary of the agenda for day 2 and contributors is as follows.

Day 2 – Friday 6th March 2026	
09:00 – 09:30	**Registration – Tea / Coffee / Refreshments**
09:30 – 10:15	**Keynote: Design and Validation of RISC-V based Secure Microcontroller Chips** Prof Georg Sigl, Director, Fraunhofer AISEC
10:15 – 10:35	National Cyber Security Centre (NCSC)
10:35 – 11:05	**Break & Networking**
	Session 4: Hardware-Rooted Security in RF, Photonic and Semiconductor Systems Chair: Prof Gareth Howells, University of Essex
11:05 – 11:25	Securing Device Identification Using Hardware Impairments in RF Circuits Dr Junqing Zhang, University of Liverpool; Prof Aydin Sezgin, Ruhr-Universität Bochum
11:25 – 11:45	Security of Photonic Integrated Circuits Dr Cillian McPolin, Digital Catapult; Prof Mahdi Nikdast, Colorado State University
11:45 – 12:05	Optical Sources for Secure Timing in Critical Infrastructures Dr Samuel Shutts, Cardiff University
12:05 – 12:25	Security Assurance of Semiconductor Manufacturing (SASM) Dr Sridhar Adepu, Swansea University; Mayura Padmanabhan, SEMI
12:25 – 13:40	**Lunch, Poster Session & Networking**
	Session 5: AI & Hardware Security Chair: Prof David Oswald, Durham University
13:40 – 14:00	Establishing a Low-Cost Platform for Advanced Security Testing of AI Hardware Dr Chongyan Gu, Queen's University Belfast; Dr Aydin Aysu, North Carolina State University
14:00 – 14:20	Security-Enhanced AI Inference Edge Processors Dr Amro Awad, University of Oxford; Prof Hussam Amrouch, Technical University of Munich
14:20 – 14:40	AI-Sec – Secure NoC Architectures for Deep Learning Systems Dr Arnab Biswas, Queen's University Belfast; Prof Ankur Srivastava, University of Maryland
14:40 – 15:00	RISE Updates & Future Opportunities
15:00	**Closing Remarks**

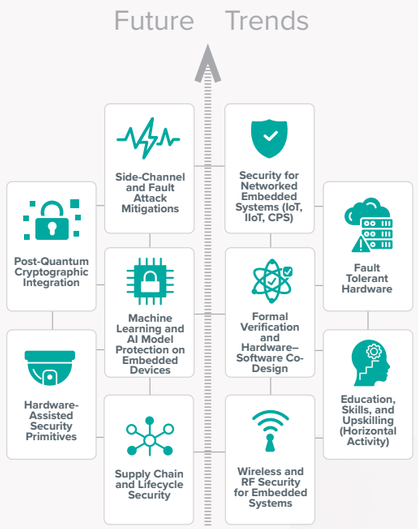


2025 RISE Impact Competition winners

FUTURE RESEARCH TRENDS REPORT

The RISE Industry and Stakeholder Advisory Board (ISAB) enables member companies and other stakeholders to engage directly with researchers, ensuring that RISE activities and funding calls are informed by real-world challenges. Following review of a draft at the 2025 Annual Conference, RISE published the 2025 ISAB report, Future Research Trends in Security Hardware and Embedded Systems, updating the previous report published in 2022.

The report outlines the projected future trends for 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. It draws on contributions from non-academic industry experts and sets out the social, legislative and threat-landscape context driving hardware security priorities.



The ten future trends identified by the ISAB

Priorities

The report sets out a phased roadmap of research priorities, with education, skills and upskilling identified as an overall horizontal priority underpinning every phase:

Phase 1: Foundation and Immediate Challenges (2025–2026)	Side-channel attack mitigation; low-overhead cryptographic primitives for embedded devices; secure firmware update and boot; threat modelling and risk assessment.
Phase 2: Post-Quantum and Lifecycle Integration (2026–2028)	PQC implementations for embedded systems; secure design and verification tools from RTL to FPGA/ASIC; hardware–software co-design (e.g. CHERI); trustworthy supply chains and anti-counterfeiting; secure decommissioning.
Phase 3: AI and Edge Security (2028–2030)	Adversarial resilience of ML on edge devices; secure inference and federated learning; on-device model watermarking and IP protection; security for autonomous systems; energy-efficient security for AI hardware.
Phase 4: Formal Methods and Resilient Architectures (2030–2032)	Formal verification from transistor level to firmware; runtime monitoring and adaptive security; secure composable microarchitectures; global certification frameworks; fault tolerance.



The full report is available on the RISE website:

RISE IMPACT COMPETITION FUND

IMPACT COMPETITION 2026 – CALL 2

Building on the success of the first competition, RISE launched a second Impact Competition call, offering awards of up to £40k to accelerate the translation and pull-through of research in secure hardware and embedded systems into practical tools and technologies. The following projects were funded:

Securing Cloud Computing with Hardened Hypervisors	Dr Marius Muench, University of Birmingham This project aims to create technology for securing cloud computing by introducing separation of security domains with strict isolation of sensitive resources. The project will extend Quarantine, their hardened-hypervisor prototype, to provide efficient isolation via hardware-enforced compartmentalisation. This provides strong security guarantees while reducing run-time overhead, as hardware-enforced compartmentalisation will protect against both transient execution attacks and traditional software vulnerabilities.
HARDAI: Hardware Assisted & Adaptive AI Framework for Cross-Platform Real-time Detection of Zero-Day Ransomware	Dr Shancang Li, Cardiff University While hardware-level signals (e.g., CPU performance counters, memory access patterns and cache behaviour) have shown promise in improving detection robustness, existing approaches are typically hardware-specific and lack adaptability, limiting their deployment across diverse computing environments. The proposed HARDAI project addresses this critical gap by introducing a hardware-aware and adaptive AI framework. Rather than relying on fixed hardware features, HARDAI will dynamically identify and utilise the most informative hardware-level signals available on a given platform. This enables cross-platform deployment, allowing the system to operate effectively across heterogeneous environments while maintaining high detection accuracy and a low false negative rate.
GridGuardian: Cyber Resilient Embedded Protection for Distributed Energy Hardware	Dr Mohammed Eisa, University of Sheffield GridGuardian is a hardware-embedded cyber-security co-processor for solar inverters and EV-charging stations. Rather than relying on external gateways or cloud-based monitoring, it is designed to integrate directly with the existing controller stack, where it validates sensor data streams using lightweight AI/ML anomaly detection, embeds a traceable cryptographic voltage-vector watermark, and triggers anomaly-aware control fall-backs that maintain safe power delivery during cyber-attacks.

RISE-FUNDED WORKSHOPS

To further grow the UK hardware security community, RISE introduced a new call for workshops, providing funding to support academics in the RISE community to host their own workshops and events around the UK.

Funding of up to £15k is available to host individual events in emerging areas relevant to the RISE technical research challenges. Applications are considered on a rolling basis, with expressions of interest submitted to **info@ukrise.org.**

The following workshops have been funded to date.

CONFAD 2026: THE 1ST WORKSHOP ON ADVANCES IN CONFIDENTIAL COMPUTING

Dr Amro Awad

UNIVERSITY OF OXFORD

Dr Ahmad Atamli

University of Southampton

University College, University of Oxford
8th May 2026

The 1st Workshop on Advances in Confidential Computing (ConfAd) bridges academic research and industrial developments to help envision the future of confidential computing. The workshop is a forum to discuss key enablers, anticipate challenges, and understand current limitations toward a coherent vision for next-generation confidential computing. ConfAd includes invited talks by academic and industry leaders, along with competitively selected research presentations from its call for papers.

BUILDING SUPPLY CHAIN CONFIDENCE IN SECURE HARDWARE SYSTEMS

Dr Basel Halak

University of Southampton

University of Southampton
10 September, 2026

This one-day, training-focused workshop is aimed at PhD students, early career researchers and professionals working in, or moving into, secure hardware, embedded systems, semiconductor assurance and supply-chain resilience. Through lectures, discussion, case studies and hands-on activities, participants will:

- **Explore the hardware lifecycle** – from IP and fabrication to deployment and maintenance.
- **Identify real-world threats** – including hardware Trojans, counterfeit components, IP piracy and reverse engineering.
- **Think critically about assurance** – learning to assess evidence, test assumptions and build confidence under uncertainty.

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS



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

UK RISE