RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

QUEEN'S UNIVERSITY BELFAST

RISE ANNUAL REPORT

2024–2025

Funded by

in association with National Cyber Security Centre

EPSRC
Pioneering research and skills

CONTENTS

FOREWORD

The Research Institute for Secure Hardware and Embedded Systems (RISE) continues to strengthen its position as a national and international focal point for research, innovation and skills development in hardware and embedded systems security. Hosted at the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, RISE remains committed to addressing security challenges across the full lifecycle of hardware systems, from design and manufacture through to deployment and operation.

This reporting period marks an important milestone for the Institute, with RISE Phase 2 funding extended by a further two years, supported by an additional £1m investment. RISE Phase 2 will now continue until 31 March 2028, enabling the Institute to continue delivering its programme of activity and deepen its impact. This extension provides continuity and momentum for our research portfolio, community building activities, training initiatives and engagement with industry, government, and international partners.

RISE continues to align closely with national priorities, including the UK National Cyber Strategy and the National Semiconductor Strategy, both of which emphasise the importance of secure by design approaches and the critical role of hardware security in protecting future digital infrastructure. Against a backdrop of increasing supply chain complexity, advanced cyber threats, and geopolitical uncertainty, RISE is well positioned to contribute evidence based research and practical solutions that support UK resilience, sovereignty, and economic competitiveness.

During this period, RISE has continued to support its three EPSRC funded affiliated research projects addressing trustworthy deep learning based hardware Trojan detection, trusted execution beyond the CPU, and the security of composable hardware platforms. Alongside these research projects, we have delivered a vibrant programme of community and skills focused activities, including the RISE Summer School and Annual Conference, a UK wide Hardware Security Training Roadshow, and new mechanisms to support early stage innovation and impact through our Impact Competition Fund. In particular, it was especially encouraging to see the launch of international collaborative seed funding calls in semiconductor security, strengthening global partnerships in this strategically important area.

Looking ahead, the extended Phase 2 programme will enable RISE continue delivering its annual conference, training activities, a further Impact Competition, while deepening engagement with international partners to explore longer term collaborative opportunities. We will also maintain a strong focus on supporting policy development, working closely with government and industry stakeholders to ensure that research insights translate into real world security improvements.

RISE will continue to play its part in advancing world leading research in hardware and embedded systems security, growing the UK skills base in this strategically important area, and supporting the delivery of national cyber security and semiconductor ambitions.

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

Three RISE affiliated projects are currently being delivered and are due to be completed in 2026-2027. These include:

TRUDETECT: TRUSTWORTHY DEEP-LEARNING HARDWARE TROJAN DETECTION

Prof Máire O'Neill
Dr Ihsen Alouani
Dr Niall McLaughlin

QUEEN'S UNIVERSITY BELFAST

The modern semiconductor supply chain increasingly relies on overseas foundries and third party IP and test facilities, exposing chips to hardware based security threats such as counterfeiting, IP piracy, reverse engineering, and hardware Trojans (HTs).

HTs are malicious circuit modifications designed to alter or compromise system behaviour, and while publicly confirmed cases are rare, real world incidents involving counterfeit hardware demonstrate the feasibility of stealthy backdoor insertion. These threats pose serious risks to safety critical and embedded systems in sectors such as medical, automotive, and transport, and have raised growing concerns around supply chain sovereignty and cyber security.

Reflecting this, recent policy initiatives, including the EU Cyber Resilience Act and the UK National Cyber Strategy. emphasise the need for secure by design approaches. In response, the TruDetect project aims to develop a trustworthy deep learning based HT detection system, integrating robust, adversary resilient detection and explainable AI techniques within EDA security verification workflows.

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

Trusted Execution Environments (TEEs) allow users to run their software in a secure enclave while assuring the integrity and confidentiality of data and applications. However, cloud computing these days relies heavily on peripherals such as GPUs, NICs, and FPGAs.

Extending the security guarantees of CPU TEEs to such accelerators is currently not possible. New technologies are being proposed to address this, notably the PCIe Trusted Device Interface Security Protocol (TDISP). IOTEE is aims to evaluate the security guarantees of this new PCIe standard and its ability to provide trusted execution against strong adversaries.

This will involve developing an emulator for the protocol, the use of formal modelling, as well as researching countermeasures against various software and hardware attacks.

SECCOM: SECURING COMPOSABLE HARDWARE PLATFORMS

Prof John Goodacre
Dr Bernardo Magri
Dr Lucas Cordeiro

MANCHESTER 1824
The University of Manchester

Aligned with RISE, this project addresses the security challenges introduced by composable hardware platforms, where dynamically assembled components undermine the fixed security assumptions of traditional, statically defined architectures.

While existing systems rely on predetermined security properties, composable designs—such as those enabled by PCIe and emerging standards like Compute Express Link (CXL)—introduce arbitrary configurations for which no established security models exist. The project seeks to characterise security properties and threat models across the composable hardware design space, and to determine whether robust security models can be derived and enforced, including through dynamic runtime verification.

The ultimate goal is to provide industry with a principled, verifiable security framework for composed hardware platforms that can reason about and demonstrate security despite their dynamic nature.

REVISED RISE TECHNICAL RESEARCH CHALLENGES

As part of continuing development and evolution of RISE, a review was undertaken of the research challenges that RISE aims to meet. Views were gathered from attendees during a breakout session at the Summer School & Annual Conference, as well as follow-up discussion with the RISE industrial advisory board and with NCSC representatives. This input was distilled into a refresh of the RISE technical research challenges.

IMPORTANCE OF HARDWARE SECURITY

The UK National Cyber Strategy 2022 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, 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'.

But today's semiconductor industry faces serious security challenges due to advanced cyber threats and complex geopolitics. This is exacerbated by both the complexity of securing microelectronic systems across their lifecycle, and the reliance on third-party IP, overseas foundries, and third-party test facilities. This outsourcing introduces hardware-based threats, including counterfeiting, IP piracy, reverse engineering, and trojans.

Compounding the issue, unintentional design flaws in Integrated Circuits (IC) can go undetected for years, further exposing the supply chain to vulnerabilities across all IC design and manufacturing stages. With the drive towards Net Zero, security solutions also need to be as energy efficient as possible.

Effective hardware and embedded systems solutions are becoming increasingly important in a range of industries and applications. Examples include:

- Connected devices/IoT: Hardware security is essential for connected devices, such as sensors in autonomous vehicles or network-connected medical devices, as it provides a foundational layer of protection against physical and cyber threats. In such connected environments, hardware security ensures that the devices themselves are trustworthy, protecting sensitive data and preventing unauthorized access.
- Cyber physical systems (CPS): CPS systems integrate digital components with physical processes, typically in environments where safety, reliability, and real-time responses are needed. Hardware security provides the backbone for ensuring that CPS can perform securely and safely, especially in critical infrastructure, autonomous systems, and industrial applications.
- Advanced manufacturing /Industry 4.0: These systems involve safety-critical, highly interconnected, and automated operations across industrial, manufacturing, and logistical processes. Hardware security offers foundational trust to such systems, protection against unauthorised access, protection of sensitive data, tamper resistance, and assurance of real-time operations, reducing the risk of downtime and operational disruptions.
- Critical national infrastructure (CNI): Sectors like energy, water, transportation, telecommunications, and others underpin society's ability to function. Hardware security is crucial for CNI as it provides resilience against cyber and physical attacks, preventing service disruptions, protecting sensitive data and providing assurance that CNI operate securely and reliably, helping to build public trust and confidence in these fundamental services.

RISE is set up to foster research into these security challenges, to contribute to the security goals set out in the National Cyber Strategy and National Semiconductor Strategy.

RISE TECHNICAL RESEARCH CHALLENGES

1.

Understanding the behaviour of technologies at the root of hardware security.

a. What makes a resilient hardware security primitive?
b. How do we analyse hardware behaviours to ensure technologies work as desired and are trustworthy?
c. How can novel primitives be used to provide trust to a system?
d. How do we advance secure-by-design technologies?
e. Can we develop hardware security metrics to help assess the effectiveness of security technologies?
f. How to evaluate hardware security vulnerabilities of new computing technologies, e.g neuromorphic, quantum, biological?

2.

Developing more secure products.

a. What novel architectures (hardware or hardware/software) add to the security of a product or system?
b. Can we understand the security of a system of components with their own individual security properties?
c. How can we make a product or system more resilient to faults and attacks?
d. Can hardware be used to replace or simplify security elsewhere in a system?
e. Can we enhance security without significantly impacting performance and energy efficiency?

3.

Maintaining confidence in security throughout the design and manufacturing processes.

a. How can we improve hardware security in automated semiconductor design and manufacturing processes?
b. Can we develop new (trustworthy) AI approaches for automating security verification, creating more accurate and efficient AI models for security analysis, and integrating these technologies into the hardware design lifecycle?
c. What tools and techniques could help to reduce the risks associated with third party hardware design and manufacturing services?
d. Can we build security mechanisms with hardware traceability and provenance functionality?

RISE SUMMER SCHOOL AND ANNUAL CONFERENCE

A summer school and joint annual conference event was held at the university of Birmingham campus in July 2024. The programme covered 2 days with talks from research community on topics related to hardware and embedded system security, as well as practitioners from industry including Amazon Web Services, Codasip, LowRISC and Crypto Quantique. This event was also an opportunity for the RISE projects to be introduced to the wider community, and to raise awareness and dissemination of the NCSC problem book.

The event was co-chaired by Prof. Máire O'Neill and Prof. David Oswald.

Edgbaston Hotel and Conference Centre on the University of Birmingham campus.

Summary of the agenda and some photos of the event are as follows.

DAY 1

RISE Summer School & Annual Conference, 30th July 2024	
09:30 – 10:00	Registration & Tea/Coffee on Arrival
10:00 – 10:10	Opening Remarks
10:10 – 10:50	**Rene Henriquez** and **Dr Zitai Chen**, Amazon Web Services *Relentless evaluation of the foundational security of AWS Nitro systems early in the design*
10:50 – 11:30	**Dr Shweta Shinde**, ETH Zurich *Ahoi Attacks: Breaking Confidential VMs with Malicious Interrupts*
11:30 – 12:10	**Luca Wilke**, University of Lübeck *Single-Stepping Attacks and Defences for Confidential VMs*
12:10 – 13:20	**Lunch & Networking (Posters + Show & Tell)**
13:20 – 14:00	**Ranga Desikachari**, Crypto Quantique *Quantum-Driven crypto primitives at the heart of Hardware Root of Trust (HRoT)*
14:00 – 14:40	**Dr Carl Shaw**, Codasip *How to work with industry*
14:40 – 15:00	**Break & Networking**
15:00 – 15:40	**Prof Simon Moore**, University of Cambridge *CHERI memory protection: pathways to industrial adoption*
15:40 – 16:20	**Prof John Goodenough**, University of Sheffield *Towards Secure Integrated Semiconductor Systems*
	Closing Remarks
18:00 – 21:00	Dinner at The Studio, 7 Cannon St., Birmingham, B2 5EP

DAY 2

RISE Summer School & Annual Conference, 31st July 2024	
09:00 – 09:20	Registration & Tea/Coffee on Arrival
09:20 – 09:30	Opening Remarks
09:30 – 10:10	**Dr Greg Chadwick**, lowRISC *Building secure hardware with Open Silicon at lowRISC*
10:10 – 10:40	RISE Project Update for TruDetect: *Trustworthy Deep-Learning based Hardware Trojan Detection* **Prof Máire O'Neill**, **Dr Ihsen Alouani**, **Dr Niall McLaughlin**, Queen's University Belfast
10:40 – 11:00	**Break & Networking**
11:00 – 11:30	RISE Project Update for IOTEE: *Securing and analysing trusted execution beyond the CPU* **Dr Ahmad Atamli**, **Prof Vladi Sassone**, Peiyao Sun University of Southampton **Prof David Oswald**, **Prof Mark Ryan**, University of Birmingham
11:30 – 12:00	RISE Project Update for SECCOM: *Securing composable hardware platforms* **Prof John Goodacre**, **Dr Bernardo Magri**, **Dr Lucas Cordeiro**, University of Manchester
12:00 – 12:30	*UK-US Semiconductor Security Workshop Whitepaper* **Prof Máire O'Neill**
12:30 – 13:30	**Break & Networking**
13:30 – 13:45	NCSC Problem Book
13:45 – 15:00	RISE Challenges: Breakout Session & Feedback
	Closing Remarks
15:15 – 16:00	RISE ISAB Meeting (Closed session)

Breakout session to discuss RISE Technical Research Challenges

Prof John Goodacre and Dr Lucas Cordeiro, University of Manchester, and Dr Ihsen Alouani, Queens University Belfast introducing their RISE research projects to attendees.

Dr Greg Chadwick, lowRISC; Dr Peiyao Sun, University of Southampton and Dr Qifan Wang, University of Birmingham

HARDWARE SECURITY TRAINING ROADSHOWS

Our planned hardware security training roadshow was successfully delivered in February 2025. The training targeted PhD's, postdocs, and early career researchers, with 3 training sites selected as Queens University Belfast, the University of Sheffield, and the University of Surrey. The training was delivered by Joe Fitzpatrick of Securing Hardware LLC from the USA.

This training aimed to 'distil the art of hardware hacking into the science of a standardised penetration testing procedure'. The course analysed how and why hardware hacks belong in scope of certain pen tests, and what that means to threat modelling and deliverables. Building upon basic skills to see how more advanced hardware and firmware analyses reveal more about the software vulnerabilities in a system. Hardware exploits were prototyped and developed into compelling demo concepts and tools for potential red-team activities. The course was centred around a standardised pen testing procedures, applied to case studies.

- Pre-engagement
- Intelligence Gathering
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

Case studies:

- A consumer, off-the-shelf Solid-State Drive
- A customised 'smart' thermostat

Training roadshows at Queens University Belfast (top) and the University of Sheffield (bottom)

RISE IMPACT COMPETITION FUND

One of the key challenges in commercialising University research through either licensing or the creation of a spin-out, is access to the early-stage funding necessary to take a novel idea to an early stage of proof – thereby validating the commercial potential to attract additional investment. To help address this challenge RISE developed the Impact Competition Fund to support projects and individuals to identify potential to deliver economic impact via a licence, open sourcing, or creation of a spin-out.

In May 2025, RISE ran a UK-wide Impact Competition, offering awards of up to £40,000 for projects of up to 6 months in duration, with the intention of moving research concepts to the next stage of proof, for example, to develop an early prototype, more in-depth market understanding or generation of additional data to support idea validation.

The following three projects were awarded Impact funding:

PARTIAL EXECUTION OF ENCRYPTED DATA USING RECONFIGURABLE HARDWARE (PREFERABLE)

Professor Gareth Howells

University of Essex

The proliferation of connected devices has exposed valuable code and data to increasing risk from physical capture and forensic attacks, while existing protection mechanisms, including TEEs, TPMs, PUFs, OS-level controls and even advanced cryptography, have proven vulnerable, impractical, or too costly for edge systems. This project proposes a fundamentally different hardware–software co design approach that embeds confidentiality by default, keeping all code and data persistently encrypted and only transiently decrypted within modified CPU execution units.

SHIELD: A NEW LAYER OF DEFENSE WITH INTELLIGENT HARDWARE MONITORING FOR SAFER EMBEDDED SYSTEM

Dr Sangeet Saha

University of Essex

SHIELD is a novel hardware-based approach for anomaly detection. It establishes trust and provenance in the integrity of on-board computing units and critical embedded systems (ES), such as those found within industrial robots, autonomous vehicles etc. by analysing their inherent physical and behavioural characteristics.

COMBATING FAKE MEDIA WITH EDIT-TOLERANT AUTHENTICATION

Daniel Fentham
Prof Mark Ryan
Dr Xiao Yang

UNIVERSITY OF BIRMINGHAM

This project aims to develop and demonstrate practical techniques that enable the authenticity of digital video content to be verified even after common post processing edits such as cropping or blurring. By allowing cryptographic verification of unaltered video regions while supporting necessary privacy preserving modifications, the work addresses growing challenges around trust, misinformation, and the misuse of AI generated media.

COLLABORATIVE RESEARCH SEED FUNDING CALL

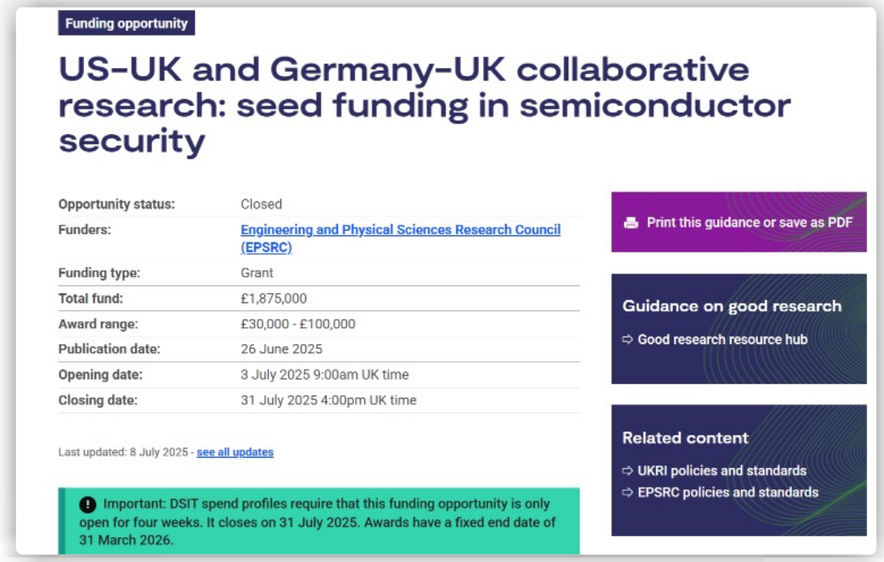
RISE was pleased to partner with DSIT and EPSRC to issue a US-UK and Germany-UK Collaborative Research call for seed funding in Semiconductor Security.

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 new RISE technical research challenges.

Applications from early career researchers (ECR) were encouraged and applications from post-doctoral researchers were eligible as a researcher co-lead with a suitable PL 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.



Funding opportunity

US-UK and Germany-UK collaborative research: seed funding in semiconductor security

Opportunity status:	Closed
Funders:	Engineering and Physical Sciences Research Council (EPSRC)
Funding type:	Grant
Total fund:	£1,875,000
Award range:	£30,000 - £100,000
Publication date:	26 June 2025
Opening date:	3 July 2025 9:00am UK time
Closing date:	31 July 2025 4:00pm UK time

Last updated: 8 July 2025 - see all updates

Important: DSIT spend profiles require that this funding opportunity is only open for four weeks. It closes on 31 July 2025. Awards have a fixed end date of 31 March 2026.

Print this guidance or save as PDF

Guidance on good research
⇨ Good research resource hub

Related content
⇨ UKRI policies and standards
⇨ EPSRC policies and standards

The call opened 3 July 2025 and closed 31 July 2025.

“RISE will continue to play its part in advancing world leading research in hardware and embedded systems security”

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

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

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

ukrise