RITICS

A portal to cutting edge UK research
into the cyber security of cyber physical, critical systems

Annual Report 2025

RITICS is a network of academics, industrialists and government working on the cyber security of cyber physical systems.

FUNDED BY :

HOSTED AT :

IMPERIAL

Contents

Co-Directors: Chris Hankin and Emil Lupu

Welcome to the 2025 Annual Report from the Research Institute for Trustworthy Interconnected Cyber-Physical Systems (RITICS). This last year has been a busy one. Some of the highlights have included:

The completion of our second cohort of Fellows
This included our first Fellowship to be co-funded with Industry. You can read about the achievements of our Fellows later in this report.

Our second annual RITICS Fest, a dynamic two-day event showcasing contributions from both industry and academia.

The initiation of a scheme to develop training materials for presenters at RITICS events
Our Advisory Board has highlighted the need to ensure that presenters are better equipped to communicate their results to the broad audience at RITICS events – which typically ranges from policy makers through practitioners to academics. We are working with the Chair of the Advisory Board and a consultant to address this challenge.

We were also pleased to see that Community of Interest guidance which is hosted on the RITICS website was cited in the new version of the Cyber Assessment Framework.

This report delves deeper into these achievements and more. We invite you to explore our milestones and learn about how RITICS is driving innovation across the cyber-physical systems landscape. To join our expanding community or for further information, please see the contact details on the final page of this report.

Contact us at: ritics@imperial.ac.uk

Introduction

The Research Institute in Trustworthy Interconnected Cyber-Physical Systems (RITICS), founded in 2014, has evolved into a cornerstone for cyber-physical system (CPS) security research in the UK. Initially focused on industrial control systems and funded by EPSRC in collaboration with the Centre for Protection of National Infrastructure, RITICS addressed sector-specific threats in energy, digital, rail, and other critical infrastructures. Through this work, RITICS built strong academic-industry collaborations and was involved in the launch of the ICS Community of Interest, fostering knowledge exchange and contributing to cyber security strategies like the Rail Cyber Security Strategy.

The second phase, starting in 2018, broadened RITICS' remit to cover diverse CPS areas, including the Industrial Internet of Things (IIoT), with EPSRC and NCSC support. Research in this phase addressed the interactions between safety and security, CPS cloud usage, cyber security training for control engineers, and regulatory challenges under the Network and Information Security Directive.

In 2023, RITICS entered a new phase with NCSC support for the Director role and UKRI backing for research, welcoming Professor Emil Lupu as Interim Co-Director. Recent projects focus on economic impacts of cyber security for critical infrastructure and advancements in digital twins. RITICS continues to foster an open, interdisciplinary community involving over 20 UK universities and actively engages academic and industry stakeholders through fellowships, research initiatives, and regular collaborative meetings.

Workshops

The purpose of the workshops and events is to facilitate knowledge sharing, foster innovation, encourage collaboration and building networks.

1. RITICS Showcase, 28th January 2025 – *Scale Space, Imperial College London, White City Campus*

The showcase featured presentations from the 2024 fellows as the fellowships neared the end of their funding period, as well as presentations from the 3 projects associated with RITICS and funded as part of EPSRC's call "Research aligned with cybersecurity research institutes". Two of the projects are funded by EPSRC, and the third by Defence Science and Technology Laboratory (DSTL).

2. Security of Safety Critical Cyber-Physical Systems, 4th June 2025 – GM Digital Security Hub(DiSH), Heron House, Manchester

A RITICS workshop was held to assemble researchers and practitioners from the security and safety communities to discuss emerging challenges and changing trends across multiple critical sectors. Key topics included the interplay between security and safety, the impact of cyber and physical attacks, ensuring continuous assurance amidst dynamic changes, and the role of AI and formal methods in sustaining security and safety.

3. Security Enterprise Connected Devices, 11th June 2025 – *Imperial College London, South Kensington Campus*

RITICS hosted a workshop for the Department for Science, Innovation and Technology's (DSIT) Call for Views on a proposed Code of Practice for Enterprise Connected Device Security. The event provided members of the academic community with insights from government and industry and an opportunity to provide feedback on the proposed code, which outlined 11 security principles for manufacturers, as well as on supplementary policy interventions..

4. Resilient Cyber-Physical Systems: From Security-by-Design to Testing, 18th June 2025 – *Imperial College London, South Kensington Campus*

This work shop explored security assurance approaches for cyber-physical systems. The event included talks and breakout sessions covering topics such as building testing ecosystems, developing portable digital twins and attack models, and integrating security into the Model-Based Systems Engineering (MBSE) lifecycle.

5. Bridging Research and Practice in OT Penetration Testing, 27th September – *Imperial College London, South Kensington Campus*

The event brought together academic insight, practitioner experience, and strategic perspectives. During the workshop, findings from the RITICS-funded research project were presented, with talks from speakers including Adam A from NCSC and John Fitzpatrick of Lab539. Attendees, who were actively engaged in OT security, discussed challenges, shared insights, and reflected on the future direction of the field.

6. RITICS Fest 2025, 2nd and 3rd – *Imperial College London, South Kensington Campus*

In September 2025, RITICS Fest was held as a two-day annual workshop at Nova South and White City, Imperial College campus in London to discuss security advancements in Industrial Control and Cyber-Physical Systems. Professionals from government, industry, and academia attended the event. Keynote speaker Ollie Whitehouse Chief Technology Officer, of the National Cyber Security Centre (NCSC) addressed the gathering.

During the fest, Ollie from NCSC discussed the "next phase of cyber physical systems," emphasizing the implications for Critical National Infrastructure and national security due to the increased prevalence of AI, drones, and autonomous systems. He noted the growing complexity of the threat landscape, requiring the cybersecurity industry to adapt and foster innovation despite not always having full knowledge of complex systems. Ollie also highlighted lessons from Ukraine regarding protecting Critical National Infrastructure during physical conflict and discussed new challenges presented by the energy sector's evolution toward distributed networks. He outlined key research priorities for the community, including incentivizing robust cybersecurity investment, retrofitting legacy systems, and improving threat detection. The fest featured discussions on topics such as post-incident reviews, using research to inform policy, and probabilistic models for designing resilient systems. It also included "5-minute madness" sessions where early career researchers presented their work.

Projects

The following RITICS-associated projects have been funded by the EPSRC's "Research aligned with cybersecurity research institutes" grants.

Countering HArms caused by Ransomware in the Internet Of Things (CHARIOT)

Dr G Oikonomou, Dr J Pope, University of Bristol, Dr LB Arief, Professor J. Hernandez-Castro, University of Kent.

Project Collaborators: Loetec Limited, National Nuclear Laboratory (NNL), Toshiba Europe Limited (UK), u-blox Malmö AB (Sweden)

The CHARIOT project, a three-year funded project, aims to mitigate the risks and reduce the impact of ransomware attacks on Industrial IoT (IIoT) networks, which include highly constrained wireless embedded systems and other cyber-physical devices. By advancing research in this area, CHARIOT seeks to make ransomware attacks on IIoT and cyber-physical systems more challenging and less appealing for attackers. To achieve this, the project focuses on developing, designing, and prototyping innovative, state-of-the-art solutions for detecting, preventing, recovering from, and immunising against ransomware in IIoT environments.

The CHARIOT project has collected evidence and demonstrated that the threat of ransomware in resource-constrained IIoT environments is not only plausible, but also that it has different properties compared to ransomware attacks against traditional desktop systems, necessitating a new and more appropriate approach to deal with this threat. A paper demonstrating the real threat of IIoT ransomware has been published (https://doi.org/10.1109/DCOSS-IoT65416.2025.00116), and another paper is currently being prepared to report on the propagation/spreading techniques that can be utilised by IIoT ransomware — along with potential countermeasures.

In the second year of the project (September 2024 to August 2025), the Bristol and Kent teams continued their collaboration through regular online meetings and in-person meetings at both locations (roughly every 3-4 months for the in-person meetings, alternating between Bristol and Canterbury). On top of continuing with the development of proof-of-concept ransomware prototype for computationally-constrained devices and low-power wireless communication protocols, the project has explored ways to detect and mitigate IIoT ransomware threat. For instance, the team has been working on a micro-auditing approach for detecting IIoT ransomware, resulting in another published paper (https://research-information.bris.ac.uk/en/publications/micro-auditing-for-ransomware-detection-in-resource-constrained-i).

Additionally, the last couple of years have seen the emergence of Large Language Models (LLMs) as a dominant force in Artificial Intelligence (AI), leading to potential ways for automation and optimisation (e.g., for better threat detection). At the same time, LLMs potentially open up new attack vectors, in which malicious actors may misuse them for nefarious purposes, including malware and ransomware generation. We have been exploring this promising — and yet potentially threatening — area of development, leading to the publication of several papers related to LLMs and cyber security (https://doi.org/10.1109/DCOSS-IoT65416.2025.00116, https://doi.org/10.48550/arXiv.2505.09974, https://doi.org/10.48550/arXiv.2503.09334).

In the final year of the project, efforts will be made towards finding solutions to deal with IIoT ransomware, including novel techniques for containment and recovery, as well as a continued exploration on the threat of ransomware in IIoT domain, which will not disappear anytime soon.

RESICS: Resilience and Safety to attacks in ICS and CPS

Prof. EC . Lupu (Imperial College London), Dr S. Adepu (University of Swansea), Luca Castiglione, Dipojjwal Ray

Project Partners: Adelard (UK), Airbus Operations Ltd (UK),Carnegie Mellon University (US), QinetiQ (UK), Reperion (Singapore), Siemens (UK), Singapore University of Tech & Design, (Singapore), Thales Ltd (UK), University of Naples Federico II (Italy)

During the past year we have refined the framework for our risk and impact assessment method, clarifying further some of the differences between the safety and the security perspectives. These aspects were presented at the RITICS Thematic Workshop on Safety and Security, and then in a position paper being accepted and presented at SafeComp 2025. We have also elaborated further our approach to learning causal models using the VARLiNGAM and VARMALiNGAM approaches focussing on evaluating the most likely time lags and refining the directionality. The approach was evaluated on data from the individual stages of the SWaT testbed. We have combined our Bayesian Attack Graph (BAG) method and the causal model in a combined continuous risk evaluation approach. Bayesian Attack Graphs can be used to evaluate the likelihood of an attacker obtaining a position (i.e. a set of privileges) in the system and updating that likelihood when parts of the system have been compromised. Considering the attack actions that can be performed from that position, we then use causal inference to determine the impacted process variables through cascading effects and show results of our approach on the Secure Water Treatment (SWaT) testbed with a risk measure for each of the affected components. We have further refined the work on the generation of Security Assurance Case fragments presented at the Safety Critical Systems Conference (SSS 2025) and continued to investigate the integration of our toolchain with Model Based Systems Engineering (MBSE).

We are working now on resilience aspects and methods to select intrusion response actions that can ensure the resulting system configuration isolates compromised elements whilst satisfying safety properties and transitioning the system to a working operating state.

Post-Quantum Blockchains Based on FALCON++

Dr. C. Ling, Prof. WJ Knottenbelt, Imperial College London

Project Collaborators: PQ Solutions Limited

In recent years, blockchain technology has emerged as a transformative force in the digital landscape, best known as the foundation of cryptocurrencies such as Bitcoin and Ethereum. However, cryptocurrencies represent just one of many potential applications of blockchain. The technology's scope extends to areas such as smart contracts, e-voting, and the Internet of Things (IoT). With the NIST standardisation process marking the start of a broader transition to post-quantum cryptography, our project aims to explore these advances by applying a lattice-based post-quantum digital signature scheme known as FALCON (Fast-Fourier Lattice-based Compact Signatures over NTRU).

A key component of the FALCON protocol is discrete Gaussian sampling over lattices. We have made significant progress by proposing a new sampling algorithm for a family of lattices widely used in cryptography. Our work uncovers a novel connection between discrete Gaussian sampling and linear codes under the Lee metric. When applied to well-known cryptographic lattices, the proposed sampler achieves an order-of-magnitude speed-up compared to state-of-the-art sampling algorithms. Our findings have been recognised with acceptance at a prestigious cryptography conference:

Bollauf, M.F., Lie, M., Ling, C. (2025). On Gaussian Sampling for q-ary Lattices and Linear Codes with Lee Weight. In: Tauman Kalai, Y., Kamara, S.F. (eds) Advances in Cryptology – CRYPTO 2025. CRYPTO 2025. Lecture Notes in Computer Science, vol 16000. Springer, Cham. https://doi.org/10.1007/978-3-032-01855-7_11.

2025-26 Fellowships

The following projects are RITICS funded fellowships as part of the 2025 call. The number of applications for RITICS-funded fellowships has increased from 11 in 2023, to 14 in 2024 and to 25 in 2025. This growth demonstrates a rising interest and engagement in research within this area, which is a positive indicator of the relevance and reach.

UK Strengthens Cyber-Physical Infrastructure Security Amid Rising Threats

Pantelis Koutroumpis, Oxford University

Cyber-Physical Systems (CPS), integral to daily life and national infrastructure, are facing escalating cyber threats due to increasing interconnectivity. The UK is now the third most targeted country for cyber-attacks globally, behind the US and Ukraine, according to the House of Commons (2023). In response, the head of the National Cyber Security Centre recently warned that UK providers of essential services must take these threats seriously.

Over the past decade, academic researchers and regulators have ramped up efforts to address vulnerabilities in Critical National Infrastructures (CNI) while multiple studies have shown that organised groups pose the single greatest threat to Industrial Control Systems (ICS). In an effort to identify threat actors and their methods, researchers have focused on predicting the implications of cascading system failures by modelling attack paths and performing in-depth penetration testing.

On the regulatory front, the UK government is actively planning to further deter these threats by implementing the Cyber Security and Resilience (CSR) Bill in 2025. This legislation follows extensive overhauls of the existing NIS directive (akin to NIS2 in the EU) and is expected to broaden regulatory coverage, increase penalties, and raise compliance demands. Acknowledging the targeted equipment cyber attacks, the Product Security and Telecommunications Infrastructure (PSTI) regulation introduced in 2023 aims to cover all smart products sold in the UK, imposing strict security requirements and penalties for non-compliance.

These regulatory interventions jointly form a two-pronged strategy— a holistic top-down enforcement via the Cyber Security and Resilience Bill and increasing bottom-up requirements via the Product Security and Telecommunications Infrastructure regulation. Together, they aim to shift the cost burden of cyber-attacks from society to organisations, incentivising stronger security practices and reallocating the negative externalities from improper security practices to their rightful owners. This fellowship will address whether these changes are sufficient and proportional to the risks posed by the threat actors, given the concerns around increases in the cost of service provision that could potentially strain labour and capital resources, especially in non-market sectors.

Confidence in Security of Critical Infrastructure

Taimoor Khan, University of Greenwich

In the frame of this fellowship, we are exploring the foundational question: “How do we have confidence in the security of a cyber-physical system (CPS)?” We are seeking to examine and define what constitutes confidence in the security of systems that integrate physical and digital components, where vulnerabilities in either domain can have cascading effects. The inquiry addresses several sub-problems identified in the NCSC Cyber Physical Problem Book, including security assurance, security testing, operational technology (OT) and cyber-physical interface security, and security risk management. By bridging these domains, the fellowship is establishing a theoretical and methodological foundation to guide future interdisciplinary research across technical, assurance, and policy-oriented communities

As a starting point, we are exploring the problem space, grounded in literature review and exploratory studies, which examines how different disciplines conceptualize, measure, and justify confidence in CPS security. The project is focused on two distinct but complementary research paradigms: model-driven and data-driven approaches.

Model-driven approaches emphasize the use of formal models, simulations, and structured reasoning to assess whether a system meets its defined security objectives. In contrast, data-driven approaches rely on empirical evidence, monitoring, and analytics to infer security posture and detect anomalies at runtime.

Continued on the next page

Together, these methodologies represent the dual strategies by which confidence in CPS security can be built, validated, and maintained throughout the system's lifecycle.

The findings are articulated in a taxonomy that categorises the various ways confidence is generated and validated across different lifecycle stages—specifically, at design-time and run-time. Design-time confidence focuses on assurance activities conducted before deployment, such as formal verification, static analysis, or model-based security testing. Run-time confidence, on the other hand, pertains to ongoing evaluation and adaptation through monitoring, risk management, and operational resilience strategies. The taxonomy will address how these forms of confidence interact, overlap, and evolve in response to both cyber and non-cyber threats, whether man-made or natural.

The research systematically addresses the following questions:

- Notions of confidence: What forms or conceptualisations of confidence are supported by current practices in security assurance, testing, OT, and risk management?
- Requirements for confidence: What technical, procedural, and contextual requirements are necessary to establish each type of confidence?
- Measurement approaches: How is confidence determined—qualitatively, quantitatively, or through hybrid methods—and what metrics or indicators are employed?
- Strengths and limitations: What are the inherent constraints, trade-offs, and blind spots of each notion of confidence, particularly when applied to complex CPS environments?
- Integration and unification: How can these disparate notions of confidence be harmonised into a coherent framework that allows for quantifiable assessment of CPS security confidence?

Through these questions, we are producing both conceptual clarity and practical insights into how diverse assurance and testing practices contribute to confidence in CPS security. The expected outcome provides a foundational framework that not only delineates how confidence can be justified across different stages of system development and operation but also facilitates communication among stakeholders in engineering, cybersecurity, assurance, and policy domains.

Ultimately, we aim to advance scientific understanding and practical methodologies for establishing and reasoning about confidence in CPS security. By articulating a common language and taxonomy, it will support evidence-based security assurance and guide future research agendas across interdisciplinary communities concerned with cyber-physical resilience, governance, and regulation.

From top to bottom Presenting at the RITICS Fest 2nd and 3rd September 2025: Ollie Whitehouse, Vijay Kumar and Andrew Martin

2024-25 Fellowships

The following projects are RITICS funded fellowships as part of the 2025 call.

OT Penetration Testing

Dr Ric Derbyshire, Orange Cyber Defense

Effective penetration testing is crucial for securing the operational technology (OT) environments of critical sectors, such as water, power, and manufacturing. However, traditional IT penetration testing techniques have not yet been successfully adapted to fragile OT assets, as set out in problem 4 of the NCSC Problem Book and as alluded to by the Cyber-Physical problem set question: "How do we have confidence in the security of a cyber-physical system?".

This fellowship aims to explore OT penetration testing in its current state to understand its efficacy. The overall aim is to use relevant literature and the expertise of industry practitioners to expose both technical and methodological gaps, and to offer solutions that may improve security assurance in the OT domain. The fellowship's output will:

- Produce a consolidated set of research questions in the field of OT penetration testing;
- Suggest pathways to potential solutions to make OT penetration testing suitably effective; and
- Stimulate continuing academic/industry collaboration and research in OT penetration testing.

Phase 1 of the fellowship will establish the current state of the art, draw out key themes, and uncover initial gaps by conducting a thorough review of academic and industry literature. The review will focus on tooling, methodologies, guidance, and novel research available to penetration testers approaching the OT space.

Phase 2 will conduct semi-structured interviews with industry practitioners to discern their awareness, interpretation, and expert opinions regarding the key themes and gaps identified in the literature. However, to best understand the efficacy of OT penetration testing, the perspective of OT operators commissioning penetration tests must be considered, as well as OT penetration testers. Therefore, the participants will be distinguished and evenly distributed by the group to which they belong.

The interviews will use Orange Cyber defense's ethics process that prioritises participant anonymity and safety, while holding the interviewer and their management accountable.

Highlighting the gaps uncovered and it was then discussed of any potential technical and methodological solutions for improving OT penetrate testing the gaps uncovered and discuss any potential technical and methodological solutions for improving OT penetration testing. This analysis, along with the literature review and interview process, will be formally written up as a paper to be submitted to an appropriate academic venue.

The final project will disseminate the results of the fellowship to a wider audience, which will attract further community collaboration. This will be achieved through submitting talks to recognised venues, including multiple BSides, CYBERUK, S4, CyberTek, and the IET's annual OT cyber security conference. The dissemination strategy will be to describe the current landscape of OT penetration testing and its challenges, before presenting the gaps, research questions, and potential solutions to explore, which will provide an effective call to action for further engagement.

Due to the primary research of this fellowship being derived from interviews, a crucial requirement is to recruit a variety of participants from each group. To reach data saturation and for a suitable variety of participants, a minimum of 10 will be interviewed (5 per group). Participants will be recruited from the applicant's own contacts, the NCSC Industrial Control Systems Community of Interest's Security Testing Expert Group (STEG), and RITICS. Recruitment will begin from notification of funding. Participants will be informed of the research intentions and why they have been approached via participant information sheets and consent forms, which will be collected before each interview.

Dr Ric Derbyshire Presenting at the RITICS Fest 12th September : Dead Man's PLC: Ransoming the Physical World via Operational Technology

Towards Security Assurance for Cyber Physical Systems

Dr. Ashraf Tantavy, Cranfield University

Cyber-physical systems are typically mission-critical; therefore, establishing trust in their secure operation is essential for resilience against cyber-attacks. Security assurance refers to the confidence that security mechanisms comply with established policies and effectively protect the system. In practice, security assurance is achieved through a combination of methods and techniques applied throughout the system design lifecycle, including requirements analysis, design, implementation, testing, and operation & maintenance. However, the mission-critical nature of cyber-physical systems limits the techniques that can be applied. For example, large-scale penetration testing on operational systems is often infeasible due to the potential impact on system performance. Consequently, new approaches and methods are required to address the security assurance challenges in cyber-physical systems.

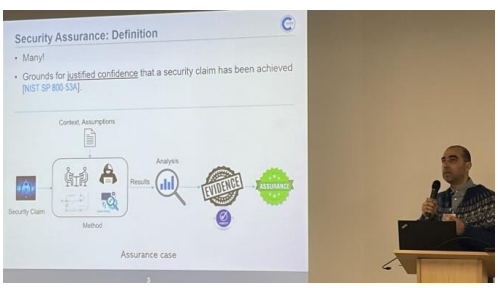
This project explored two key approaches to security assurance—penetration testing and security-by-design—along with their associated challenges and potential. Given the difficulty of performing penetration testing on live systems, testbeds and cyber ranges have emerged as practical alternatives for offline testing. The study found that, despite the abundance of testbeds in both academia and industry, there is a lack of coordination between efforts, particularly in hardware replication and software reuse. This is partly due to confidentiality constraints. To address this, the project proposes a testbed ecosystem in which developed testbed artefacts conform to a standard architecture and interface, supported by a centralised repository for reuse. These artefacts could include digital twins, software implementations of industrial protocols, virtual machines for IoT devices, datasets, and more. Although challenges such as domain variability exist, such an ecosystem could significantly accelerate research in cyber-physical systems security.

Security by design, where security considerations are embedded from the earliest stages of system development, also emerged as a key principle in the design of cyber-physical systems. Integrating security into the system design lifecycle is challenging, as it requires an ecosystem of languages, tools, and methods to support the process. To address this, the project proposes the use of Model-Based Systems Engineering (MBSE) as a framework for security-by-design. MBSE is a methodology that uses formalised models to support the design and verification of complex systems, supported by the SysML language standard. MBSE offers a viable framework for embedding security-by-design principles into the design process and integrating security assurance methods by utilising SysML system models. The combination of MBSE, security-by-design, and security assurance provides a comprehensive approach to addressing the security assurance challenge in cyber-physical systems. Given the existing gaps and multidisciplinary challenges, this project proposes the formation of a special interest group focused on integrating cybersecurity with MBSE.

If you are interested in one or more of the directions explored in this project, please contact Dr Ashraf Tantavy:

Email: ashraf.tantavy@cranfield.ac.uk

LinkedIn: https://www.linkedin.com/in/ashraf-tantawy/



Dr Ashraf Tantavy Presenting at the RITICS Showcase 28th January : Towards Security Assurance for Cyber Physical Systems

Exploring Security and Motivation

Dr Neetesh Saxena, Cardiff University

The Fellowship focused on understating cyber-physical assets and their impacts on operational technology (OT) systems, addressing challenges posed by system complexity and legacy equipment. Cyber-physical systems are widely used in critical industries such as energy, healthcare and manufacturing; however, their complexity and interdependence increase their vulnerability to cyber-attacks. Effective asset management is essential to mitigate risks in cyber-physical systems. However, the management of cyber-physical assets poses unique challenges due to the dynamic nature of physical and digital systems. Traditional asset management methods often struggle to maintain real-time synchronisation between physical and cyber assets. In one of the works, the project discussed a new asset management approach which blends physical tracking techniques and cyber asset discovery methods to enhance visibility, track changes in real-time, and identify

vulnerabilities. Furthermore, the work addressed a research problem of developing an asset-criticality identification framework in smart grids. Existing frameworks typically focus on identifying critical assets within a specific domain, such as electric systems or cyber assets, without considering the interdependencies between cross-domain assets linking the cyber and power layers. This work has built a comprehensive framework for physical and cyber layers in smart grids. In another contribution, the work developed a comprehensive comparative analysis framework for evaluating CVSS and IVSS methodologies in industrial contexts. The work transformed complex scoring data into actionable insights through intuitive visualisations, enabling security professionals to grasp the implications of different assessment approaches through correlation plots, severity shift analyses, and distribution comparisons. The work further explored cyber risks, looking at why there's often a big gap between what cybersecurity frameworks recommend and what actually gets implemented on the ground. The work argues that while frameworks, such as NIST CSF and IEC 62443 are useful, they're often too broad to be applied effectively without more practical support. It highlights the need for adaptive, real-time defences — like Zero Trust and AI-based threat detection — and calls for more collaboration across government, regulators, and industry to keep these critical systems secure.

The increasing sophistication of cyber-attacks targeting critical infrastructure necessitates robust incident response strategies to safeguard operational continuity. This part of the work examined the development of effective incident response measures against advanced threats, such as the Industroyer malware, through the lens of the Industrial Control System (ICS) Cyber Kill Chain framework. By analysing the 2016 Ukraine power grid attack, the work identified Tactics, Techniques, and Procedures (TTPs) employed by adversaries and maps them to defensive countermeasures across each phase of the kill chain. The findings emphasise the importance of tailored incident response protocols to mitigate risks to critical assets, ensuring the resilience of industrial control systems against evolving cyber threats.

The work also included international visits and collaborations, such as IIT Delhi (India), attending and presenting work to international conferences (e.g., IEEE CSR, IEEE PerCom, ACM AsiaCCS), and interreacted with national and international experts, researchers, and industry practitioners. The Fellowship also enabled organisation of events, workshops, and special issues.

The Fellowship work also created an interdisciplinary community group aiming to promote research, interaction with community members, and interdisciplinary collaborative work with industry and academic partners on related topics. Link to the group page: https://sites.google.com/view/cycis/events/cyber-physical-assets-interdisciplinary-group-cpaig

Neetesh Saxena Presenting at the RITICS Showcase 28th January 2025 : Exploring Security and Impacts of Cyber Physical Assets

The Bristol Cyber Security Group team (L-R) picture from 2024 : Louise E, Sridhar A, Jacob W, Feras S, Joe G, Stanislav A, Kostas A, Manolis S, Alma O, Marios S, Awais R.

Funding

Bristol Capture the Flag

The BrICS CTF 2025 was the third industrial control systems (ICS)-focused capture-the-flag (CTF) event hosted by the University of Bristol. It followed the Bristol Cyber Defence Exercise (BCDE) held in September 2023, funded by the PETRAS Institute, and the second event in 2024, rebranded as BrICS and funded by RITICS. The 2025 event took place from 25th to 27th June 2025 and was fully funded through a £10,000 grant from RITICS.

Expressions of interest were received from 21 teams, 18 from industry and 3 from academia. To ensure sectoral diversity, 12 industry teams were invited, with 6 additional teams held in reserve. Ultimately, 11 teams participated, as one team withdrew too late to invite a replacement. Most teams consisted of four members, resulting in 42 registered participants.

Participating organisations represented several sectors, including Critical Infrastructure Operators (Welsh Water, Yorkshire Water, EDF, National Grid, and Transport for London), Aerospace and Defence (Rolls-Royce and Leonardo), and Engineering Consultancies (Amentum, Arup, Bilfinger, and Arcanum).

Pre-event training was delivered by Hacktonics Limited, a University of Bristol start up specialising in ICS/OT security training. The four-hour session, provided at no cost, covered topics such as:

- Introduction to ICS
- Asset scanning in ICS
- Gaining unauthorised access to HMIs through VNC
- Manipulating running processes using industrial protocols in Python

Most participants attended the training, which used LINICS, a new ICS testing distribution from Hacktonics, provided on university laptops. Challenges in the CTF aligned with the training content, enabling participants to apply newly acquired skills.

The CTF competition was conducted over two days, The team from Welsh Water won first place, followed by Amentum and Rolls-Royce.

The event utilised extensive physical ICS equipment from the Bristol Cyber Security Group testbed. Each team received a Siemens and Allen-Bradley ICS training box, as well as a laptop equipped with a process simulator, PLC programming software (such as Siemens TIA Portal), and a Kali virtual machine with ICS-specific tools.

Travel Grant

Dr. Popov was awarded a travel grant of up to £5,000 to support research travel undertaken during his sabbatical leave. The grant enabled several research visits across Europe, which led to new collaborations, research outputs, and ongoing projects. A detailed financial breakdown of the expenditure was provided separately by City Finance.

University of Florence (Resilient Computing Lab)

The main visit took place from 10 February to 11 April 2025. During this period, Dr. Popov collaborated with Dr. Tommaso Zoppi on confidence-based machine learning ensembles for classification, resulting in a joint publication in Information Fusion. He also applied quantitative models of software design diversity to machine learning ensembles, generating novel insights into ensemble diversity, sample difficulty, and trade-offs between classifier performance and diversity. The visit produced a comprehensive 40-page technical report, which is being developed into several joint publications.

Dr. Popov also delivered a guest lecture on “Software Design Diversity” to MSc students, which was well received. In recognition of his contributions to research and teaching, he was appointed Visiting Fellow (Researcher) by the University of Florence.

University of Naples Federico II
A subsequent visit to Naples included a seminar on “Safety Assessment of Autonomous Vehicles,” attended by over 40 participants. Dr. Popov held discussions with Dr. Roberto Pietroantonio and his team on the use of causal reasoning for optimal test-case generation in autonomous vehicle safety assessment, leading to plans for continued collaboration.

ISTI-CNR, Pisa
An additional visit to ISTI-CNR allowed Dr. Popov to meet with Dr. Felicita Di Giandomenico and her research group. The discussions focused on extending software design diversity models to incorporate cyber-attack modelling, resulting in a joint publication in Reliability Engineering and System Safety. The group also explored the novel concept of “diversity in specifications” as an innovative extension to traditional design diversity models.

EUROCOMP, Sophia-Antipolis, France
Dr. Popov also visited Prof. Ludovic Apvrille at EUROCOMP in Sophia-Antipolis, France, to discuss a potential joint project on the safety and security of adaptive cyber-physical systems using TTool-AI. The parties agreed to establish an international consortium and pursue EU research funding. This visit was not supported by the travel grant.

Research Outcomes
The sabbatical and associated travel resulted in several publications and submissions related to the safety assessment of autonomous vehicles, including:

- Popov, P. (2025). Dynamic Safety Assessment of Autonomous Vehicles based on Multivariate Bayesian Inference (DyAVSA). Journal of Reliable Intelligent Environments.
- Popov, P. Why Black-Box Bayesian Safety Assessment of Autonomous Vehicles is Problematic and What Can Be Done About It? (Under review, IEEE Transactions on Intelligent Vehicles).
- Popov, P. et al. Stochastic Modeling of Road Hazards on Intersections and Their Effect on Autonomous Vehicle Safety (Under review, IEEE Transactions on Intelligent Transportation Systems).
- Zhao, X. et al. (2025). On the Need for a Statistical Foundation in Scenario-Based Testing of Autonomous Vehicles (IEEE ITSC 2025).

External Activities

Community Events

Throughout the reporting period, several external engagement activities were undertaken that supported and extended the objectives of RITICS. These activities included participation in workshops, conferences, collaborative meetings, and industry events with key partners across academia, government, and the private sector. Each activity contributed to strengthening research collaborations, promoting knowledge exchange, and enhancing the visibility of RITICS within the wider cyber security and critical national infrastructure communities.

Date	Activity	Organisation	Location	Purpose	Brief Description
05/02/2025	Panel	Plexal	Sunderland City Hall	Cyber runway	Dragons' Den event for Plexal-supported cyber start-ups. Chris also contributed to a panel
19/02/2025	Attendee	SWAN	University of Bristol	Showcase	SWAN is a prosperity partnership that focuses on Secure Wireless
24/02/2025	Interviewee	DSIT	Online	Quantum and ICS/CNI	Interview about the impact of QC on security of CNI and ICS
17/03/2025	Keynote speaker	Bristol Uni	Watershed, Bristol	Keynote lecture	Lecture about QC impact on CNI
25/03/2025	Panel	Future Water Assoc	Arup HQ	Future cyber threats to Water	Panellist discussing emerging threats
11/06/2025	Participants and host	DSIT	Imperial College London	Provide members of the academic community with insights from Government and industry and opportunity to provide feedback on the proposed code, the supplementary policy interventions, and DSIT's wider approach.	The Department for Science, Innovation and Technology (DSIT) has published a Call for Views on a proposed Code of Practice for Enterprise Connected Device Security.
27/10/2025	Board Meeting	INCS-CoE	British Ambassador's Residence Tokyo	Presenting RITICS to Board	INCS-CoE is an international collaboration (incs-coe.org).
10/09/2025	Interviewee/Reviewer	UK Parliament Post	https://researchbriefings.files.parliament.uk/documents/POST-PN-0753/POST-PN-0753.pdf	To explain the importance of cyber resilience for the UK's digital infrastructure, outline major threats and challenges, summarise current policies and regulations, and present strategies to improve national resilience against cyber incidents.	"POSTnote 753 – Cyber Resilience of UK Digital Infrastructure" is a UK Parliament briefing that outlines key cyber threats to national digital systems, explains current resilience policies, and highlights strategies to strengthen the UK's ability to withstand and recover from cyber incidents.

Future Plans

Community Events

RITICS plans to host a showcase event where its projects and fellows will present updates and accomplishments in their work. Additionally, RITICS will continue to host an annual RITICS Fest, providing a platform to explore the latest advancements in Industrial Control and Cyber-Physical Systems security and foster collaboration among experts from government, industry, and academia.

Two thematic workshops are also planned, each focused on advancing critical areas requiring deeper knowledge and enhanced collaboration. Lastly, a broader RITICS workshop will bring together the national community, offering an opportunity to present challenges from industry and government and to showcase progress within the RITICS scope at locations across the UK.

Community Building

We have developed outline plans aiming to create an industrial club that companies would subscribe to. The intention is that funds raised through this mechanism would be available to the RITICS community to support meetings and some seed-corn funding. This would supplement the NCSC funding which is available for fellowships. The club would also further collaboration between industry and academia. The next stage will be to test the feasibility of our plans with a small number of industrial supporters.

RITICS
Imperial College London

South Kensington Campus
London SW7 2AZ

E-mail: ritics@imperial.ac.uk

ritics.org