# RITICS Newsletter


## UPDATES

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.

## PROJECT UPDATES

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

## ANNOUNCEMENT

RITICS has commissioned a training programme for RITICS Fellows to develop and mature their presentation skills. This will be a blend of online learning followed by an onsite workshop offering hands-on practice and personalised feedback. This training is designed to help researchers translate complex technical content into accessible, engaging presentations for diverse audiences.

The online training will be extended to all who presented at RITICS Fest 2025 and there may also be opportunities to extend the online workshop to those interested, too.

## FUNDING OPPORTUNITIES

We are excited to announce the availability of a small fund to support members of the RITICS community. This funding can be utilised for various purposes such as travel grants, workshop organisation, feasibility studies, and similar activities. Individual awards will be capped at £5,000.

To apply, please submit a one-page document (A4 size) with reasonable margins and a minimum font size of 11pt. The application should outline the purpose of the funding, the benefits it will bring to the RITICS community, and include a detailed breakdown of the costs.

Applications will be reviewed twice a year, during Spring and Autumn. Preference will be given to early career researchers. All applications to be sent to ritics@imperial.ac.uk

## UPCOMING EVENTS

Register and save the dates for the following events:

| Title | Location | Date | Registration |
|---|---|---|---|
| Economics of Security | Oxford Martin School (University of Oxford) | Friday 5th December | Register here |

## GET IN TOUCH

Email us with your news that you would like to share with the community or reach out on LinkedIn