Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

RITICS

Research Institute in Trustworthy Inter-connected Cyber-physical Systems

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

Annual Report 2023

RITICS is a research community addressing the security challenges in Trustworthy Inter-connected Cyber Physical Systems

It is hosted by the Institute for Security Science and Technology; Imperial College London's hub for security research and engagement.

SUPPORTED BY:

National Cyber Security Centre
a part of GCHQ

UKRI Engineering and Physical Sciences Research Council

HOSTED BY:

Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

Contents

For more information

Discover the latest research and funding news, copies of the RITICS newsletter, and contact details for the whole RITICS network at: www.ritics.org

To learn more about the RITICS community please contact us at: ritics@imperial.ac.uk

Introduction

RITICS (RITICS) was founded in 2014 as a consortium of five related research projects funded by the UK Engineering and Physical Sciences Research Council (EPSRC) in collaboration with the UK Government's Centre for Protection of National Infrastructure (CPNI). At that time, we were focused on industrial control systems and particularly interested in exploring the physical harms that could arise from cyber interference, communicating risk and developing novel mitigations. The projects on harms and mitigations explored specific sectors such as power distribution (CAPRICA), the digital railway (SCEPTICS) and general modelling techniques (CEDRICS and RITICS@IC). Risk was addressed by CEDRICS and MUMBA, the latter team also developed extensive test-bed facilities. Whilst the research was relatively long-term, the projects established strong links with relevant industries; for example the Birmingham SCEPTICS team have subsequently been major contributors to the establishment of the UK Rail Research and Innovation Network (UKRRIN). This period also saw the creation of an industry-based Community of Interest in Industrial Control Systems (ICS CoI) which has now grown to hundreds of members. RITICS contributed to the development of a number of cyber security strategies (for example the Rail Cyber Security Strategy) and European work on standards (ERNCIP).

The second phase of RITICS (2018-2022) saw a change in the funding regime and a slight change of focus, broadening the remit to include more general cyber physical systems including the Industrial Internet of Things. EPSRC continued to support the Director but the UK National Cyber Security Centre (NCSC) took on responsibility for supporting the research activity. RITICS also continued to engage with the Community of Interest and contribute to the development of cyber security strategies in various sectors. The Network and Information Security Directive (NIS) came into force in mid-2018 and placed various requirements on the operators of essential services. A group of the projects funded through RITICS explored the implications of the NIS Directive on various sectors. The other projects were inspired by issues facing the Community and the NCSC; these covered topics such as the use of cloud services in industrial control systems, cyber security training requirements for control engineers and other roles, the conflicting requirements of safety and security, the role of software and hardware diversity in protecting systems against attack and the use of novel networking approaches in cyber physical systems. During 2022, we started a new funding scheme which led to the creation of two short-term fellowships: one of these continued the socio-technical work on the roll-out of the requirements of the NIS Directive and the other looked at the interactions between safety and security.

The current phase of RITICS started in January 2023. The Director role is now supported by NCSC and UKRI supports a research programme. Since April 2023, Pr ofessor Emil Lupu has joined RITICS as Interim Co-Director alongside Professor Chris Hankin. EPSRC call for research projects took place at the end of 2022 (link) and we report on the funded projects below. The NCSC funding includes provision for the continuation of the fellowship scheme. Two fellows have been appointed in 2023; one is focusing on economic aspects of cyber security for critical infrastructure and the other is focused on digital twins and modelling. We are looking to appoint a further two fellows in 2024, following a call for proposals issued in December 2023. Further details of the RITICS projects and fellowships are given below.

RITICS is an open community with over 20 UK universities involved in our various activities. We hold regular meetings and welcome new participants

Workshops

1. 2023 Fellowships, 8th March 2023 - online workshop; Registrations: 20

This workshop introduced the 2023 call for fellowship proposals and gave potentials applicants an opportunity to clarify aspects of the call

2. Cybersecurity in the Lifecycle of Orbital Systems, 6th July 2023 – Imperial College London, White City Campus; Registrations: 42

This workshop sought to highlight the wide array of design and operation topics that are required to secure an orbital system across the whole life of the device. Through insights from leading figures in the field of security and orbital engineering, this event looked at a breadth of challenges that the industry faces and initiated a dialogue on the approaches that can begin to address them.

3. Cyber-Physical Security Challenges of Maritime Operations Event, 26th October 2023 – University of Greenwich; Registrations: 58

This workshop included an overview of the Plymouth ecosystem which includes a cyber range, Cyber-SHIP (a re-configurable physical twin of a ship) and various simulation tools. The talk highlighted some vulnerabilities and the long term economic consequences of a successful attack. The workshop also considered port security and guidance issued by the IET (updated in 2020) and a cloud-based exercise with the US National Coast Guard.

4. Addressing the Economics of CNI Security in Railways, 16th January 2024 – Swansea University; Participants: Academia, Policy, Industry, Students; Registration 3

This workshop sought to uncover some of the research themes underlying CNI security in railways. A selection of speakers representing policy, industry and academia emphasised securing such CNI has to factor in the economic principles that govern the dynamics and relationships of the various stakeholders involved in terms of technology adoption and, behaviour and culture. The decisions of operators, suppliers and regulators affect key measures of risks, incidents and disruptions are also important. Equally relevant is the impact of digital and physical lock-ins, externalities and asymmetries. A depiction of some of the key themes is presented in the figure below.

ICS Community of Interest

The Industrial Control System Community of Interest (ICS COI) is an industry led UK community where knowledge of cyber security (and related safety information) can be exchanged to benefit the wellbeing of the UK. RITICS has been involved in the

CoI since its inception.

The community recognises the benefit in creating a network that's open to all organisations that have a vested interest in the improvement of ICS security and safety. This includes UK-based ICS operators, asset owners, security researchers, vendors, regulators, integrators, the UK government and academia.

The community now has over 300 members. Much of its activity is focused through expert groups which produce guidance documentation. This is hosted on the RITICS website (https://ritics.org/ics-coi/).

Projects

The following projects associated with RITICS have been funded as part of EPSRC's Call: Research aligned with cybersecurity research institutes.

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)

Summary: The aim of the 3-year CHARIOT project is to reduce the risk and potential adverse consequences of ransomware attacks in Industrial IoT (IIoT) network deployments comprising severely constrained wireless embedded and other cyber-physical devices. Through the proposed research, the proposers want to increase the difficulty of mounting successful ransomware attacks against IIoT and cyber-physical systems, making them less attractive targets for perpetrators. To that effect, CHARIOT will devise, design, and prototype creative, cutting-edge solutions for the detection, prevention, recovery and immunisation of/from ransomware attacks in IIoT environments.

Post-Quantum Blockchains Based on FALCON++

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

Project collaborators: PQ Solutions Limited (UK)

Summary: Blockchain hype has pervaded mainstream consciousness, largely owing to the capital growth of cryptocurrencies inspired by Bitcoin. This has been further driven by the increased adoption of cryptocurrencies by institutional investors and corporations. However, cryptocurrencies are just one of the many applications of blockchain technology; other areas include smart contracts, e-voting, and the Internet of Things (IoT). The NIST process of standardisation marks the beginning, not the end, of a paradigm shift to post-quantum cryptography. In this project, the proposers will apply one such lattice-based post-quantum digital signature scheme, FALCON (Fast-Fourier Lattice-based Compact Signatures over NTRU), and implement with modifying its existing trapdoor sampler with Monte-Carlo Markov Chain (MCMC) sampling. Moreover, we will also procure an example of blockchain implementation which incorporates this FALCON++ signature scheme, in order to compare classical and post-quantum digital signatures in the context of blockchains.

RESICS:Resilience and Safety to attacks in ICS and CPS

Prof. EC . Lupu (Imperial College London), Dr S. Adepu (University of Bristol)

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)

Summary: RESICS aims to significantly advance the state-of-the-art and deliver novel contributions that facilitate: a) risk analysis for cyber physical systems in the face of adversarial threats taking into account the impact of security events across the cascading inter-dependencies; b) characterising attacks that can have an impact on the safety of the system, identifying the paths that make such attacks possible; c) identifying countermeasures that can be applied to mitigate threats and contain the impact of attacks; and d) ensuring that such countermeasures can be applied whilst preserving the system's safety, operational constraints and maximising its availability. These contributions will be evaluated across several test beds, digital twins, a cyber range and a number of use-cases across different industry sectors. They will deliver increased automation, lower the skill requirements involved in the safety and security analysis and in mitigating threats and improve response times to security incidents. To achieve these goals RESICS will combine model-driven and empirical approaches across both security and safety analysis, adopting a systems-thinking approach which emphasises Security, Safety and Resilience as emerging properties of the system. RESICS leverages preliminary results in the integration of safety and security methodologies with the application of formal methods and the combination of model-based and empirical approaches to the analysis of inter-dependencies in ICSs and CPSs.

Fellowships

Economics of CNI Security

Professor Siraj Ahmed Shaikh, Swansea University

This fellowship pursues exploratory reserch questions on security economics of critical and national infrastructure protection. The aim is to establish foundational arguments (building over past literature and fresh research during the fellowship), to foster future research for diverse scientific communities across cyber-physical security, economics, supply chains, and policy and regulation. Professor Shaikh adopts a

- Macroeconomic framework to study incentives and penalties around CNI security. This will include how the decisions of operators, suppliers and governments affect key measures of risks, incidents and disruptions. This will also extend to understanding CNI supply chains (in terms of self-

sufficiency and national security) as part of strategic industries, and where may tax breaks, subsidies and protection from foreign competition be effective;

- Microeconomic framework to study the impact of digital and physical lock-ins, externalities and asymmetries (arising out of technologies and vendor-customer relationships), alongside organisational models of investment returns on spending on raising security awareness, and improving security behaviours and culture.

The goal is to accumulate evidence based on past research systematically, and conduct fresh interviews and focus groups with CNI, policy and research communities. Where possible, he aims to draw out case studies from a select few CNI verticals for dissemination.

Siraj will conduct a systematic literature review, where the search strategy is time-bound and keyword-wise within relevant disciplines, and the analysis and evaluation are qualitative. This will serve to uncover critical themes and track the emergence of relevant issues over time with a critical review.

Siraj aims to engage security practitioner communities across CNI verticals (preferably energy, water, transport, but he is open to others), through existing contacts and with the help of RITICS/ NCSC, and also invite new stakeholders from supplier and policy ecosystems. He proposes to conduct twelve individual interviews followed by two focus groups. The interviews will be semi-structured and open-ended, and will engage senior technical upwards to c-suite participants. The two focus groups would engage estimated participation of 6~8 individuals from cross-sector operational, technical and mid-management. The focus group participants would be encouraged to shape as a formal community under the banner of RITICS, with a soft governance structure to sustain beyond the two engagements.

What's next for Digital Twins (DTs) and Modelling in the context of Cyber-Physical Systems Security (CPSS)? Dr. Sridhar Adepu, University of Bristol

The DTs community in the UK has existed since 2018. The National Infrastructure Commission (NIC) (2018) report highlighted the idea of DTs. The National Digital Twin Programme was afterwards established, and DAFNI also began to support DTs platforms. A recent announcement from UKRI to "Develop a UK digital twinning research community with a NetworkPlus" will also build a community around DTs.

The main concern, as a CPSS researcher, is the lack of usability/applicability of DTs to CPSS in settings such as water, power and manufacturing systems, in particular security, accuracy, fidelity, security of DTs itself, human-interaction with DTs and explainability of DTs. There is a need to answer the following research and community questions (Majority picked from the RITICS workshop on 8th March):

1) DT: How to set foundations for future work in DTs for CPSS? In what situations DTs are useful and in what situations not useful in CPSS? Is DT able to help model, detect and mitigate attacks?

2) Stakeholders: How to ensure that research in DTs for CPSS is accessible? How to find new ways to build and interact with the community and support wider research activities? How do we promote the value of security and how can we provide security training in CPS using DTs? How to convince stakeholders by presenting risks arising from insecure CPS using DTs?

3) Fidelity: How to define the trade-off between fidelity, scalability and usefulness of the DT? What is the trade off in creating DTs in different life cycle of CPS? How to build a reconfigurable DT that can be configured for CPSS in the context of different CNIs such as water treatment plants, natural gas plants etc.

4) Human operator: How the human operator interacts with DT as well as real system under cyber-attacks? How to ensure feedback loop, human feedback and explainability in DTs for CPSS?

5) Resilience: How to assess, measure and improve resilience of CPS using DTs including in the context of cascading effects in Interconnected CPS? Can we use DTs to reduce downtime of CPS? Is it possible to use DTs to develop holistic approach for safety & security?

6) Trustworthy: How do we secure the DT? Is it act as a new threat vector for our CPS? How do we ensure DTs are trustworthy? What are the new types of security architecture and access control models required to support DTs for CPSS?

This project will build a community of CPSS experts together with modelling experts (such as simulation, formal & AI modelling) and CPS engineers to formalise DTs applicability to CPSS and any operational concerns. Our community of interest (COI) will work together to draw a roadmap for an improved version of DTs use in CPSS and suggesting a range of approaches inspired by 'agile delivery of infrastructure projects' (NCSC, 2017). The COI will advocate in the future iterations of DTs and communicate training needs wrt CPSS for future DT stakeholders. It is also essential to understand the policy aspects of DTs in CPSS. In addition to a policy strand of the roadmap, the fellow will draw on the National Cyber strategy outlining a set of cognisant research questions and matching research institutions with industry needs.

Proposed outputs include:

1) A community of practitioners dedicated to improving Digital Twins in CPS security (this could become a new working group in the NCSC ICS COI);

2) A co-designed roadmap with recommendations for future implementation of DTs use in CPS security;

3) A report outlining a research strategy for DTs use in CPS security for RITICS and NCSC: key questions, appropriate methods, timescales, training needs.

4) Recorded Podcasts and webinar for the DTs and RITICS communities

Future Plans

Community Events

RITICS aims to organise four workshops each year: a RITICS showcase where the RITICS projects and fellows present updates and achievements of their work, two thematic workshops focusing on specific areas where there is a critical need to advance knowledge and collaboration, finally, a more general RITICS workshop

aims to bring together the national community and offers an opportunity to present industry and government challenges and showcase advances made in the RITICS scope, anywhere in the UK.

Industrial

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.

Seminars

We plan to hold a regular virtual seminar series inviting leading UK and International researchers to present their work and their perspectives on the security of industrial control and cyber-physical systems. We anticipate that these will happen at lunchtime on a monthly or bi-monthly schedule.

Cyber Security Network

Following the recent UKRI call for a Network+ to strengthen the cybersecurity ecosystem, RITICS will be working with the other research institutes to prepare a proposal to run the network.

Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

RITICS
Imperial College London
Level 2 Admin Office, Central Library
South Kensington Campus
London SW7 2AZ

E-mail: ritics@imperial.ac.uk

ritics.org