

The Alan Turing Institute

RESEARCH ENGINEER, AGENTIC CRITICAL-SYSTEMS CYBER SECURITY– D&NS

THE ALAN TURING INSTITUTE

There has never been a more significant time to work in data science and AI. There is recognition of the importance of these technologies to our economic and social future: the so-called fourth industrial revolution. The technical challenge of keeping our data secure and private has grown in its urgency and importance. At the same time, voices from academia, industry, and government are coming together to debate how these technologies should be governed and managed.

The Alan Turing Institute, as the UK's national institute for data science and artificial intelligence, plays an important part in driving forward advances in these technologies in order to change the world for the better.

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. The Institute's goals are to undertake world-class research, apply its research to real-world problems, driving economic impact and societal good, lead the training of a new generation of scientists, and shape the public conversation around data and algorithms.

After launching in 2015 with government funding from EPSRC and five founding universities, the Institute has grown an extensive network of university partners from across the UK and launched a number of major partnerships with industry, public and third sector. Today it is home to more than 500 researchers, a rapidly growing team of in house research software engineers and data scientists and a business team.

BACKGROUND

Building on the successes of AI for Cyber Defence (AICD) Research Centre, the Defence & National Security (D&NS) team at the Alan Turing Institute is developing an ambitious programme of research to deliver a fundamental shift in Critical National Infrastructure (CNI) cyber-resilience using AI. The focus of this new programme is the cyber resilience of CNI, including legacy operational technology (OT) and end-of-life operating systems; both of which underpin critical sectors from energy and water to data operations, but that cannot be patched, upgraded, or modified without risking operational disruption or invalidating safety certification.

Working alongside a team of talented researchers and engineers at the intersection of machine-learning and cyber security, you will advance the research and engineering needed to:

- Build and support the development of LLM-based, agentic systems that can autonomously assess and harden hosts which have reached end-of-life status but are necessary for critical infrastructure. In the context of networks that include legacy / cyber-physical hosts, you will build and evaluate autonomous systems capable of discovery, vulnerability assessment, firewall policy generation, traffic monitoring, and defensive response.
- Build and refine simulation environments that are representative of genuine CNI use cases, including legacy operating systems running industrial software communicating over OT protocols.
- Research novel methods to guarantee the operational properties of systems are unharmed by agentic monitoring and hardening interventions.
- Contribute to high-quality research publications and open source code repositories supporting the overall project aims.

As a team we aim for high-impact research and innovation that delivers value for our stakeholders and the wider scientific, industrial, and government communities. Day to day, we collaborate with technical and subject matter experts from our partner organisations as well as academics, software engineers, and data scientists from across the Turing's research community. We present our work to a range of audiences including research colleagues, senior decision makers and non-technical stakeholders.

We are a cross-disciplinary team and encourage applications from computer and information security researchers, cyber security practitioners, software engineers, computer scientists, machine learning scientists, mathematicians, statisticians, data scientists, and data engineers.

The Alan Turing Institute

The team practices an agile, experiment-driven approach and values a positive, supportive and collaborative environment in which 'radical candour' and 'lifelong learning' are encouraged. We embrace failure as a learning opportunity and necessary precursor to success. We are empowered to take ownership of our work and operate with a high level of autonomy in our roles, to deliver measurable impact to our partners.

ROLE PURPOSE

This role will sit within the Defence and National Security team and will focus on advancing resilience of CNI by designing, building, and evaluating LLM-driven agentic systems for the autonomous hardening of legacy operational technology and industrial control systems.

Eligibility for Security Check (SC) clearance is a requirement for this role. Eligibility criteria and further information on the process can be found on the UK Government security vetting website.

HOW YOU WILL MAKE AN IMPACT

- Collaboratively design, build and maintain agentic, AI systems and evaluation suites that support CNI cyber resilience and legacy software hardening against known vulnerabilities.
- Develop virtualisation based digital twin environments and implement techniques for assuring operational continuity in the context of CNI.
- Develop realistic virtualised environments with legacy OT/ICS hosts, including legacy operating system instances running OT/ICS control software and with representative OT protocol traffic.
- Contribute to high-quality collaborative research as part of the Turing's CNI resilience mission.
- Develop CNI-relevant scenarios with clear threat models, operational continuity criteria, and defensible assumptions; document limitations and known failure modes explicitly.
- Implement reproducible evaluation pipelines: configuration-driven runs, dataset/version management, baseline implementations and auditable reporting outputs.
- Develop and validate metrics and scoring methods.
- Carry out analysis that supports credible interpretation of results (failure case analysis, ablations and sensitivity checks).
- Build high-quality research software to support evaluation at scale including maintainable code that other teams can run repeatedly and trust.
- Run large-scale evaluations on HPC and cloud platforms, improving performance and reliability through batching/parallelisation, resource-aware execution, and systematic debugging of non-determinism and environment drift.
- Produce high-quality technical artifacts and research outputs where appropriate, including technical reports, methodological notes, open-source contributions, and papers; ensure outputs are evidence-backed and technically precise.
- Communicate methods and findings clearly to a range of audiences (research colleagues, senior decision-makers, and non-technical stakeholders), without oversimplifying or overclaiming.
- Horizon scanning across relevant research domains for new advancements and methodologies.
- Undertake high-quality collaborative research to enhance resilience of CNI using machine learning and cyber security methods.
- Play a role in planning and running AI-based CNI red-blue teaming competitions, ensuring robust environment design and evaluation protocols are in place.

Please note that job descriptions cannot be exhaustive, and the postholder may be required to undertake other duties, which are broadly in line with the above key responsibilities. This job description is written at a specific time and is subject to changes as the demands of the Institute and the role develop.

The Alan Turing Institute

PERSON SPECIFICATION		
Skills and Requirements Post holders will be expected to demonstrate the following:	Essential (E) Desirable (D)	Tested at application (a) Tested at interview (i)
Knowledge and Experience		
Experience integrating with LLM APIs and building agentic or tool-calling pipelines to implement multi-step reasoning workflows (e.g., MCP, LangGraph).	E	A/I
A Master's degree (or equivalent qualification or experience) in cyber/information security, AI, machine learning, computer science, engineering, or a related discipline.	E	A
Understanding of network security principles including at least one of: defensive or offensive security techniques, network traffic analysis, or cyber-physical systems security.	E	A/I
Strong software development in a scientific computing context, ideally Python, with standard tooling (Git, Linux), and a track record of delivering working research software or applied engineering artefacts with measurable outcomes.	E	A
Ability to plan and carry out research independently or collaboratively, evidenced by high-quality outputs commensurate with career stage including publications, technical reports, or significant open-source contributions.	E	A/I
Familiarity with operational technology (OT) protocols or CNI/ICS/SCADA environments (e.g. Modbus, DNP3, OPC-UA), whether from research, industry, or hands-on experimentation.	D	A/I
Ability to work effectively in a multidisciplinary team, sharing knowledge and supporting others, while taking ownership of your own work including prioritising, meeting deadlines, and making evidence-based decisions with appropriate autonomy.	E	A/I
Excellent written and verbal communication, including presenting complex technical information to diverse audiences (research colleagues, senior decision-makers, non-technical stakeholders) and representing the Institute externally.	E	A/I
Must be eligible for SC (Security Check) clearance	E	A/I
Commitment to EDI principles and to the Organisation values	E	A/I

APPLICATION PROCEDURE

If you are interested in this opportunity you will need to register on the careers portal and complete the application form including your CV and cover letter. Your cover letter should focus on the following:

- Your motivation for applying for this role
- An overview of your experience developing software in a scientific computing context
- Publication list (if not covered in CV)

If you have questions about the role or would like to apply using a different format, please contact us on recruitment@turing.ac.uk.

TERMS AND CONDITIONS

This post is offered on a full time, fixed-term basis for 12 months. The annual salary is £45,505 - £51,241 plus excellent benefits, including flexible working and family friendly policies, [Employee-only benefits guide | The Alan Turing Institute](#)

Eligibility for Security Check (SC) clearance is a requirement for this role.

The Alan Turing Institute is based at the British Library, in the heart of London's Knowledge Quarter. We expect staff to come to our office at least 4 days per month. Some roles may require more days in the office; the hiring manager will be able to confirm this during the interview.

SECURITY CLEARANCE

The successful candidate may be required to undergo a pre-screening check prior to an offer being made. This check will be carried out by HMG Defence and Security Partners. Please be advised, by submitting your application you are consenting to this check, and your personal details (full name, date of birth and home address) to be passed onto our HMG Defence and Security Partners to carry out this check.

Many roles in the Defence and National Security Programme require higher levels of National Security Vetting where applicants must typically have 5 to 10 years of continuous residency in the UK or a NATO country depending on the vetting level required for the role, to allow for meaningful security vetting checks, amongst other factors. These roles are subject to security restrictions by Turing's partners. The restrictions mean that factors such as your nationality, any nationalities you may have previously held, your foreign connections, and your place of birth can restrict your eligibility to perform the role.

Eligibility criteria and further information on the process can be found on the UK Government security vetting [website](#). Applicants should check whether they are eligible to apply for SC clearance before applying to this role.

EQUALITY, DIVERSITY AND INCLUSION

We value diversity of background, experience, and perspective, and are proud to be an inclusive employer. We warmly encourage applications from all backgrounds, particularly from groups currently under-represented in our sector. If you feel passionate about this role but don't meet every single requirement, please apply – we recognise that great candidates may bring strengths beyond the criteria listed.

We are committed to making sure our recruitment process is accessible and inclusive. This includes making reasonable adjustments for candidates who have a disability or long-term condition. Please contact us at recruitment@turing.ac.uk to advise us how we can assist you.

Please note all offers of employment are subject to obtaining and retaining the right to work in the UK and satisfactory pre-employment security screening which includes a DBS Check.

Full details on the pre-employment screening process can be requested from HR@turing.ac.uk.

OUR VALUES

The Alan Turing Institute is committed to equality diversity and inclusion and to eliminating discrimination. All employees are expected to embrace, follow and promote our [EDI Principles](#) and Our Values.

