National Cyber Security Centre, in Collaboration with the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS)

Call for Proposals

Closing date: Friday 11 September 2020, 16:00

Summary

The National Cyber Security Centre (NCSC), working in collaboration with the Research Institute for the Trustworthy Inter-connected Cyber-physical Systems (RITICS), is inviting proposals from academic researchers for research into the topics relevant to the research challenges described below.

Working in conjunction with NCSC whilst undertaking research which is published in the public domain, RITICS has a strong track record of delivering high-quality academic research with the potential to significantly improve the field of cyber security, particularly in the field of operational technology (OT) or, more generally, cyber-physical systems. The RITICS community is multidisciplinary in nature, and includes a significant number of stakeholders in cyber security for OT practice, drawn from across government and industry. The successful projects will form part of the RITICS community and will share their research outputs and join in community events.

Background of the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS)

RITICS was founded in 2014, as the third of the cyber security Institutes set up by the UK Government in conjunction with the Engineering and Physical Sciences Research Council (EPRSC). Its early focus was to improve Cyber Security of Industrial Control Systems. RITICS was renewed and relaunched in spring 2018, with funding for a further 5 years, now sponsored by the National Cyber Security Centre in partnership with EPSRC.

The vision is that RITICS will carry out high-quality research which advances knowledge in research areas identified as having the greatest potential to transform the academic state of the art and user practice. In addition, it is anticipated that RITICS will provide a focus for liaison with stakeholders from the NCSC and other parts of government and business.

EPSRC and the NCSC aspire to promote wide visibility of the outputs of RITICS in order to enable fast dissemination and, where appropriate, application of the research to improve Cyber Security of cyber-physical systems and critical infrastructure in the UK as a whole.

Research challenges

This call concerns a number of research challenges that have been identified and refined through discussion with stakeholders. The broad areas are:

- Safety and Security
- Autonomous Systems
- Incident Response and Forensics
- Cyber Controls
- Interconnected Systems
- Supply Chain

These areas are elaborated below.

Context for the research

Evidence proving the effectiveness or not of different options or approaches, in different circumstances, is a key output of this research.

Other Research

The intention of this initiative is to identify and build on the work that has already been done, rather than duplicating it. Similarly, there are other research initiatives that complement this work. The topic space is large, and the intention is to align these initiatives where possible to avoid duplication of work and maximise our coverage as a community.

Safety and Security

- ICS sectors have concerns with the safety and security of ICS. The safety regime is well understood, but safety in these industries has the upper-hand, and it is often to the detriment of the security. *Why would you do an update to protect the security of a system, if it means you are unable to operate the system because the 'safety case' is no longer valid?* Are there best practices or processes used within the safety world which could apply in the cyber security world? How can those responsible achieve a level of assurance of the safety and security capability of a system as a whole?
- Research is required into the sociotechnical challenges faced by industry to improve safety and security related to ICS. What is preventing these communities coming closer together? How can these be addressed?
- Research is required to understand the trade-offs that may have to be made when the security of the system is put before safety, and when the safety of a system is put before security. What is the true safety cost of security? What about the security of the safety system itself?

Autonomous Systems

- Research is required to understand what assurance/assessment process can be used with systems that autonomously continue to learn, changing from their starting state. Can they be assessed? At what stage of 'learning and changing' should they be assessed? What level of assurance can be provided? How do you define the boundary of such a system? How do you know when it is secure, and when it is safe?

Incident Response and Forensics

- Research is required to define and test an approach for how to effectively respond to and recover from a cyber security incident in an Operational Technology (OT) context. What does an effective methodology look like for OT incident response? How does this differ across industry verticals? What planning must an organisation do ahead of an incident to ensure they can respond and recover? How does this differ from an IT incident response plan?
- Research is required to understand what (and how) technical artefacts can be recovered from Operational Technologies (OT) during incident response. How do these differ across different real time or embedded operating systems? Which platforms are most prevalent in common ICS systems? What capability can be proven for the recovery of volatile data during live response?

Cyber Controls

- Many Operational Technology (OT) protocols lack encryption. Research is required in to the 'trade off' of using encryption to protect OT protocols vs. not using encryption. Research should consider aspects such as the ability to monitor and maintain real time equipment when using and not using encryption. Does using encryption cause real-time issues or is there insufficient latency to raise concerns? What are the real risks of not using encryption? How can encryption be safely employed?
- Many Operational Technology (OT) protocols lack authentication. Research is required to explore controls to enact authentication within OT environments, when the devices and protocols by default do not support it. How can you safely prevent OT accepting or responding to protocol instructions from untrusted or unintended sources? What technology agnostic measures might be possible to address this issue? How can these be implemented and tested?
- Research is required to understand how to do unplanned change detection across cyber-physical systems. Is there a methodology that can be applied to do this across different families of devices and contexts?
- Research is required to understand how enumeration and identification of ICS/cyber-physical system assets can be safely undertaken. How can this be done in a way that ensures the system is not broken or compromised? What passive and active methods can be proven to do so safely?

Interconnected Systems

- Research is required into how a CNI sector or sub-sector can be most effectively modelled. Can a CNI sector be modelled to a level that is practical whilst providing insight into these dependencies and inter-dependencies? Can these sector models be combined into a single, system of systems view of the whole CNI?
- Research is required into how effectively digital twins can support security analysis, including identification of systemic vulnerabilities and points of low resilience.

Supply Chain

- Research is required to explore solutions to reduce risk to cyber-physical systems from remote, often untrusted, or less trusted environments. This includes cases such as remote access from a supplier or vendor. What controls can be explored to mitigate the risk from such third-party connections. How can the effectiveness of such controls be measured to provide assurance?

Research Institute – way of working

The successful projects will join the RITICS portfolio, with all project staff becoming community members. Representatives from the projects will be expected to attend the majority of the regular RITICS community meetings, workshops and/or conferences. The projects will be asked to present their progress at some of these meetings.

There will be the opportunity to engage directly with the NCSC during the course of the projects.

The projects will also be expected to supply brief progress reports each quarter, and an annual progress summary, via RITICS.

What should be in the proposal?

Each proposal must make it very clear how it addresses the challenge areas described above. Proposals should also include details of any planned engagement with 'real world' security.

The proposal should specifically address each of the following items:

- Background: An outline of the context of the research.
- Aim: A description of what understanding of the topic space the research is progressing and what potential impact it will have in practice.
- Relevance to the call: A description of which challenges the research addresses, and how it addresses them.
- Data: Whether the research is planning to create or make use of any specific datasets, and how they will be generated/handled.
- Field work: Whether the research will be carried out in any 'live' environments as opposed to lab based work. Details of the trials environments should be provided and the degree to which access has been agreed.
- Resources: An overview of the timescales, resources and structure of the research. A workplan should illustrate how these aspects combine to progress the research. The resources being used should be detailed, and CVs for named and visiting researchers included where these are known. Whether the research is planning to involve and draw on any expertise from within the security community should be described, including the nature and extent of the

engagement and the degree to which it has been agreed with the appropriate people/organisations in the security community.

- Method: An outline of how the research will be carried out, detailing techniques and approaches that intend to be used. An indication of the level of previous experience of these approaches should be included.

- Potential impact in practice: How the outcomes of the research will make a difference in a real-world setting.

Application submissions should be no more than eight sides of A4 and should include a breakdown of all costs involved, including equipment, travel & expenses etc. Proposals that attempt to engage with real-world partners are welcomed.

How will proposals be assessed?

Following eligibility checks, research proposals will be reviewed by an expert Assessment Panel comprising representatives from academia, industry, and HMG. The panel will produce a ranked list of proposals based on consensus scores.

The Assessment Panel will consider the following criteria:

- Quality – this will consider the method & concept for the proposed research, and its ability to move forward fundamental understanding within the field.

- Viability – this will assess how feasible the research is to carry out, eg whether the research concept is practicable to deliver. It will take into account the difficulty of the task, the logistical factors, and the track record of team.

- Significance – this will consider the research's potential impact on practice and its relevance to the Call. Note that the impact on practice does not have to be immediate. A long term, highly aspirational piece of research could produce a higher "Significance" score than a more tactical "applied" piece of work eg designed to produce an immediately usable tool. Neither does this preclude research which may have a 'negative' outcome, eg proving that a technique does not work. The proposal should outline the potential for transformative thought or progress within the cybersecurity profession, whether this be near or long term.

All three criteria will be equally weighted. However, "Significance" will have a minimum threshold, below which proposals will be rejected.

Key dates

Activity	**Date**
Call for Research Published	Mid July 2020
Proposals due to be submitted	Friday 11 September 2020
Announcement of results	Mid October 2020

Activity	Date
Research starts	1 April 2021
Research completed	31 March 2022

Funding available

This call will be funded by NCSC with an indicative budget of £0.5M over 12 months. The funding and contract will be under the NCSC's standard terms and conditions: a draft copy of the contract can be made available on request. The research will be funded at Full Economic Cost. Budgets for attendance at academic conferences to publicise and disseminate the work should be included within the research proposal. In addition to the travel budget for attending conferences, proposals should include adequate funding for travel between academic partners within the project, and to attend the regular Institute meetings.

The cross-disciplinary, exploratory and novel nature of the Institute is likely to require a significant commitment of time on the part of its permanent academic members.

The funders are committed to full and open publication of the research outputs of the Institute in line with normal academic practice.

The funding is available for Financial Year 2021/2022. Proposers should be ready to start activity on 1 April 2021 and must complete by 31 March 2022 latest; there will be no possibility for project extensions.

Both NCSC and RITICS believe that this is a broad scale research call, with the potential to offer significant transformative value. We will be campaigning for more attention to be given to this topic at a national scale and seeking additional sources of funding for further research from government and industry partners.

Eligibility

Applicants need to be based in institutions eligible to apply for EPSRC funding.

How to apply

Applications should be sent to Abby K, NCSC Research Office via email: researchoffice@ncsc.gov.uk. We must receive your application by **1600 on Friday 11th September 2020.**