BU STUDENTSHIPS 2023

PROJECT DESCRIPTION

PROJECT TITLE

Towards Productive Cyber Resilience and Safety Analysis in Model-Based System Engineering

PROJECT SUMMARY

Cyber resilience is an important system-level feature. It is affected by design trades made during the systems engineering process (e.g. the use of architectural dissimilarity in parallel control channels). These trades are likely to affect other system properties such as system security and safety, as well as programme schedule and cost.

Model-Based Systems Engineering (MBSE) is being increasingly used in critical systems to help manage system complexity. MBSE aims to transform Systems Engineering to a model-based practice and is a formalised application of modelling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later lifecycle phases (INCOSE, 2023). MBSE's use of models formalise descriptions of a system, allowing for automated analysis, in contrast to the historical approach of document-based engineering. MBSE is also seen as key to lowering the cost of defence platforms. For example, the Ministry of Defence's PYRAMID programme envisages simplifying upgrades, and reducing software development costs though a reusable and open mission system architecture, by using a suite of reusable software components for legacy and future air platforms (UK MoD PYRAMID, 2021).

MBSE artefacts should allow automated analyses to establish cyber resilience and system safety properties, alongside other system-level characteristics and programme features (e.g. schedule, cost). This integrated view should allow systems engineers to more fully understand the effects of design decisions. Elements of this theory have been demonstrated in small-scale trials and academic papers. However, to date, there is little empirical evidence that such approaches can scale to the necessary degree. Part of this scaling relates to the size (e.g. number of components) of the system model that is being considered. Another part relates to the manual effort associated with defining the automated analyses and assessing the associated results. The extent to which this analysis and assessment can be conducted by general systems engineers, rather than cyber (or safety) specialists is another key issue.

Applied empirical research, at an appropriate scale, on the integration of cyber resilience and system safety analysis into MBSE workflows would be highly useful. For example, action research to evaluate the creation and cyber resilience and safety analysis of representative system models, and the integration of analysis approaches and tooling into standard model-based systems engineering workflows. However, in isolation, this might not be sufficient to achieve widespread adoption of such techniques across the defence supply base. There may also be a need to evaluate how suitable techniques and tools can be promoted to facilitate their adoption, especially among key system integrators.

This project aims to improve the productivity of cyber resilience and safety analysis in programmes using MBSE. Its objectives are:

1. Identify challenges and opportunities associated with cyber resilience and safety analysis in MBSE analysis through a review of peer-reviewed literature and best practice in the Defence Science & Technology sector, and other cogent domains where MBSE is employed;
2. Identify the quality improvements that can be made to cyber resilience and safety analysis in MBSE through empirical research conducted with stakeholders and exemplar projects where MBSE is employed;
3. Develop prototype tools, techniques, and guidelines for improved cyber resilience and safety analysis in MBSE in collaboration with stakeholders and exemplar projects where MBSE is employed.
4. Conduct intervention-based empirical research to evaluate the effectiveness and impact of prototype tools, techniques and guidelines for improved cyber resilience and safety analysis in MBSE.

The project will be based around a number of exemplar cases to ensure relevance of the research and to enable

knowledge exchange and technology transition. To facilitate adoption of the research outputs by the broader defence community, evidence will be captured on the impact to productivity of theories, tools, techniques and guidelines resulting from this research.

ACADEMIC IMPACT

The PhD research work is timely and innovative dealing with important research objectives. There are at least four types of academic impact that will be achieved through this project:

1. Scientific output should be published in high-impact journals and conferences;
2. Networking: the candidate will collaborate with researchers from BU and The Defence Science and Technology Laboratory (Dstl);
3. Approach and platform: the project will deliver a model-based development demonstration in a relevant application;
4. Research roadmap: in collaboration with the sponsor, the project will identify future R&D activities required to transition the research into deployed systems.

SOCIETAL IMPACT

The actionable evidence-based guidance for safety and security analysis resulting from this PhD could have significant impact in the national and international defence sector and beyond. For example, we aim to apply the guidance and principles gleaned from the formative stages of this research in action research interventions on currently running projects. Where efficiencies lead to a reduction in the time and tax-payer money spent building and maintaining MBSE artifacts, this reduction will provide evidence of research impact. We also aim to share the results of our work with regulators responsible for assessing the airworthiness of air platforms, e.g. the Military Aviation Authority, with the aim of improving their accreditation practices, e.g. increasing the confidence in accreditation results while simultaneously reducing the associated costs.

PGR DEVELOPMENT OPPORTUNITIES

This project offers a very interesting learning and training opportunity for the candidate. Different subjects are involved in the project such as model-based development, systems engineering, software quality and testing, cyber security, etc. Issues like project planning and management will also be part of the learning process. The candidate will be exposed to the academic and industrial environments, having access to periodic secondments at Dstl (subject to security clearance). Dstl will support the student in understanding different applications of the technology developed, and will facilitate meetings with users of the technologies to help understand future applications.

While at BU, the candidate will receive research-based training. At Dstl, he/she will become familiar with research and development in the industrial setting, and will be given insights into the exploitation of the results of this project. The candidate will gain various skills, especially scientific skills, employability skills, and industrial experience from interacting with the industrial partners. Moreover, the candidate will have the opportunity to interact with local and international researchers. Last but not least, he/she will be expected to attend international conferences to present the research findings conducted during the project.

BU has various MSc programmes, including MSc in Data Science an AI, and MSc in Cyber Security and Human Factors. The candidate will have the opportunity to gain some applicable teaching and marking experience within the bounds permitted by the terms of the studentship.

The candidate will also have the opportunity to collaborate with the Defence BattleLab in Dorset to use their facilities and have access to expertise for test cases and running experimentations. There will be a secondment opportunity at the BattleLab due to existing collaborations between BU, Dstl, and BattleLab.

SUPERVISORY TEAM	
First Supervisor	Dr Huseyin Dogan
Additional Supervisors	Dr Cagatay Yucel, Dr Shamal Faily, Prof Keith Phalp
Recent publications by supervisors relevant to this project	Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2022. Assessing system of systems information security risk with OASoSIS. Computers and Security, 117. Ashmore, R., Howe, A., Chilton, R. and Faily, S., 2022, October. Programming Language Evaluation Criteria for Safety-Critical Software in the Air Domain. In 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (pp. 230-237). IEEE. Alrubaee, A.U., Cetinkaya, D., Liebchen, G. and Dogan, H., 2020. A process model for component-based model-driven software development. Information (Switzerland), 11 (6). Altaf, A., Faily, S., Dogan, H., Thron, E. and Mylonas, A., 2022. Integrated Design Framework for Facilitating Systems-Theoretic Process Analysis. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13106 LNCS, 58-73. Naseir, M.A.B., Dogan, H. and Apeh, E., 2021. Assessment of national cybersecurity capacity for countries in a transitional phase: The spring land case study. Frontiers in Artificial Intelligence and Applications, 341, 144-153. Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E., 2021. Use-Case Informed Task Analysis for Secure and Usable Design Solutions in Rail. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13139 LNCS, 168-185. Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E., 2020. Identifying safety and human factors issues in rail using IRIS and CAIRIS. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11980 LNCS, 98-107. Naseir, M.A.B., Dogan, H., Apeh, E. and Ali, R., 2020. National cybersecurity capacity building framework for countries in a transitional phase. ICEIS 2020 - Proceedings of the 22nd International Conference on Enterprise Information Systems, 2, 841-849. Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2018. Assessing system of systems security risk and requirements with oasosis. Proceedings - 2018 5th International Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE 2018, 14-20. Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2018. System of Systems Characterisation assisting Security Risk Assessment. In: IEEE 13th System of Systems Engineering Conference 19 June-22 April 2018 Paris, France. IEEE.

INFORMAL ENQUIRIES
Please contact the lead supervisor on the following email for informal enquiries: hdogan@bournemouth.ac.uk
ELIGIBILITY CRITERIA
The BU PhD Studentships are open to UK, EU and International students. Candidates for a PhD Studentship should demonstrate outstanding qualities and be motivated to complete a PhD in

4 years and must demonstrate:

- outstanding academic potential as measured normally by either a 1st class honours degree (or equivalent Grade Point Average (GPA) or a Master's degree with distinction or equivalent
- an IELTS (Academic) score of 6.5 minimum (with a minimum 6.0 in each component, or equivalent) for candidates for whom English is not their first language and this must be evidenced at point of application.

HOW TO APPLY

Please complete the online application form by **the deadline on the project webpage.**

Further information on the application process can be found at: www.bournemouth.ac.uk/studentships