Physics-Informed Data-Driven Techniques for Secure and Safe Autonomous Systems

Main supervisor: Dr Amy Nejati (amy.nejati@newcastle.ac.uk)

Summary. The central vision of this project is to pioneer groundbreaking advances in the data-driven techniques that offer mathematical confidences for verifying and designing secure and safe autonomous systems (AS). As complex real-world applications expand, distributed physical systems increasingly interact with computational components, all functioning within uncertain environments. This interaction between the cyber components and the physical environment in AS can lead to information leaks, putting system security at risk. Consequently, it is essential to address both security and safety simultaneously. The modern applications exemplify AS and play a crucial role across diverse industries, especially within safety-security-critical systems such as intelligent transportation systems, robotics, biological networks, and automated manufacturing systems.

Data-Driven Techniques. Accurately capturing the behaviour of AS through mathematical models requires detailed representations of every component. However, in systems with thousands of components and interacting software elements, this complexity *grows exponentially*, making the construction of precise models extremely challenging. This underscores the urgent need for data-driven methods that employ input-output measurements for verification and synthesis purposes.

Objective and Vision. This project aims to pioneer advances in integrating fundamental physical principles into data-driven techniques to substantially reduce the data required to ensure high-confidence security and safety for AS. In fact, while mathematical models are often imprecise in practice, they can still provide valuable insights that can be combined with data-driven methods [1]. This integration enables effective formal analysis of AS using a smaller dataset that still captures the essential behaviour of the system. The specific objectives of this project include:

- **Integrating physical principles:** Develop methodologies to incorporate fundamental physical principles into data-driven techniques, enhancing the robustness and adaptability of AS for real-world applications with less amount of data.
- **Offering high confidence:** Develop data-driven approaches that offer provable security and safety guarantees for AS with higher confidence.

Broader Impacts. This project addresses critical national priorities by advancing the safety and security of autonomous systems, which underpin transformative technologies in areas such as intelligent transportation, healthcare, and automated manufacturing. By integrating physics-informed approaches with data-driven techniques, the research aligns with the UK's long-term strategies for digitalisation and innovation, such as the UK Government's Industrial Strategy and its focus on AI and data-driven economy. The proposed work contributes to the resilience

of safety-critical systems operating under uncertainty, ensuring their robustness in real-world scenarios. Furthermore, by reducing the reliance on extensive datasets, the outcomes will enhance the scalability and adaptability of AS across multiple sectors, promoting economic growth and societal wellbeing. This research has the potential to establish the UK as a global

leader in developing secure, reliable, and efficient autonomous technologies, fostering collaborations between academia and industry to tackle pressing challenges in digital transformation and cybersecurity.

Methodology. We will utilise methodologies from formal methods, data science, and control theory to develop data-driven techniques leveraging fundamental physical principles. In particular, we will aim to enhance the performance of AI-based approaches by leveraging data-driven methods, such as scenario-based techniques, alongside machine learning methods utilising neural networks (NN). By integrating fundamental physical principles, we aim to provide high confidences over the AS correctness with significantly reduced data requirements.

Project Timeline

Year 1. Literature review on formal methods techniques for the safety and security properties, data-driven analysis of AS; embedding the candidate into the research topic

Year 2. Investigating scenario approaches; writing the first paper on the developed methodologies; visit from The University of Oxford due to having collaborations with Prof. Alessandro Abate

Year 3. Investigating NN methods; writing the second paper on the newly developed methodologies; participating in relevant workshops and conferences; visiting Co Wheels (https://www.co-wheels.org.uk/) as the project's industrial collaborator to explore applying the results to some vehicles.

Year 4. Writing a journal paper on the developed methodologies; thesis write up and viva

Supervision Environment

This interdisciplinary project will draw upon expertise in control theory and data-driven methods (Dr Amy Nejati) and formal methods and large-scale networks (Dr Abolfazl Lavaei). We have agreed on external collaborations with both academia and industry for this project, involving experts in safety-critical systems from the University of Oxford (Prof. Alessandro Abate - https://scholar.google.co.uk/citations?user=yskbfM4AAAAJ&hl=en) and an industrial partnership with Co Wheels (https://www.co-wheels.org.uk/), contributing 35% in-kind support.

Applicant skills/Background

Potential candidates should have background in one of the following areas: Computer Science, Artificial Intelligence, Data Science, Systems and Control, or a closely related field.

Reference

[1] A. Aminzadeh, M. Ashoori, **A. Nejati,** and A. Lavaei, A Physics-Informed Scenario Approach with Data Mitigation for Safety Verification of Nonlinear Systems, *submitted for publication*, 2024.