

Department	School of Computing
Supervisors	Dr Naghmeh Moradpoor, Prof. Berk Canberk, Dr Keng Goh, Dr Brian Davison
Project Title	Cyber Digital Twin for Clean Water Treatment Systems

PROJECT DESCRIPTION

Most organisations/companies use bug bounty hunting programs to identify and then fix security vulnerabilities in their systems. Bounty hunters, in return for a reward, address cybersecurity flaws faced by organisations/companies before criminals/state-sponsored hackers exploit them. However, these programs do not fit Critical National Infrastructures such as clean water services given the nature of the program and the sensitivity of these systems. Nations are highly dependent on the operation and continuity of CNI therefore any failure/damage to them and/or their services will disturb day-to-day activities. Addressing this challenge will unlock a vast number of opportunities for cyber defenders.

This project is inspired by Digital Twin or digital clone for Cyber Physical Systems, which is an evolving field of research, and aims to produce a cyber replica of a real physical system. Digital Twin has been considered as a feasible digital platform due to its ability to simulate use case scenarios without directly operating on real physical systems. It has been employed for several Cyber Physical Systems (e.g., smart transportation), however, this does not cover water services. Additionally, the use of Digital Twin to mitigate two-way and realtime monitoring of cyberattacks against its real counterparts has not been well studied. Furthermore, this work proposes to move away from using Information Technology security paradigm (e.g., security of Cloud) to Operational Technology security (e.g., security of machinery) by the direct monitoring of hacker's behaviour in Digital Twin. Therefore, our proposed work leverages the recent progress in Digital Twin for Cyber Physical Systems with a particular focus on 1) water services, 2) use of Digital Twin for cyberattack mitigation of Cyber Physical Systems, and 3) Operational Technology security. This project puts the system admin a step ahead of the hackers regarding the protection/hardening of their systems.

This work will consider our ongoing work on cybersecurity of Industrial Control System and Critical National Infrastructure. It will be based on our existing MPS Filtration System, which is representing a scaled-down version of a one-of-a-kind water treatment system, and will be linked to simulations to produce a cyber replica of such a system.

Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.

Academic qualifications

A first degree (at least a 2.1) ideally in automation & control, industry 4.0, cybersecurity with a good fundamental knowledge of simulation tools like Ansys, Anylogic, Matworks Simulink, Labview, programming languages like Python, R OR cybersecurity.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. [Full details of the University's policy](#) are available online.

Essential attributes:

- Experience of fundamental cybersecurity
- Competent in software development and algorithmic design

- Knowledge of /interest in application of machine learning, Programmable Logic Control (PLC), critical national infrastructure protection
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

Knowledge of water services (e.g., clean water supply systems and/or clean water treatment systems)

Indicative Bibliography	<p>Robles-Durazno, A., Moradpoor, N., McWhinnie, J., Russell, G., & Tan, Z. (2021). Newly engineered energy-based features for supervised anomaly detection in a physical model of a water supply system. <i>Ad Hoc Networks</i>, 120, 102590.</p> <p>Barricelli, B. R., Casiraghi, E., & Fogli, D. (2019). A survey on digital twin: Definitions, characteristics, applications, and design implications. <i>IEEE access</i>, 7, 167653-167671.</p> <p>Homay, A., Chrysoulas, C., El Boudani, B., de Sousa, M., & Wollschlaeger, M. (2021). A security and authentication layer for SCADA/DCS applications. <i>Microprocessors and Microsystems</i>, 87, 103479.</p>
Enquiries	For informal enquiries about this PhD project, please contact Dr Naghmeh Moradpoor (n.moradpoor@napier.ac.uk)
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process