# SUMMER RESEARCH 2024/25
# PROJECT ABSTRACT

THE UNIVERSITY OF WAIKATO
*Te Whare Wānanga o Waikato*

## PROJECT # 23

| | |
|---|---|
| **SUPERVISOR/S:** | Dr Farzana Zahid & Dr Vimal Kumar |
| **PROJECT TITLE:** | Analysing ICS-Specific Malware |
| **FIELD:** | Cybersecurity |
| **DIVISION/SCHOOL:** | HECS - Au Reikura School of Computing and Mathematical Sciences |
| **PROJECT LOCATION:** | Both Hamilton and Tauranga |

### PROJECT ABSTRACT:

An industrial control system (ICS), an integral part of the critical infrastructure, is responsible for the real-time control and monitoring of industrial operations. Increased automation and connectivity among various components of ICS have brought tangible benefits, including economic stability, public safety, and business continuity. Digitisation and connectivity, on the other hand, have also created new entry points for cyber-attacks targeting ICS, specifically using malware. ICS-specific malware are increasing in frequency and sophistication, evident by threats like Triton and PIPEDREAM. In this project, we will investigate ICS-specific malware to gain insight into their behavior, structure, and capabilities. These insights will further help us to understand the attack vectors, propagation methods, and exploitation techniques used by such malware, which can be used to devise appropriate countermeasures against the analysed malware. This project can be continued further as honours or master's thesis/dissertation work.

### STUDENT SKILLS:

- Knowledge of cybersecurity (Preferably would have taken COMPX519).
- Working knowledge of a programming language (no preferences).

### PROJECT TASKS:

1. Collect appropriate ICS malware samples using publicly available malware repositories like Malware Zoo, Malware Bazaar or Virus Total.
2. Set up a safe and secure analysis environment.
3. Performing a literature review of malware analysis techniques/frameworks.
4. Analyse malware in accordance with MITRE and other frameworks.
5. Prepare the poster and a brief report with the analysis and methodology.

### EXPECTED OUTCOMES:

- Student's Research Poster (as per clause 6 of the Scholarship regulations)
- Student's Research Poster (as per clause 6 of the Scholarship regulations).
- Collection of ICS malware samples from publicly available malware repositories and set up of a safe malware analysis environment.
- Mapping of malware analysis techniques and framework on STRIDE framework.