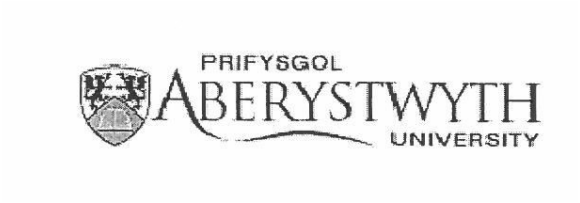

This summary sheet should be completed after you have read the guidance notes. The complete sheet should be submitted by you to your Department/School/Institute at the time of submission of your work and the supporting documentation.

Candidate's Surname/ Family Name:	Scully	
Candidate's Forenames:	Peter Matthew David	
Candidate for the Degree of	PhD	(PhD, MPhil, LLM(Res) etc)
Full title of thesis:	CARDINAL-Vanilla: Immune System Inspired Prioritisation and Distribution of Security Information for Industrial Networks	

Summary:

This thesis has made advances in Distributed Self-Healing Security Systems (DSHSS) -- a tool for the future to defend against the problems faced by industrial automation computer networks, such as critical national infrastructure (CNI), Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA), caused by computer malware and cyber attacks (Ch.2).

Based on principles of an holistic view of the biological immune system (Ch.3) and recent Artificial Immune System (AIS) research (Ch.4), CARDINAL-Vanilla -- a self-healing and collaborative host-based security architecture has been designed (Ch.5) for application into real-world ICS and SCADA networks. Using a novel evaluation framework for DSHSS (Ch.6) the architecture has been assessed by 'immunisation rate' scores, to measure self-healing performance and resource feasibility, under rigorous virtual and real-world enterprise networks experiment conditions.

These empirical studies (Ch.7 and Ch.8) identified that the CARDINAL-Vanilla module dispatch algorithm scores significantly worse than a near-optimal engineered dispatch algorithm; however the performance score difference is not important for a real-life application. In addition, the engineered dispatch algorithm is impossible to apply directly to real-world systems. The dispatch heuristics of CARDINAL-Vanilla are interesting to apply if the mult-agent system architecture's memory overhead can be reduced to and modelled as mathematical approximate equations.

A comprehensive theoretical DSHSS architecture (Ch.9) to address the cyber attack problems identified (Ch.2) using a reinforcement classification pipeline, role switching and additional hardware to integrate into industrial networks is proposed as the future theme for DSHSS.