SCADA Test Environment for Cybersecurity Analysis of Critical Infrastructure Systems

Sponsor – School of Mechanical and Electrical Engineering

Peter Compton

Bachelor of Engineering

Bachelor of IT

Supervisor: Dr Tobias Low, USQ

Keywords: SCADA, Control Systems and Cyber Security.

1. Introduction

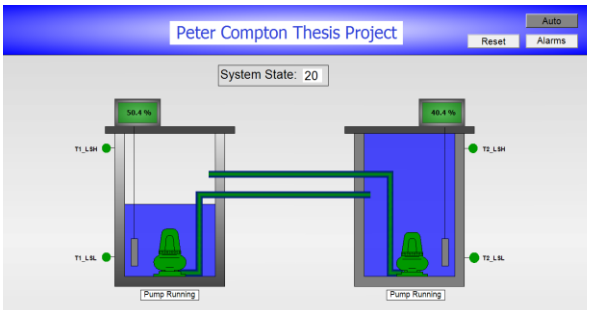
Critical infrastructure systems around the world are currently being controlled by out of date, un-secure computer systems that are vulnerable to various malware attacks. The primary purpose of this project is to highlight the potential risks that industrial control systems are exposed to, through the design of a small-scale control system. By utilising cyber security testing techniques, it is expected that this project will provide insight into what dangers exist in these systems and how they can be potentially mitigated.

2. Background

Throughout history there have been numerous examples of critical systems being brought down due to malware. Some of these attacks include the infamous Stuxnet attack, Russian attacks on Ukraine's Electricity Grid and the recent attacks on a Florida water treatment facility. However, with proper system design and testing, it is possible to mitigate the risk posed by malicious software and prevent malicious agents from impacting our critical assets.

3. Methodology

There were a broad range of tasks required to accomplish the outcomes of this project. A functional description was prepared to describe the control system operation and outline the system equipment. Software, electrical and networking components were then designed and built which included an electrical control panel, PLC programming, SCADA system interface development, and the controlled process. Figure 1 details the SCADA overview page that was developed for this system. The system was then tested using standard penetration testing techniques utilising the Kali Linux operating system distribution to analyse security of the system.



Peter Compton Thesis Project

System State: 20

Figure 1 – SCADA Overview Page

4. Key Outcomes

A fully functional control system has been successfully designed and built. The control system meets the requirements of the fucntional specification and can be ran fully autonomously. Testing of the system is well underway with interesting insights into the vulnerability a typical system has to cyber attacks.

5. Further Work

The project is approaching completeness, with only final exploitation testing remaining and the analysis of the testing data.

6. Conclusions

This project successfully highlighted the vulnerabilities present in typical control systems and how they can be exposed. The project has also identified the frighteningly large amount of system data that is available to people with the right software tools. Thankfully, a major insight that came from this project, is that it is quite simple to secure a system. If software is kept up to date and user policies are kept strict, it makes it quite hard to gain unauthorised access to a system.

Acknowledgements

I would like to thank my wonderful wife and children for putting up with my study for the past six years and allowing me to turn our back room into a control room. Without their support I would never have got to where I am now.

References

Chen, T. M. & Abu-Nimeh, S. (2011), 'Lessons from Stuxnet', Computer 44(4), 91–93

Highland, H. J. (1988), 'The brain virus: Fact and fantasy', Computers and Security 7(4).

Verma, A., M.S.Rao, A.K.Gupta, Jeberson, W. & Singh, V. (2013), 'A literature review on malware and its analysis', IJCRR 5(16).