PLC Code Vulnerabilities Through SCADA Systems

Sidney Valentine

Abstract

Supervisory Control and Data Acquisition (SCADA) systems are widely used in automated manufacturing and in all areas of our nation's infrastructure. Applications range from chemical processes and water treatment facilities to oil and gas production and electric power generation and distribution. Current research on SCADA system security focuses on the primary SCADA components and targets network centric attacks. Security risks via attacks against the peripheral devices such as the Programmable Logic Controllers (PLCs) have not been sufficiently addressed.

Our research results address the need to develop PLC applications that are correct, safe and secure. This research provides an analysis of software safety and security threats. We develop countermeasures that are compatible with the existing PLC technologies. We study both intentional and unintentional software errors and propose methods to prevent them. The main contributions of this dissertation are:

- Develop a taxonomy of software errors and attacks in ladder logic
- Model ladder logic vulnerabilities
- Develop security design patterns to avoid software vulnerabilities and incorrect practices
- Implement a proof of concept static analysis tool which detects the vulnerabilities in the PLC code and recommend corresponding design patterns.