Computers
& Security
The International Source of Innovation for the Information Security and IT Audit Professional
ifip

OpenPLC: An IEC 61131-3 Compliant Open Source Industrial Controller for Cyber Security Research

Thiago Alves , Thomas Morris

PII: S0167-4048(18)30538-8
DOI: 10.1016/j.cose.2018.07.007
Reference: COSE 1369

To appear in: *Computers & Security*

Received date: 9 August 2017
Revised date: 5 July 2018
Accepted date: 15 July 2018

Please cite this article as: Thiago Alves , Thomas Morris , OpenPLC: An IEC 61131-3 Compliant Open Source Industrial Controller for Cyber Security Research, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.07.007

OpenPLC: An IEC 61131-3 Compliant Open Source Industrial Controller for Cyber Security Research

Thiago Alves
Electrical and Computer Engineering
The University of Alabama in Huntsville
USA
thiago.alves@uah.edu

Thomas Morris
Electrical and Computer Engineering
The University of Alabama in Huntsville
USA
tommy.morris@uah.edu

ABSTRACT

The last decade has seen multiple instances of cyber-attacks that have been successful in sabotaging the normal operation of SCADA systems and PLCs. To counter these attacks, researchers have put their efforts in finding defense mechanisms that can protect the network and the PLC. However, since vendors don't make available information about the hardware and firmware of their devices, it becomes challenging to perform cyber security research for PLCs. This work proposes the development of an open source PLC, compliant with the IEC 61131-3 international standard. A description of the hardware architecture, development environment, supported SCADA protocols and an additional HMI editor package is presented. Additionally, this work presents a methodology for validating PLC logic execution, performance, and SCADA connectivity, and also compares the behavior of OpenPLC with four other popular commercial PLCs when under a Modbus injection attack, to support the claim that OpenPLC is a valid platform for PLC cyber security research.

Keywords

PLC, SCADA, ICS, Cybersecurity, Vulnerability Analysis, OpenPLC, MODBUS, HMI.

1. INTRODUCTION

The closed industrial environment hides key information related to the development of technology behind patents, copyrights, and trademarks. While it is debatable how intellectual property rights of inventors must be saved from abuse, traditional modes of doing so can block the flow of information for scientific research. Since 1968, when the first Programmable Logic Controller (PLC) was invented, vendors have been developing their own proprietary hardware and software solutions targeting the industrial environment. Recently, with the advance of communication networks and the Internet, these systems have become vulnerable to a wide range of cyber-attacks. Given that PLCs are also used on critical infrastructure such as electric energy systems, nuclear energy systems, water and sewage treatment plants, gas/oil energy systems, and transportation systems, attacks on those systems can lead to catastrophic consequences for the nation. The work put forth by Alcaraz [1] identifies 5 requirements of Critical Control Systems that, if tampered, can cause impact on services, resources, operational control and sensitive information of the control system environment.

To counter these attacks, researchers have put their efforts in finding defense mechanisms that can protect the Supervisory Control and Data Acquisition (SCADA) network and the PLCs. The literature is rich in providing information about vulnerabilities and threats of SCADA systems. Alcatraz [2] [3] explore vulnerabilities and threats on SCADA systems and propose protection mechanisms on 4 areas: governance (security policies and standards), robust network design, self-healing, and modeling and simulation. Rautmare [4] identifies some threat vectors on the SCADA environment and addresses them with good network and operational security practices.

However, since vendors don't make available information about the hardware and firmware of their PLC devices, it becomes challenging to perform cyber security research for PLCs, usually having to rely on vendors to provide any security update.

Open source technologies can change this paradigm. The term "open source" refers to technology with a publicly accessible design that can be modified as desired without any restriction. By infusing open source tools into research, the results can be experimented and verified by a large number of people. The OpenPLC platform put forth in this paper is designed to specifically address this issue. Hence the main contribution of this work is the development of an open source PLC platform, that includes a program development environment, supports popular SCADA protocols such as Modbus/TCP [5] and DNP3 [6], and also includes an open source Human Machine Interface (HMI) editor called ScadaBR. The OpenPLC project was created in accordance with the IEC 61131-3 standard [7], which defines the basic software architecture and programming languages for PLCs. This means that OpenPLC can be programmed in any of the five standardized