SCADA

(Supervisory Control and Data Acquisition)

Amanda Cicilato

Northern Melbourne Institute of TAFE Waterdale Rd, Heidelberg, Australia
amanda.cicilato@gmail.com

Abstract: SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world.

Keywords: TCP/IP Stack

Introduction:

Programmable Logic Controllers (PLCs) are common in some industrial applications (especially discrete manufacturing) and increasingly have network interfaces which support Ethernet and TCP/IP protocols as well as more traditional communication interfaces such as MODBUS, DeviceNet, ContrlNet, Foundation Fieldbus, etc.

As is the case with any network device, different vendors implement their own shells on telnet and support various FTP commands, depending on their application requirements. The Ethernet communication module of the PLC typically runs an embedded operating system that includes standard network protocol as well as implementations of industrial network protocols such as Modbus/TCP or EtherNet/IP. For example, telnet and FTP servers are common and have identifying information which can be used to determine the vendor and version of software. Even on the industrial protocol side, we saw that not all PLCs support all commands of a given industrial protocol, so that implementations can be fingerprinted. Depending on the type (and capabilities) of the device there may be slight differences in the protocol.

All of these characteristics make it possible for attackers to identify specific versions and vendors of device and allow us to be able simulate the devices as well.

The term SCADA usually refers to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas (anything from an industrial plant to a nation). Most control actions are performed automatically by RTUs or by PLCs. Host control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process, but the SCADA system may allow operators to change the set points for the flow, and enable alarm conditions, such as loss of flow and high temperature, to be displayed and recorded. The feedback control loop passes through the RTU or PLC, while the SCADA system monitors the overall performance of the loop.

Implementation Approach

We followed the following approach when simulating a PLC:
Implement the generic features so that users can easily change them, add new features and re-submit them
The feature implementation should be so that the code will serve as examples for the users to change it according to their own needs.
Once the users submit enough code for more implementations, we visualize putting them into templates so that a generic configurable engine can load them according to a defined configuration

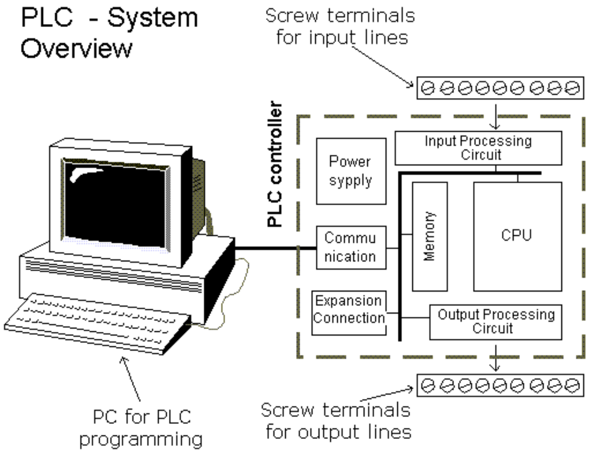

Figure showing plc system overview

Components Needed

The following are the network components in a PLC that need to be simulated:

- The TCP/IP Stack of the PLC
- The simulation of the Modbus/TCP server implementation.
- The simulation of the FTP server, that is found on some PLCs.
- The simulation of the Telnetd server, that may be found on some PLCs.
- The simulation of the management HTTP server, which increasingly common on PLCs and other industrial network devices

A feature called Sniff Subrating extends battery life by reducing the active duty cycle of Bluetooth devices like keyboards and mice to improve battery life. Bluetooth hosts can specify maximum transmit and receive latencies so that low-power devices can know how often they must exit and re-enter "sniff mode." This can result in up to five times the battery life experienced by older low-power Bluetooth devices.

Human–machine interface:
There is a difference between a user interface and an operator interface or a human–machine interface.
The term "user interface" is often used in the context of (personal) computer systems and electronic devices
Where a network of equipment or computers are interlinked through an MES (Manufacturing Execution System)-or Host to display information.
An HMI is typically local to one machine or piece of equipment, and is the interface method between the human and the equipment/machine. An Operator interface is the interface method by which multiple equipment that are linked by a host control system is accessed or controlled.[clarification needed]
The system may expose several user interfaces to serve different kinds of users. For example, a computerized library database might provide two user interfaces, one for library patrons (limited set of functions, optimized for ease of use) and the other for library personnel (wide set of functions, optimized for efficiency).

The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram. This means that the operator can see a schematic representation of the plant being controlled. For example, a picture of a pump connected to a pipe can show the operator that the pump is running and how much fluid it is pumping through the pipe at the moment. The operator can then switch the pump off. The HMI software will show the flow rate of the fluid in the pipe decrease in real time. Mimic diagrams may consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols.

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface.

References:

1. Basic SCADA Animations
2. Introduction to Industrial Control Networks". IEEE Communications Surveys and Tutorials. 2012.
3. Bergan, Christian (August 2011). "Demystifying Satellite for the Smart Grid: Four Common Misconceptions". Electric Light & Power. Utility Automation & Engineering T&D (Tulsa, OK: PennWell) 16 (8). Four. Retrieved 2 May 2012.
4. S (October 2004). "Supervisory Control and Data Acquisition (SCADA) Systems". NATIONAL COMMUNICATIONS SYSTEM.
5. Scadahoneynet.sourceforge.net/plc
6. Whatis.techtarget.com/definition/Bluetooth-20EDR
7. Wikipedia.org/wiki/scada