Descubriendo Controladores Lógicos Programables en una Red Universitaria

Héctor Fabio Jiménez Saldarriaga
Universidad Tecnológica de Pereira,
Ingeniería de Sistemas y Computación,
Pereira Security Team

Sebastian Zapata Ruiz
Universidad Tecnológica de Pereira,
Ingeniería de Sistemas y Computación

El uso de los dispositivos electrónicos como los controladores lógicos programables en el campo de la automatización y el control de procesos tienen un rol importante, estos se implementan en muchos campos, e industrias donde los procesos de producción y administración son complicados, críticos y peligrosos tanto económicamente como para la vida humana. En este artículo evidenciamos cómo es posible realizar el descubrimiento de estos dispositivos en un entorno controlado que presenta múltiples PLC's, Computadores de Monitoreo corriendo bajo sistemas operativos Windows, en una infraestructura universitaria.

Keywords: Redes Industriales , Seguridad Informática, Controladores Lógicos

Introducción

Los controladores lógicos programables (*Programmable logic controller*, de ahora en adelante PLC) fueron diseños en los años 60s[Ref1, Segovia] cuando el control de las maquinas industriales se hacía mediante el uso de relés, en ese entonces era tedioso y complicado para un técnico encontrar una falla en el sistema eléctrico de control debido a que todo los procesos se encontraban en cuartos llenos de una gran cantidad de cables y relés, lo que dificultaba la búsqueda. Con la llegada de los PLCs se resolvió el problema de la flexibilidad y solución de problemas comunes; estos reemplazaron decenas de cuartos en pocos, albergando bloques compactos de PLC, con ventajas como fácil mantenimiento, fácil instalación, fácil expansión. Su labor principal es la regulación los actuadores electromecánicos, como pueden ser válvulas, sensores, bombas, motores, etc.

Los sistemas de control utilizan como uno de los componentes a los PLCs para regular procesos industriales ejemplos de estas tareas de producción química, líneas de ensamblaje y manufactura, maniobra de maquinaria pesada, control y manejo de señales, control de mezclas, control de generación y despacho eléctrico entre otros. En un principio de estos dispositivos se presenta cada PLC como controlador individual e independiente, pero con el crecimiento y demanda de los procesos se requería tener conexiones con otros PLCs, lo cual solo funcionaba en un contexto local, sin conexiones a una red corporativa o internet (Ref ENISA, Protecting Industrial Control Systems). En los últimos 15 años con la globalización y la descentralización de las empresas que administran estos procesos se vuelve necesario tener que conectar estos dispositivos mediante enlaces privados e infraestructura pública como internet.

Una parte esencial de los sistemas de control industrial (*Industrial Control System*, de ahora en adelante ICS) son los sistemas SCADA (*Supervisory Control and Data Acquisition*,), los cuales son responsables de obtener información relevante y basados en el análisis de esta información enviar instrucciones a los sistemas de producción. Los sistemas SCADA necesitan estar conectados en varias ubicaciones topológicas dentro del sistema de control industrial por ejemplo con los PLCs, donde este tipo de conexiones se basa en tecnologías estándar, para la gran mayoría de sistemas SCADA los datos se encuentra encapsulados en TCP/IP y transmitidos vía Ethernet o en la capa de enlace como lo menciona Knapp[RefKnaapp].

Sistemas de Control Industrial (SCI)

Los sistemas de control industrial se encuentran segmentados

Sistema SCADA y Protocolos

Texto aqui.

Problemas Generales de Seguridad en un SCI

Texto aqui.

Configuración del Análisis de Seguridad

Texto aqui.

Posibles Ataques

Texto aqui.

Resultados

Texto aqui.

Texto aqui.

Conclusiones

Texto aqui.

Sample subsubsection. Texto aqui. Ejemplo de Tabla Latex.