

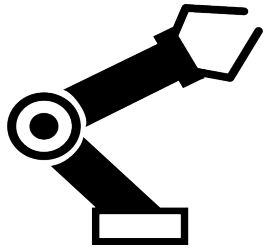
Análisis de vulnerabilidades y securización de protocolo Modbus/TCP

Ibai Marcos Cincunegui

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Curso 2017-2018

Director: Ricardo J. Rodríguez

Ponente: José Merseguer



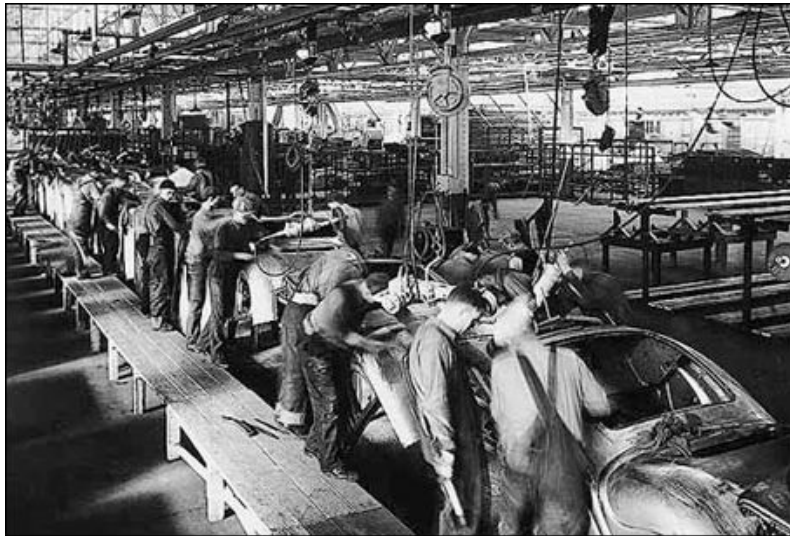
PLC



EQUIPOS DE CONTROL



SCADA



Modbus/RTU



Modbus/TCP

(IN)SEGURIDAD



PROBLEMAS



SERVICIO 24/7



MUESTRAS



SIMULACIÓN



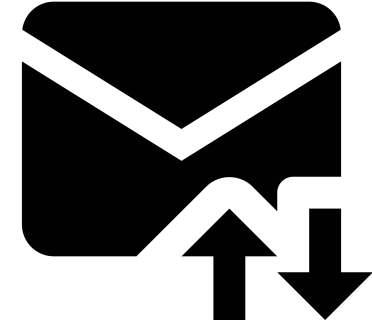
ARQUITECTURA



CAPA APLICACIÓN

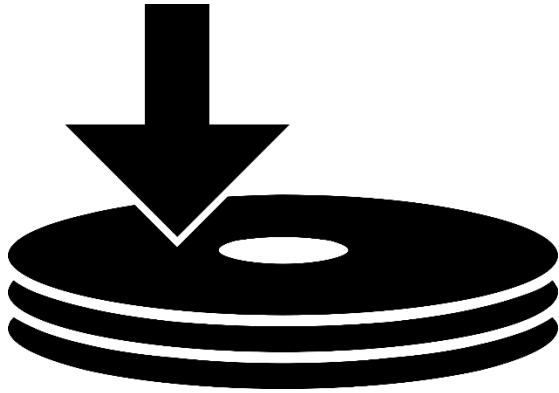


CLIENTE/SERVIDOR

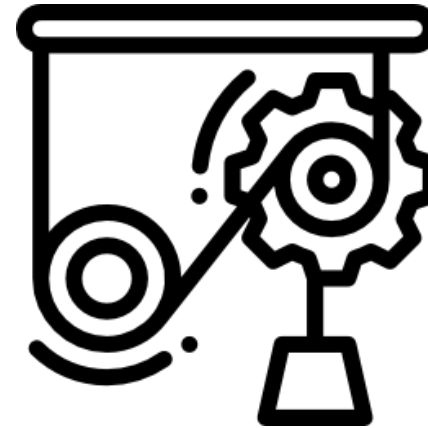


PASO DE MENSAJES

OPERACIONES

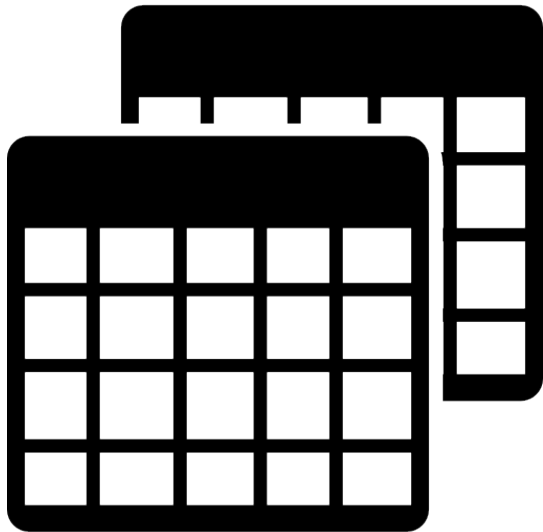


LECTURA-ESCRITURA



OPERACIONES MECÁNICAS

TABLAS DE DATOS

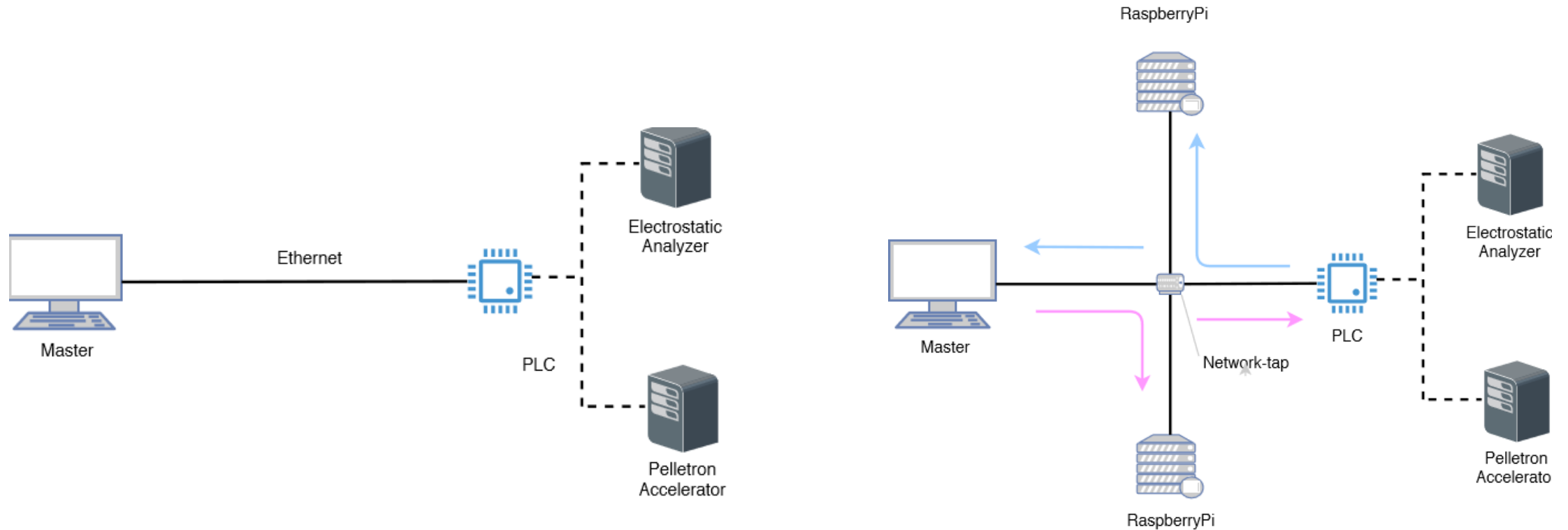


- ✓ COILS
- ✓ SINGLE INPUTS
- ✓ INPUT REGISTERS
- ✓ HOLDING REGISTERS

CIRCE

Center for **I**sotopic **R**esearch on **C**ultural and
Environmental heritage

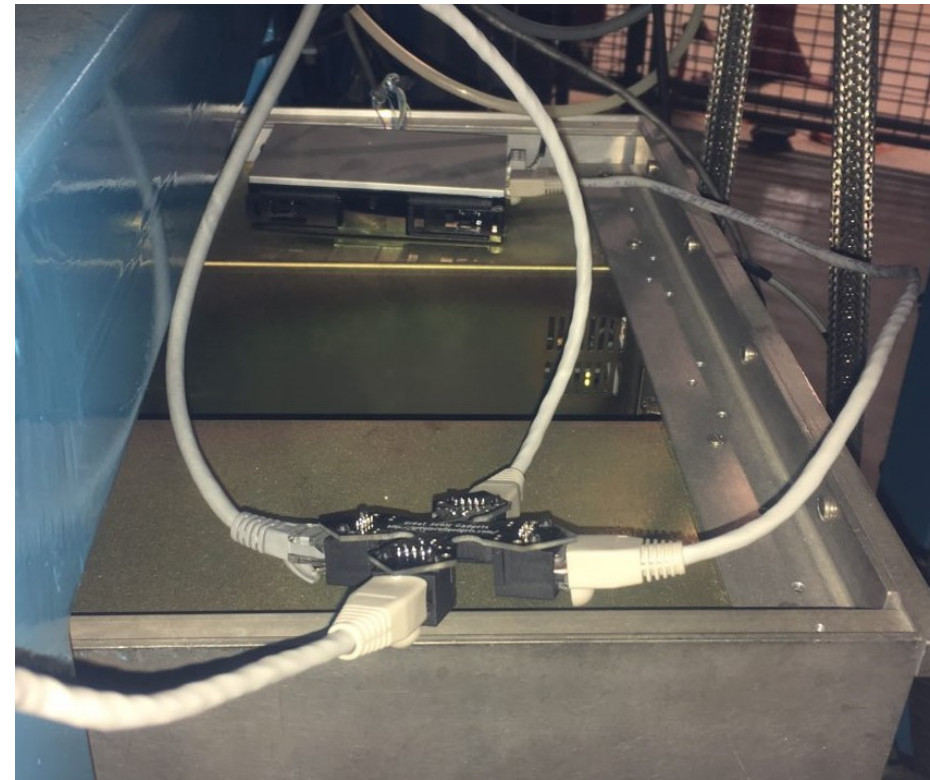
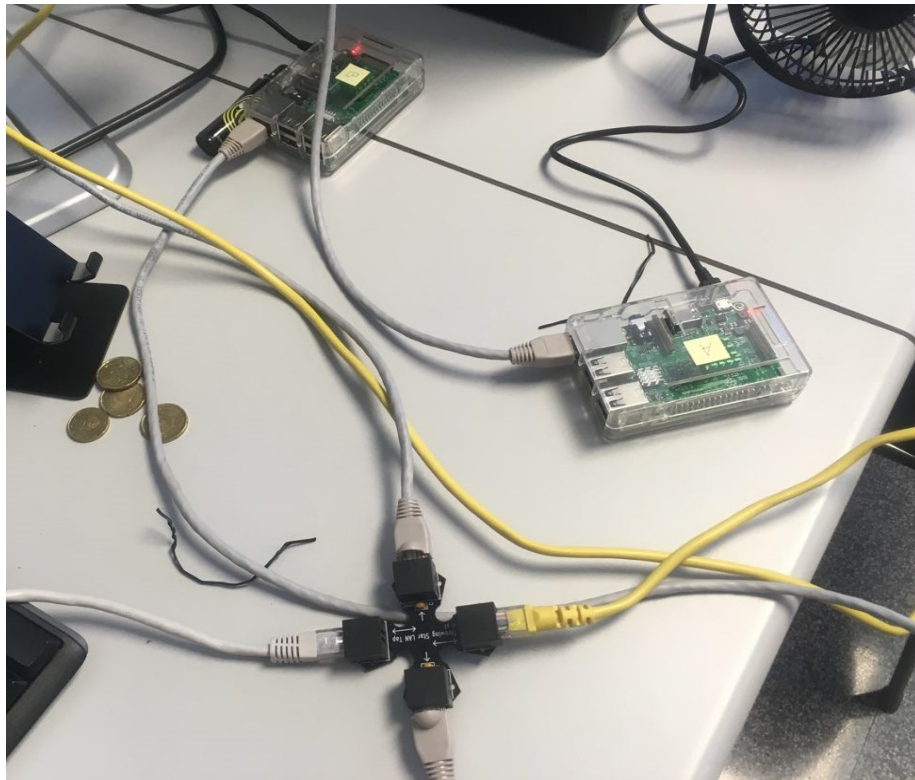
ENTORNO DE EXPERIMENTACIÓN



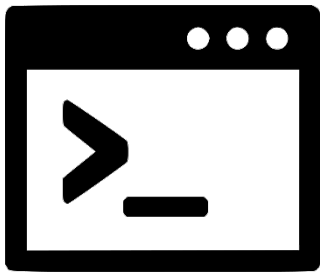
ENTORNO DE EXPERIMENTACIÓN



ENTORNO DE EXPERIMENTACIÓN



PROCESADO DE DATOS



INYECCIÓN DE TRÁFICO

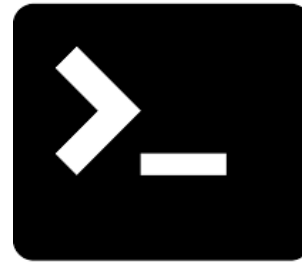


PROCESADO DE CAPTURAS

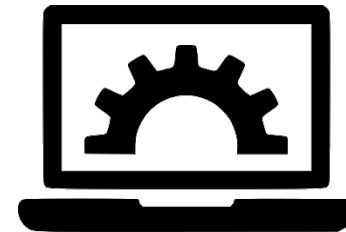


PARAMETRIZACIÓN

SIMULADORES

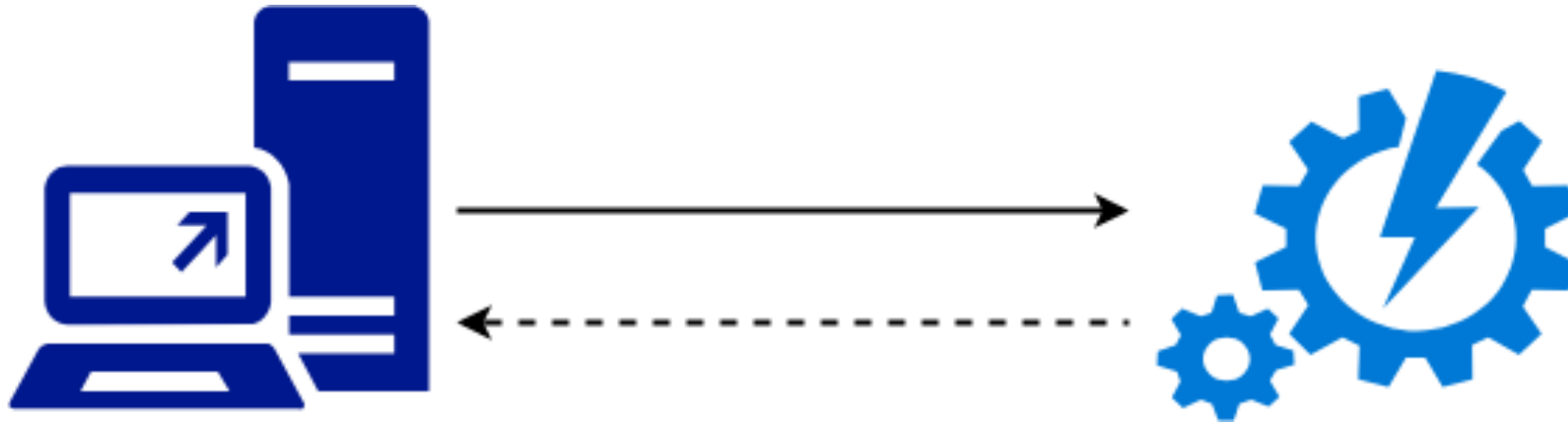


INTERFAZ



CONFIGURABLE

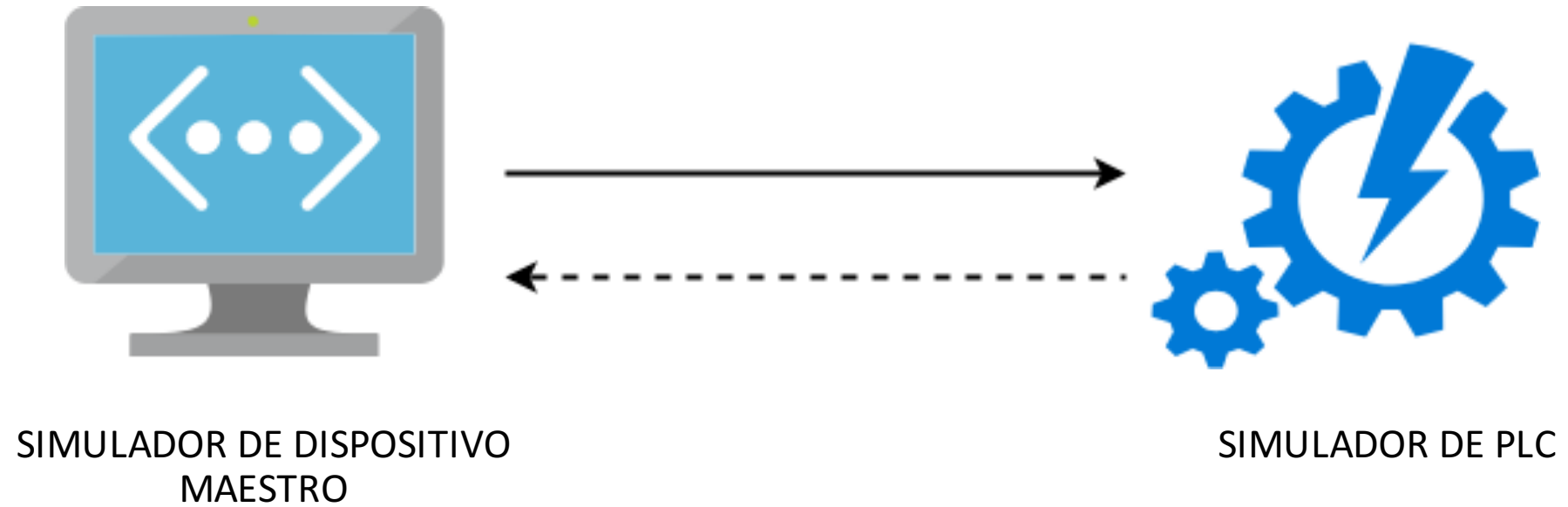
VALIDACIONES



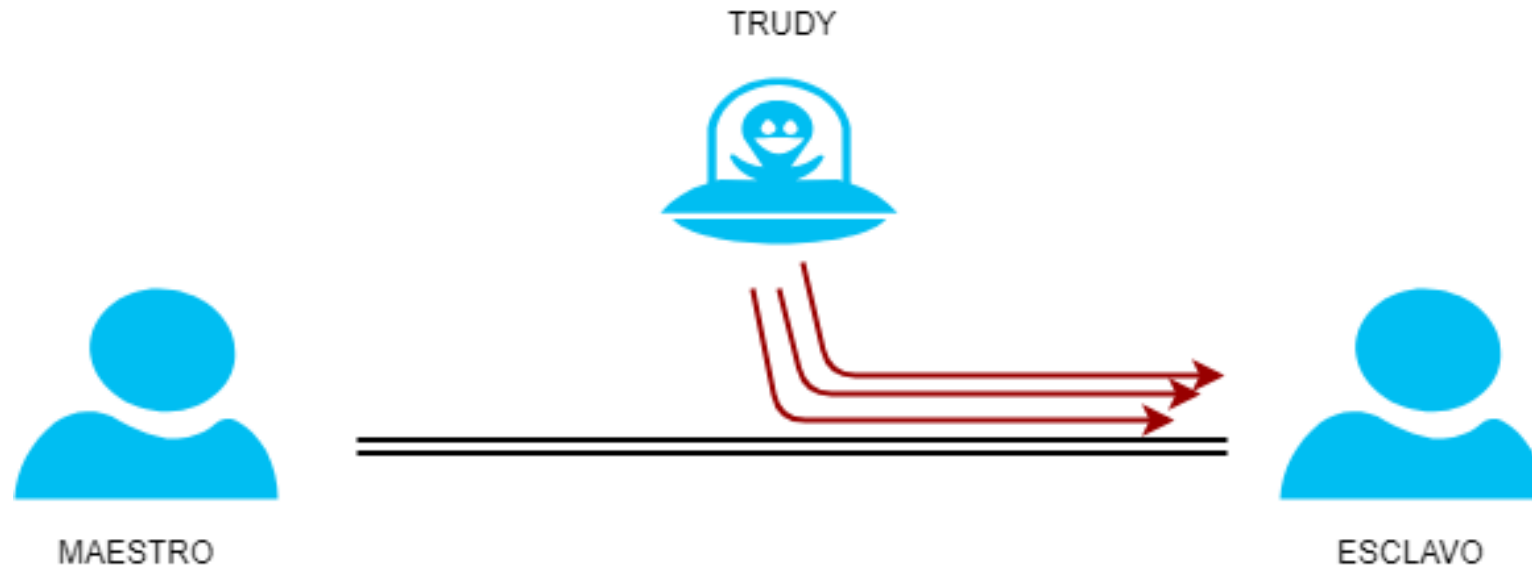
GENERADOR DE TRÁFICO MODBUS

SIMULADOR DE PLC

VALIDACIONES



REPRODUCCIÓN DE ATAQUES



CONCLUSIONES Y TRAJO FUTURO

- Escenario de simulación
- Herramientas de auditoria.
- Posibilidad de generar trafico Modbus real.

TRABAJO FUTURO:

- Mejora del protocolo sobre los simuladores.
- Sistemas de detección de intrusiones.