UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Ciberconciencia Situacional

2024/2025

Francesco Lorenzoni
PCA25403GU

Trabajo 3

Caracterización de sistemas ciberfísicos

Contents

Chapter 1

Tarea 1

1.1 Componentes del sistema de distribución de agua

- **Componentes físicos:**
  - Reservoirs
  - Tanks
  - Valves
  - Pipes
  - Pumps
  - Taps in houses
- **Componentes ciberfísicos:**
  - Sensors
    - Water temperature
    - Water pressure
  - Logic Controllers (PLCs) que, por ejemplo, pueden activar una valvula si una cisterna está casi vacía
- **Componentes ciber:**
  - Networks
  - Computadoras
- SCADA (Supervisory Control and Data Acquisition)

1.2 Tipos de ataque

Components of cyberphysical systems often do not enforce strong security measures, making them a target for attackers, who can gain initial access to a system by exploiting their vulnerabilities.

- Stealing data
- Damaging eequipment
- Cutting off water supply
- Releasing toxic chemicals
- Eavesdropping attacks
- DoS (Denial of Service)
- Deception attacks, i.e. sending bogus data to the control system

Parte de estos ataques van a mostrar efectos evidentes en el sistema de distribución, pero los atacantes también pueden cubrir sus huellas manipulando los datos que se envían al sistema de control, engañando potencialmente tanto a humanos como a algoritmos.

1.3 Defensa frente a ataques

La mejor defensa para Water Distributio Networks es la simulación de ataques, sin embargo, actualmente no existe un método estándar para hacerlo. El video muestra dos métodos de simulación:

- Attack models, que son modelos matemáticos que simulan los posibles comportamientos de un atacante. `epanetCPA` es una herramienta que funciona en MATLAB que permite, dado un modelo de ataque, de ejecutar el modelo en una red PA, que es un modelo industrial estandar de red de agua, y ver cómo se comporta el sistema. `epanetCPA` controla tanto el estado físico del sistema como el estado cibernético emulado del sistema.

Tras un estudio, se observó que ataques a distintos componentes conducen a resultados similares, entonces encontrar un comportamiento anomalo en el sistema puede ser insuficiente para determinar cual componente ha sido atacado.

Chapter 2

Tarea 2

2.1 Componentes de la red industrial

- **Componentes físicos:**
  - 100kv high-voltage incoming line
  - Power transformer
  - 10kV bus feeder
  - Primary switching equipment
- **Componentes ciberfísicos:**
  - transformer protection
  - 2 bay controllers
  - Industrial Ethernet switch
  - Router
- **Componentes ciber:**
  - Kaspersky Industrial CyberSecurity
    - Industrial Endpoint Protection (Nodes)
    - Industrial Anomaly and Breach Protection (Network)
    - Centralized security management
  - Firewall
  - Remote Control Center tools
  - SCADA server