



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Ciberconciencia Situacional

2024/2025

Francesco Lorenzoni
PCA25403GU

Trabajo 3

Caracterización de sistemas ciberfísicos

Contents

1 Tarea 1	5
1.1 Componentes del sistema de distribución de agua	5
1.2 Tipos de ataque	5
1.3 Defensa frente a ataques	6
2 Tarea 2	7
2.1 Componentes de la red industrial	7
2.1.1 Kaspersky Industrial CyberSecurity (KICS)	8
2.2 Ataque sobre la infraestructura industrial y defensa	8
2.2.1 Conclusiones sobre KICS	9

Chapter 1

Tarea 1

Tarea a realizar

Visualiza el siguiente vídeo: youtube.com/watch?v=dEvtsZNrCSQ

- ◊ Identifica en el sistema de distribución de agua los componentes físicos, ciberfísicos, y ciber
- ◊ Identifica los tipos de ataque que se describen en el vídeo, y explica brevemente como piensas que se podrían implementar.
- ◊ Explica cómo se plantea en el vídeo la defensa frente a los posibles ataques.

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
 - Actuators in general
- ◊ **Componentes ciber:**
 - SCADA (Supervisory Control and Data Acquisition)
 - HMIs
 - Networks
 - Computadoras

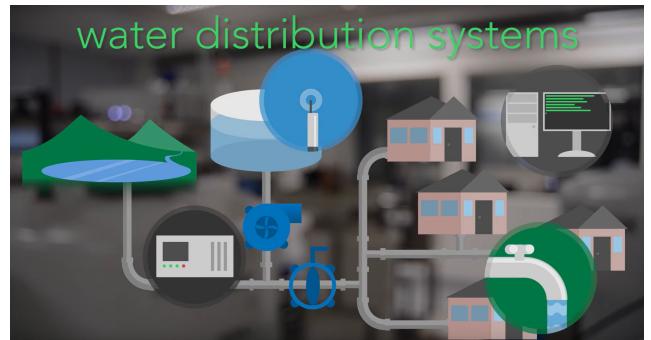


Figure 1.1: Esquema de un sistema de distribución de agua

1.2 Tipos de ataque

Los componentes de sistemas ciberfísicos a menudo no implementan medidas de seguridad fuertes, convirtiéndolos en objetivo para atacantes, que pueden obtener acceso inicial a un sistema explotando sus vulnerabilidades.

- ◊ **Robo de datos (Stealing data):** Podrían implementarse mediante la infiltración en los sistemas SCADA para extraer información confidencial sobre la infraestructura, patrones de uso, o datos de clientes. Esto podría realizarse mediante malware especializado o aprovechando vulnerabilidades en el software de control. Es posible también a través de **packet sniffing**.
- ◊ **Daño al equipamiento (Damaging equipment):** Manipulación de PLCs para operar bombas fuera de sus límites operativos. Similar al ataque Stuxnet que dañó centrifugadoras en Irán modificando frecuencias de

operación.

A veces, los sistemas empotrados no tienen **separación de privilegios** (monolithic kernel, todas las aplicaciones tienen el mismo —máximo— privilegio, falta de memory protection), lo que facilita la manipulación.

- ◊ **Corte del suministro de agua (Cutting off water supply):** Cierre de válvulas o apagado de bombas mediante acceso no autorizado a HMIs (Human-Machine Interfaces); **command injection** ataques juntos a falta de **input validation** pueden permitir a un atacante ejecutar comandos arbitrarios en el sistema.
- ◊ **Liberación de sustancias tóxicas (Releasing toxic chemicals):** Alteración de sistemas de dosificación química explotando PLCs con vulnerabilidades conocidas. Hemos mencionado en clase “**Maroochy Shire**”, donde un ex-empleado de la empresa de control de aguas trató de liberar aguas residuales en el sistema de distribución, a través de un laptop y de una transmisión de radio para manipular bombas y válvulas.
- ◊ **Ataques de interceptación (Eavesdropping attacks):** Captura de tráfico no cifrado entre sensores y controladores mediante herramientas como *Wireshark*. Hemos visto que si pueden alterar las funciones de los protocolos SCADA MODBUS y DNP3 con fines malévolos. Además, SCADA protocolos pueden carecer de **encriptación**, y, en cualquier caso, existen técnicas de *Deep Packet Inspection* (DPI) que permiten deducir información incluso de paquetes cifrados. Una práctica común es el **ARP spoofing** para redirigir el tráfico a un dispositivo de escucha.
- ◊ **Denegación de servicio (DoS):** Saturación de interfaces de red de controladores RTU/PLC, o explotación de vulnerabilidades para inhabilitar dispositivos. Ejemplos típicos incluyen **SYN flooding**, **Malformed packets injection** o **Smurf** ataques.
- ◊ **Ataques de engaño (Deception attacks):** Falsificación de lecturas de sensores mediante ataques man-in-the-middle en protocolos vulnerables como OPC UA. El ataque a una *Ukrainian Power Grid* en 2015 utilizó técnicas de engaño para hacer que los empleados obtuvieran un malware a través de correos electrónicos para comprometer la red.

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 Distribution Networks* es la **simulación de ataques**, sin embargo, actualmente no existe un método estándar para hacerlo. “Attack models” son modelos matemáticos que simulan los posibles comportamientos de un atacante. El video muestra epanetCPA es una herramienta que funciona en MATLAB que permite, dado un modelo de ataque, de ejecutar el modelo en una red EPANET (open-source toolkit para modelar y simular redes de distribución de agua), que es un modelo industrial estandar de red de agua, y ver cómo se comporta el sistema.

Se puede controlar tanto el *estado físico* del sistema como el *estado cibernético* emulado del sistema, así que se puede **comparar** el comportamiento del sistema real con el comportamiento del sistema simulado.

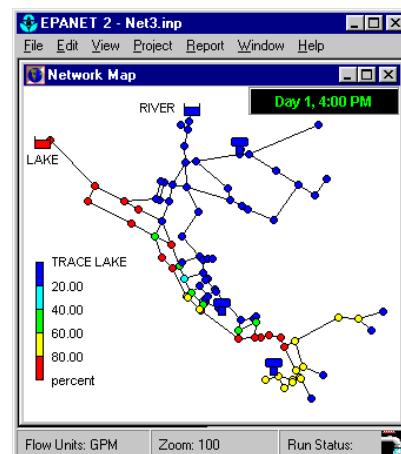


Figure 1.2: EPANET 2.0

Tras un estudio, se observó que ataques a distintos componentes conducen a resultados similares, entonces encontrar un comportamiento anormal en el sistema puede ser *insuficiente* para determinar cual componente ha sido atacado, lo que hace necesaria una evaluación humana más completa.

Chapter 2

Tarea 2

Tarea a realizar

Visualiza el siguiente vídeo: youtube.com/watch?v=7LNtjWx17mA

- ◊ Identifica en la red industrial los componentes físicos, ciberfísicos, y ciber
- ◊ Identifica los tipos de ataque que se describen en el vídeo, y explica brevemente como piensas que se podrían implementar.
- ◊ Explica cómo plantea la solución de Kaspersky en el vídeo la defensa frente a los posibles ataques.

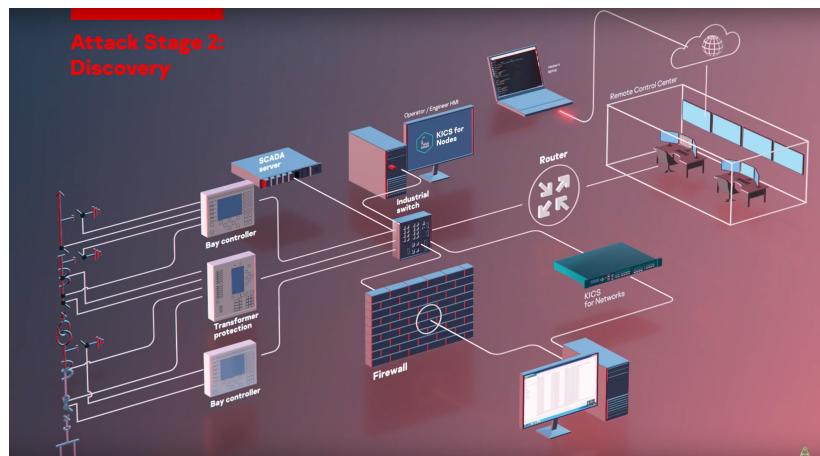


Figure 2.1: Escenario representado en el vídeo

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
- ◊ **Componentes ciber:**
 - Kaspersky Industrial CyberSecurity
 - KICS for Nodes - Endpoint Protection
 - KICS for Network - Anomaly and Breach Protection
 - Centralized security management
 - Kasperky Security Center - Manager installed on nodes
 - Router

- Firewall
- Remote Control Center tools
- SCADA server

2.1.1 Kaspersky Industrial CyberSecurity (KICS)

Las —“claimed”— features de KICS son las siguientes:

- ◊ Passive traffic analysis
- ◊ No influence on network stability
- ◊ Detection of:
 - Unauthorized network access
 - Cyberattacks and intrusions
 - Unauthorized commands to industrial equipment
 - Technological parameters anomalies:
 - Rules based
 - Machine learning
 - Assets and its parameters
 - Abnormal dataflow on network map

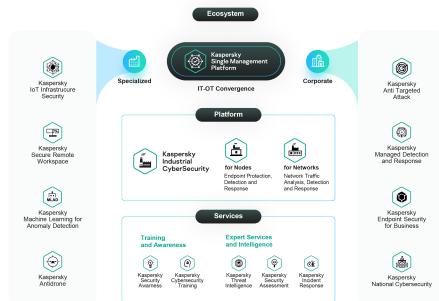


Figure 2.2: KICS schema

2.2 Ataque sobre la infraestructura industrial y defensa

El ataque que se muestra en el video comprende tres fases, también se analizan las posibles implementaciones de cada una de ellas:

1. Breach - Obtener acceso a un componente

- ◊ Instalar un malware a través de un documento .pdf en un USB, que cuando se abre, se conecta al atacante, que obtiene acceso a la computadora infectada, que puede utilizarse como fuente para futuros ataques en la red.
- ◊ Defensa - KICS for Networks detecta una comunicación no autorizada entre la computadora infectada y una dirección IP externa y un payload potencialmente peligroso, y envía una alerta a *Kaspersky Security Center*.

Si puede bloquear el ataque aquí, pero en el video se supone que no lo haces para mostrar el comportamiento defensivo en las fases siguientes

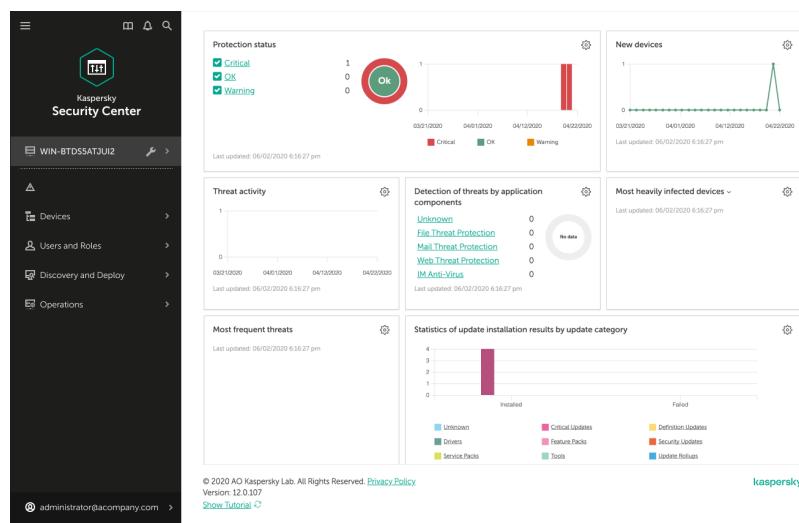


Figure 2.2: Kaspersky Security Center

2. Discovery - Obtener información y datos sobre el sistema

- ◊ A través del componente infectado, el atacante puede **escanear** la red y obtener información sobre los dispositivos ciber y ciberfísicos conectados, lo que le permite establecer las vulnerabilidades actuales y planificar futuros ataques explotándolas. A menudo las comunicaciones entre dispositivos ciberfísicos y ciber carecen de **encriptación**, potencialmente exponiendo datos y credenciales sensibles.
- Si no hay suficiente segmentación de red, o si falta apropiada configuración de los Firewalls, este proceso puede ser aún más facilitado.
- ◊ Defensa - KICS for Networks detecta un escaneo de red no autorizado y envía una alerta a Kaspersky

Security Center. Imagino que KICS también puede detectar cualquier movimiento lateral del atacante.

3. Technlogical Attack - Ataque a la infraestructura

- ◊ Si no se bloquea el ataque en la fase anterior, el atacante puede enviar **comandos no autorizados** (*command injection*) a los dispositivos ciberfísicos.

El ejemplo que se hace en el video es de utilizar una vulnerabilidad —conocida— del firmware del componente de protección del transformador para enviar un comando inapropiado para updatear el firmware de modo que el dispositivo deje de cumplir su función de protección.

Vulnerabilidades típicas de sistemas CPS incluyen:

- Permissions, Privileges and Access Control
- Improper Authentication
- Insufficient Verification of Data Authenticity

Parece claro como estas pueden facilitar un ataque como el que se muestra en el video.

- ◊ En este punto, el atacante puede causar daños físicos como cortocircuitos y similares
- ◊ Defensa - KICS for Networks detecta un comando no autorizado y envía una alerta a Kaspersky Security Center.

Aunque no se detenga el ataque, podemos utilizar la información recopilada para mitigar futuros ataques.

2.2.1 Conclusiones sobre KICS

El video no discute en profundidad la defensa de KICS, pero me parece que el punto de fuerza de KICS sea que puede operar a diversos **niveles**, y que instancias de KICS pueden **comunicarse** entre sí para compartir información sobre ataques y vulnerabilidades. Esto permite de hacer un análisis de lo que está ocurriendo más **completa y amplia**, que es el punto fundamental de la Ciberconciencia Situacional.

Sin embargo, el problema fundamental en sistemas ICS es que luego de detectar un ataque, hay que decidir como responder a él, porque no se puede hacer nada que pueda interrumpir o alterar el funcionamiento del sistema, las prioridades son la continuidad del servicio, y la seguridad del personal y de la infraestructura.

Esto es un problema que no se discute en el video y cuya gestión puede depender mucho del sistema concreto en cuestión.