Desarrollo y seguridad SCADA de una planta cerámica

Universidad de Oviedo

Enrique Murias Fernández
UO266812@uniovi.es / enrique-murias@tecdesoft.es

Tutor/es:
Marta Vales Fernández, TECDESOFT S.A., marta-vales@tecdesoft.es
José Ángel Sirgo Blanco, Universidad de Oviedo, sirgo@uniovi.es

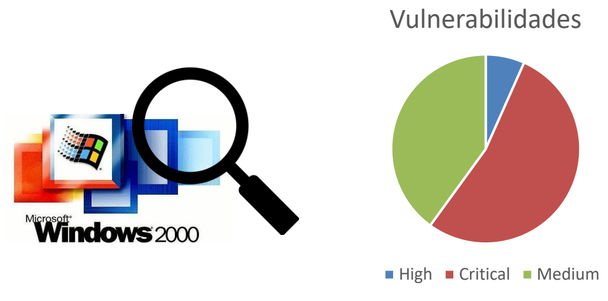
Máster en Ingeniería de Automatización e Informática Industrial

Resumen

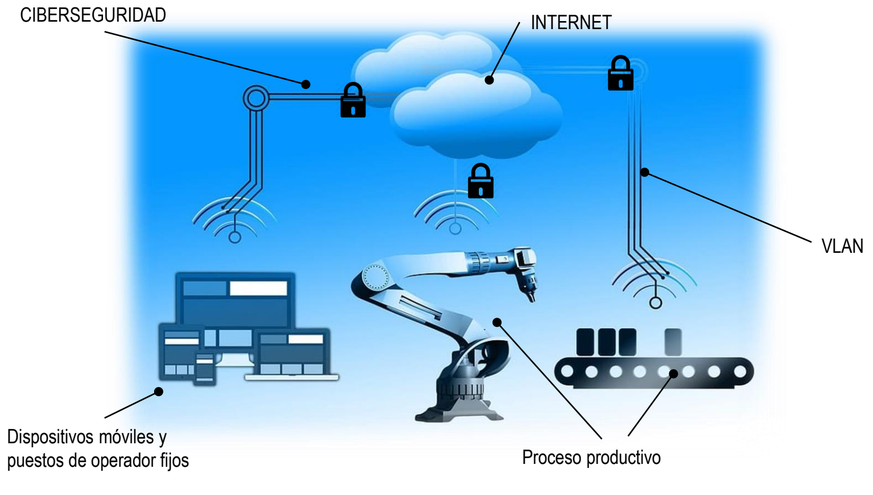
Este trabajo fin de máster consiste en la reforma de la red de comunicaciones de la planta de producción cerámica para cumplir con los requisitos actuales de ciberseguridad industrial que exige el estándar ISA99/IEC6443, así como también contempla el desarrollo de un sistema SCADA de alta disponibilidad redundante, programado en la medida de lo posible de forma que pueda reaprovecharse el código en futuros desarrollos o ampliaciones del mismo con el objetivo de reducir los costes, el tiempo y la facilidad de desarrollo. El sistema SCADA tiene la particularidad de que se puede usar tanto desde dispositivos móviles, tabletas, ordenadores, pantallas táctiles y navegadores, siempre que se respete la resolución para la que se ha desarrollado, de esta forma es posible adaptarse a las exigencias de los operadores de la planta y la tendencia a usar dispositivos portátiles en la industria.

Palabras clave: SCADA, Ciberseguridad, Virtualización, ISA99, Redundancia

1. Antecedentes y Objetivos



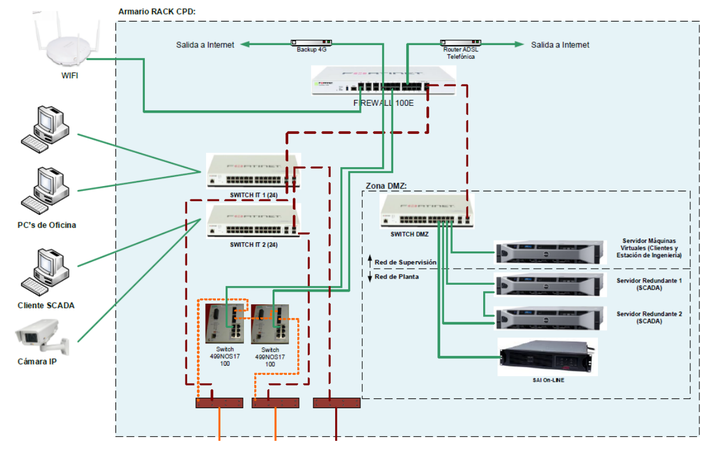
Identificación de vulnerabilidades del servidor SCADA:
- Impacto crítico: 8 (MS04-022, MS05-027, …)
- Impacto alto: 1 (MS06-035)
- Impacto medio: 6



Ciberseguridad:	*ISA99/IEC6443*
Hardware de red:	*Firewall y switches Fortinet*
Segmentación de red:	*VLAN (red de área local virtual)*
Virtualización:	VmWare ESXi (Hipervisor)
Sistema SCADA:	SIMATIC WinCC v7.4
Redundancia SCADA:	Alta disponibilidad
Dispositivos:	PC, Tablet, Smartphone
Acceso remoto:	Forticlient VPN, Internet

2. Diseño y desarrollo

Diseño de red:

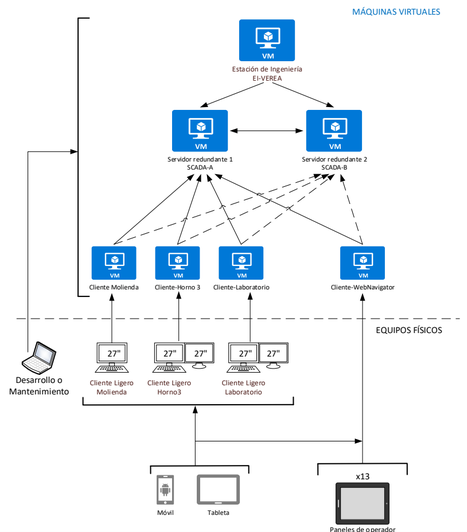


ISA99/IEC6443

- Designación de Zonas (VLAN)
- Identificación de Conductos
- Zona desmilitarizada DMZ
- Centralización acceso a Internet
- Control de las comunicaciones mediante el Firewall

- Acceso remoto
- Instalación de los equipos en un armario Rack CPD

Diseño y desarrollo SCADA:



VIRTUALIZACIÓN

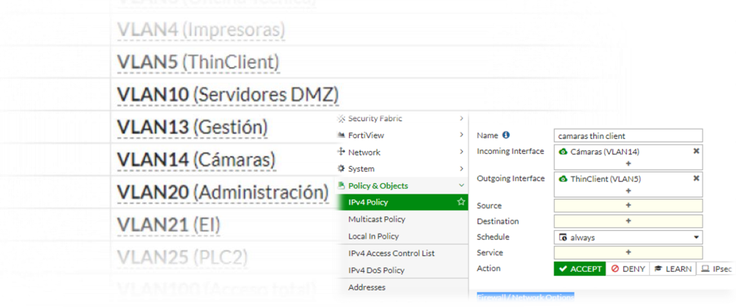
- Hipervisor VmWare ESXi
- Virtualización de los sistemas operativos
- Aumento de la fiabilidad y seguridad

- Sistema SCADA WinCC v7.4
- Redundancia (*Alta disponibilidad*)
- Acceso desde navegador web (*Webnavigator*)

- Uso de estructuras de variables
- Pantallas de mando e información fácilmente ampliables
- Empleo de objetos tipo Faceplate que facilitan la modificación gráfica de forma global
- Registro de operaciones de los operadores
- Desarrollo de funciones que permite reaprovechar el código
- Generación de alarmas de comunicación de los PLCs

3. Resultados

Seguridad de la red de comunicaciones:

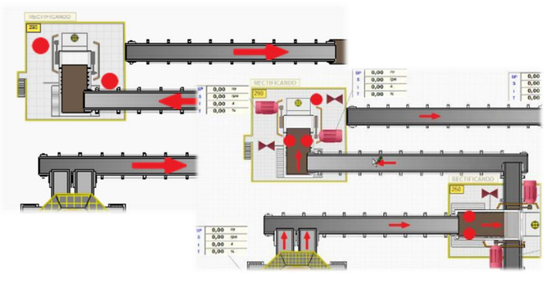


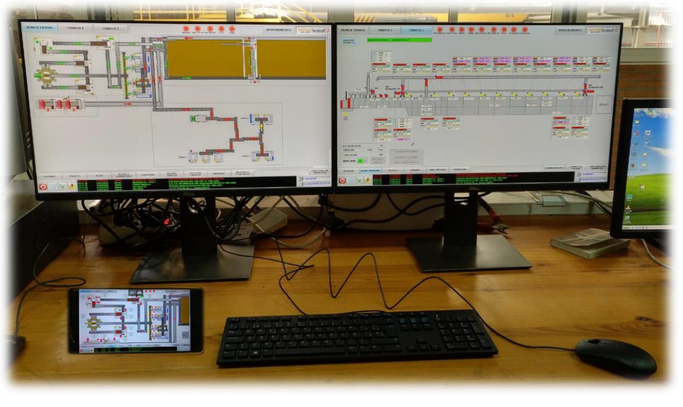
- Red totalmente segmentada mediante VLANs
- Control del tráfico de red estableciendo políticas
- Sistema de red ampliable y fácilmente configurable
- Posibilidad de actualizar las bases de firmas de virus periódicamente
- Acceso remoto seguro (SSLVPN)

Sistema SCADA:

Principales funcionalidades:

- Permite la ampliación de zonas para visualizar los detalles menos relevantes de las máquinas y destacar los más importantes de la vista general
- Se cierran las ventanas de mando al pulsar en el fondo del sinóptico (muy útil para manejarlo desde dispositivos móviles)
- Vista de las ventanas de mando en modo reducido o ampliado.





Características:

- Manejo de la planta de producción independientemente de la ubicación del operario.
- Posibilidad de emplear dos monitores independientes.
- Soporte de una alta carga táctil
- Acceso al SCADA desde dispositivos móviles

4. Conclusiones y Discusión

1. La mejora de la seguridad de la red de comunicaciones adaptándose a los requisitos que demanda la industria, ofrece confianza al cliente para operar la planta desde el exterior y evitar accesos incontrolados.
2. La posibilidad de supervisar la planta con seguridad de forma remota aumenta la productividad y reduce los tiempos de reacción ante un incidente.
3. Los sistemas SCADA comerciales son cada vez más flexibles y permiten ampliarse de una forma fácil, lo que reduce el coste de desarrollo, pero son muy mejorables en cuanto a las posibilidades de reaprovechamiento de código de forma eficiente.
4. El empleo de las nuevas técnicas de desarrollo para reciclar y centralizar el código afectan al rendimiento del SCADA y son contrarias a la rapidez de operación, por ello la implementación de estas técnicas en sistemas muy amplios deben ser consideradas previo al desarrollo del sistema.

Agradecimientos

verea tejasytejados

tecdesoft