“Aspectos Básicos de la Securitización de una Red TO, Industrial o de Planta: un caso práctico”

Cigre 2017

www.bigniss.cl

Expone:

Carlos Aracena Urrutia
Director Desarrollo de Productos y Servicios - TIC Industrial
Bigniss Ltda.
celular: + 56 9 9885 5653 - e-mail: caracena@bigniss.cl

Agenda

- Introducción
- Marco Teórico
- Elementos para Securitizar Redes Industriales
- Diseño de una Red Industrial
- Securitización de una Red Industrial
- Resumen

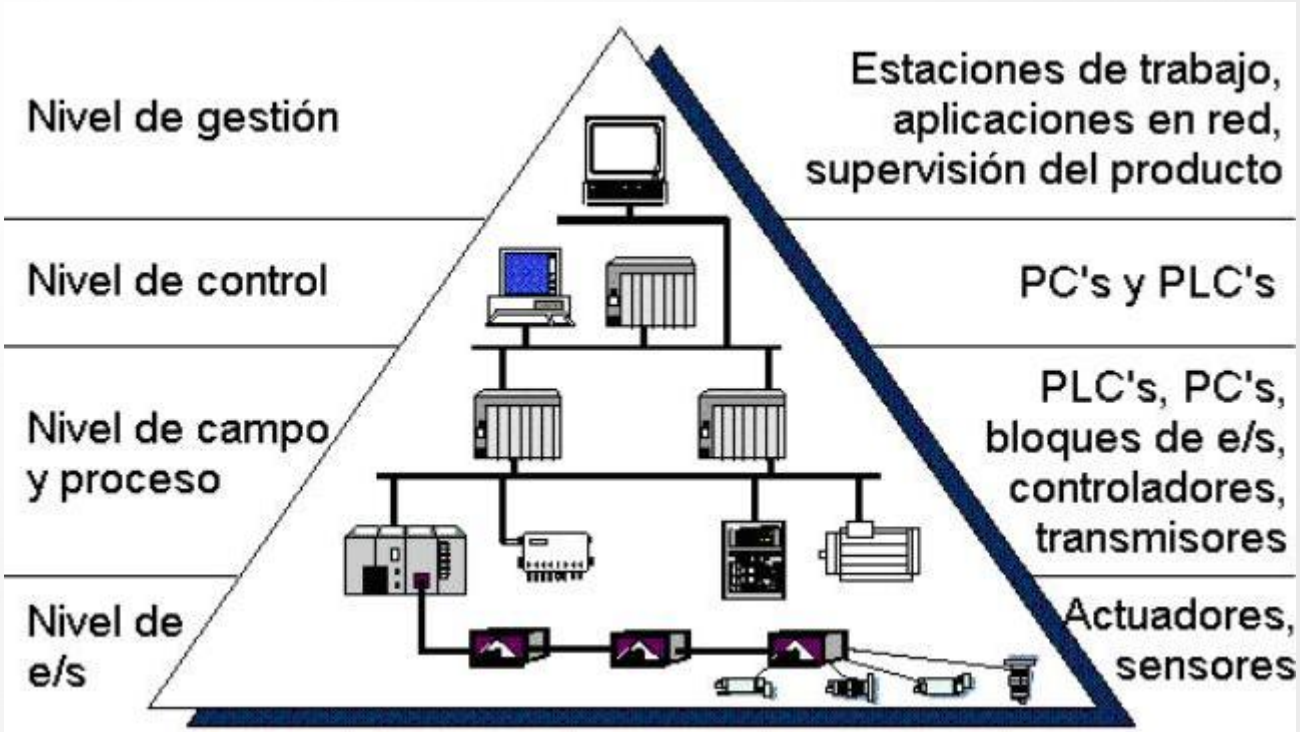
Normas y estándares

- IEC 62264 (ex ISA 95), arquitectura red PCN
- IEC 62443 (ex ISA 99), ciberseguridad industrial

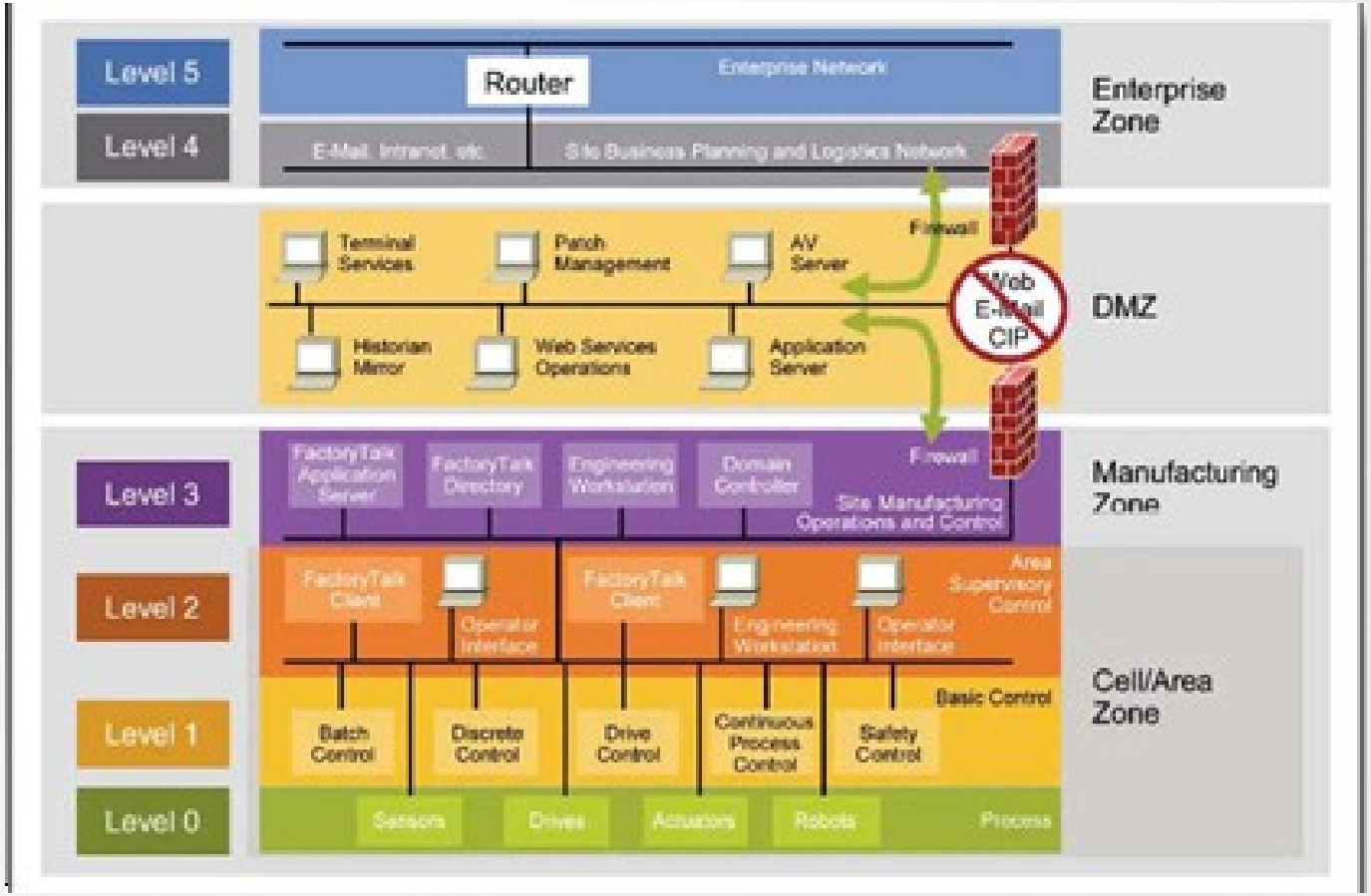
Modelo General de una red PCN

- Ambiente hostil:
  - Capa física redundante y robusta (fibra óptica, SFTP, Gabinetes con grado de protección adhoc).
  - Equipos activos industriales (fanless).
  - Fuentes de poder redundantes.
- Facilidades para gestión remota (desde Sala SCADA o de Control)

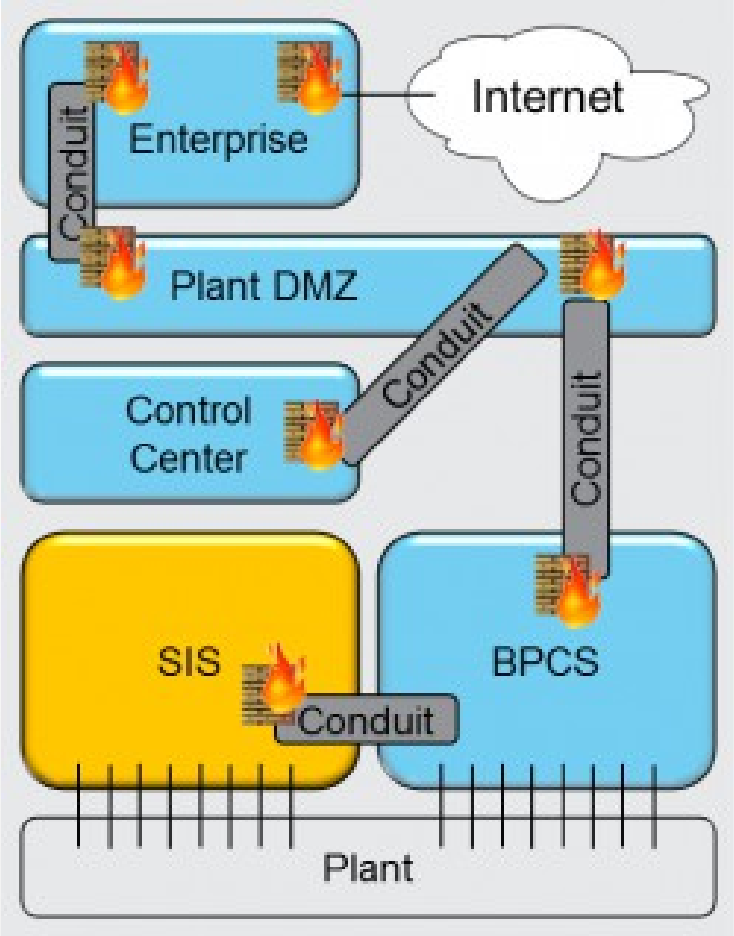
Arquitectura de una red Industrial



Norma IEC 62443 (ex ISA 99)



Zones & Conduit



Networking

- Equipos activos L2 (switches con gestión snmp)
- Separación física de las Redes
- Segmentación lógica: definición de VLAN (VLAN id, direccionamiento IP).
- Firewalls que aplican reglas, definen DMZ y hacen routing de la red (L3).

Seguridad de la red PCN

- La red PCN debe protegerse de ataques internos y externos a la red
- Para prevenir desde fuera:
  - Se debe construir un perímetro (Firewall perimetral)
  - Se debe contar con un Concentrador de VPN (VPNc)

Seguridad de la red PCN (cont.)

- Para prevenir desde dentro:
  - Soft => definir y administrar políticas de seguridad basadas en ISO 27001/IEC 62443
  - Hard:
    - Firewall en dispositivos de nivel de campo y proceso (en PLC o tipo Tofino).
    - Incorporar Sistemas de Detección/Prevención de Intrusos (IDS/IPS: DNP 3.0, ICCP -104, IEC 61850) en el segmento de los servidores SCADA, DCS, Historian, DMZ, etc.

Servicios de la red PCN

- Herramientas necesarias para el funcionamiento de los aplicativos industriales y sistemas de gestión de la red:
  - Microsoft Active Directory de la red PCN.
  - Servidor AAA simple o rubusto (Authentication, Authorization and Accounting)
  - NTP server (sincronización en el tiempo)
  - Servidor Logger (archivos syslog)

Gestión de la red

- Herramientas para saber que pasa en la red (caída de segmentos, falla en protocolos de convergencia o de componentes, ataques de seguridad (DoS, ramsomware, virus, etc.)
- Las plataformas de monitoreo se implementan en un NOC (networking vía snmp), SOC (Seguridad, colectando alertas)
- La gestión de incidentes se hace en el I-

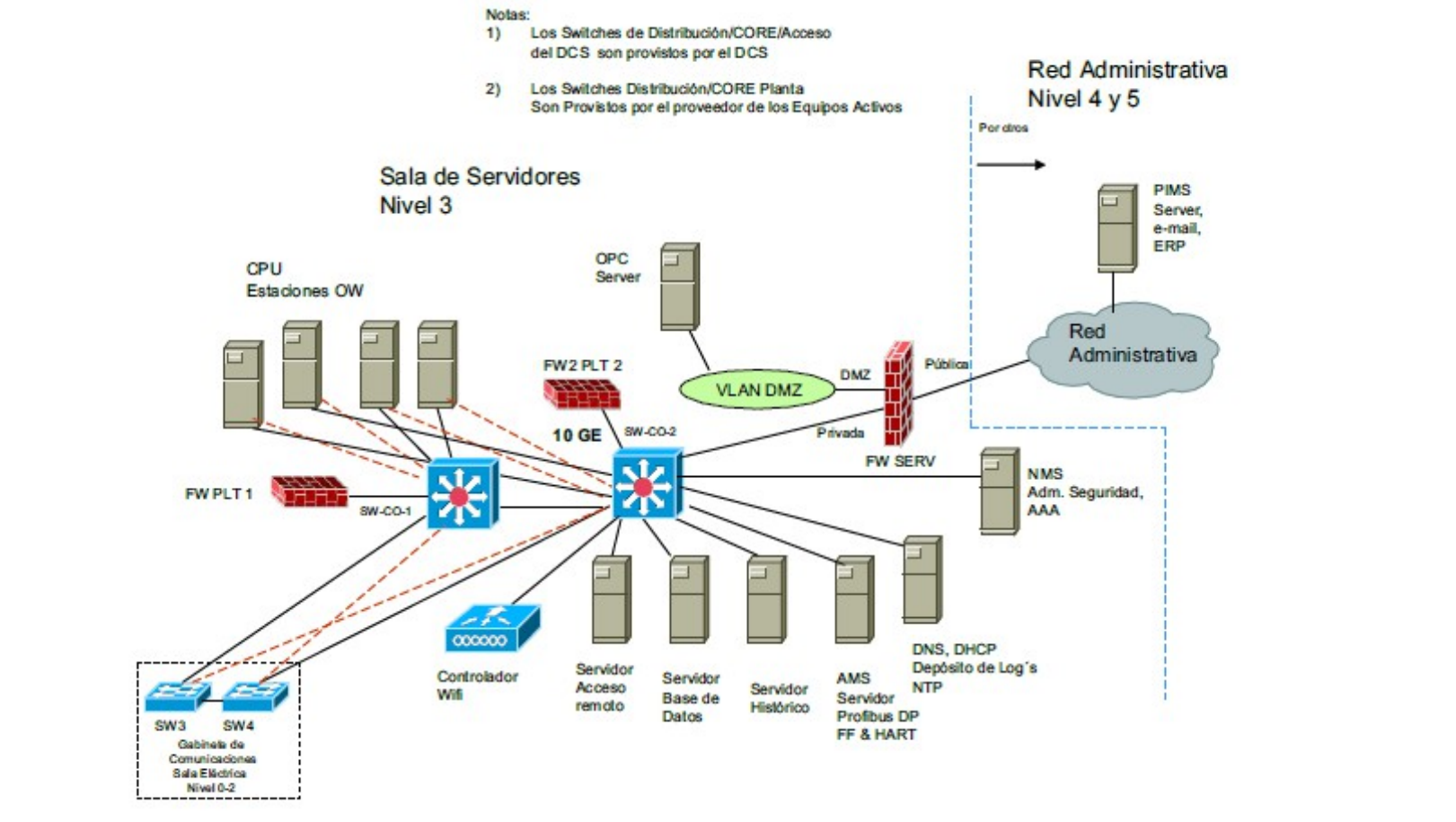
Herramientas NOC/SOC

- NOC:
  - Ruggedcom NMS
  - HiVision (Hirschmann)
  - Nagios (open source)
- Cisco Security Management (CSM)
- HP Arcsight (colector de syslog)

Abreviaturas

- NOC = Network Operation Center
- SOC = Security Operation Center
- I-SOC = Industrial Service Operation Service
- snmp = simple network management protocol
- NTP = Network Time Protocol

Red PCN - EJEMPLO



Resumen

- El diseño/rediseño de la red PCN se basa en las normas IEC 62264/62443
- La securitización de la red incorpora seguridad lógica perimetral y buenas prácticas aplicadas a la industria
- El administrador de la seguridad de su red protege “su red”

Gracias por su tiempo !!