NEOSECURE
SABEMOS DE SEGURIDAD

Ciberseguridad para Entornos Industriales: Industrial Control System “ICS”

EPRE
Ente Provincial
Regulador Eléctrico

Desafíos, Riesgos, Amenazas
Modelo y Soluciones

Septiembre-2021

Georg Gromsch Harvey
Arquitecto Soluciones

Acuerdo de Confidencialidad

- Esta presentación contiene Información confidencial de Propiedad de Neosecure

- **EPRE** acuerda mantener esta información confidencial y no difundirla a terceros sin la autorización previa de Neosecure

Relator Georg Gromsch Harvey

- Ingeniero Civil Eléctrico “Control Automático & Sist. Digitales” USACH
- Profesional con más de 35 años Experiencia Laboral
- Cuenta con 8 años de experiencia en el ámbito del Control Automático de Sistemas Industriales en Empresas de las verticales de Energía, Minería y Petroquímicas
- Tiene 17 años de experiencia en labores de diseño, implementación y soporte de soluciones de Seguridad & Ciberseguridad. Para organizaciones de Latinoamérica que incluyen entre otros los sectores Industriales, Financieros, Comercial y Retail
- Además de 14 años de experiencia directa en el ámbito del diseño e implementaciones de tecnología de la información en entidades del área Industrial y Financiero

Agenda

- **Sistema Eléctrico Nacional**
- **Estándar de Ciberseguridad**
- **Ciberseguridad en Industrial Control System “ICS”**
  - **Desafíos, Riesgos, Amenazas ICS**
  - **Modelo y Soluciones**

Sistema Eléctrico Nacional Chile 2021

NEOSECURE
SABEMOS DE SEGURIDAD

COORDINADOR ELÉCTRICO NACIONAL

Sistema Eléctrico Nacional

El **Sistema Eléctrico Nacional**, nace en el año 2017, en el momento en que los ex sistemas del norte grande y del centro sur del país, se unificaron.

Por las características de la geografía nacional, es un **sistema único** en cuanto a longitud, alcanzando los 3.100 km y abarcando casi la totalidad del territorio nacional, desde la ciudad de Arica por el norte, hasta la Isla de Chiloé, en el sur.

36.052
km de Líneas
Sistema de Transmisión año 2021
(desde Arica a Chiloé)

47.231,0
GWh
Producción Anual
a julio 2021

617
Empresas Coordinadas
año 2021

98,5
%
De cobertura de la Población Nacional
año 2021

11.038,8
GWh
Producción anual de Energías
Renovables No Convencionales
a julio 2021

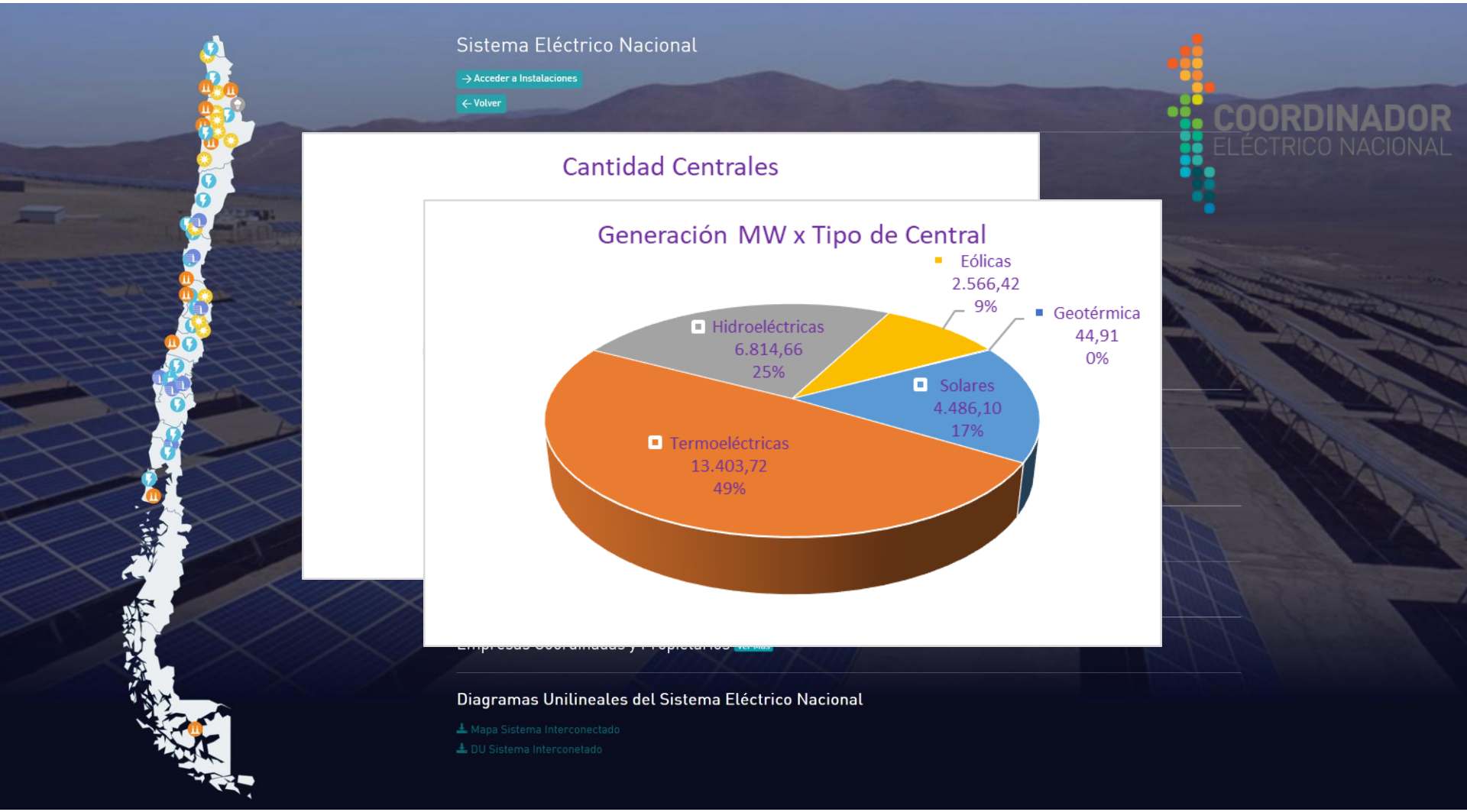
28.495,3
MW
Potencia Instalada
a julio 2021

11.227,4
MWh/h
Demanda Máxima Horaria
a julio 2021

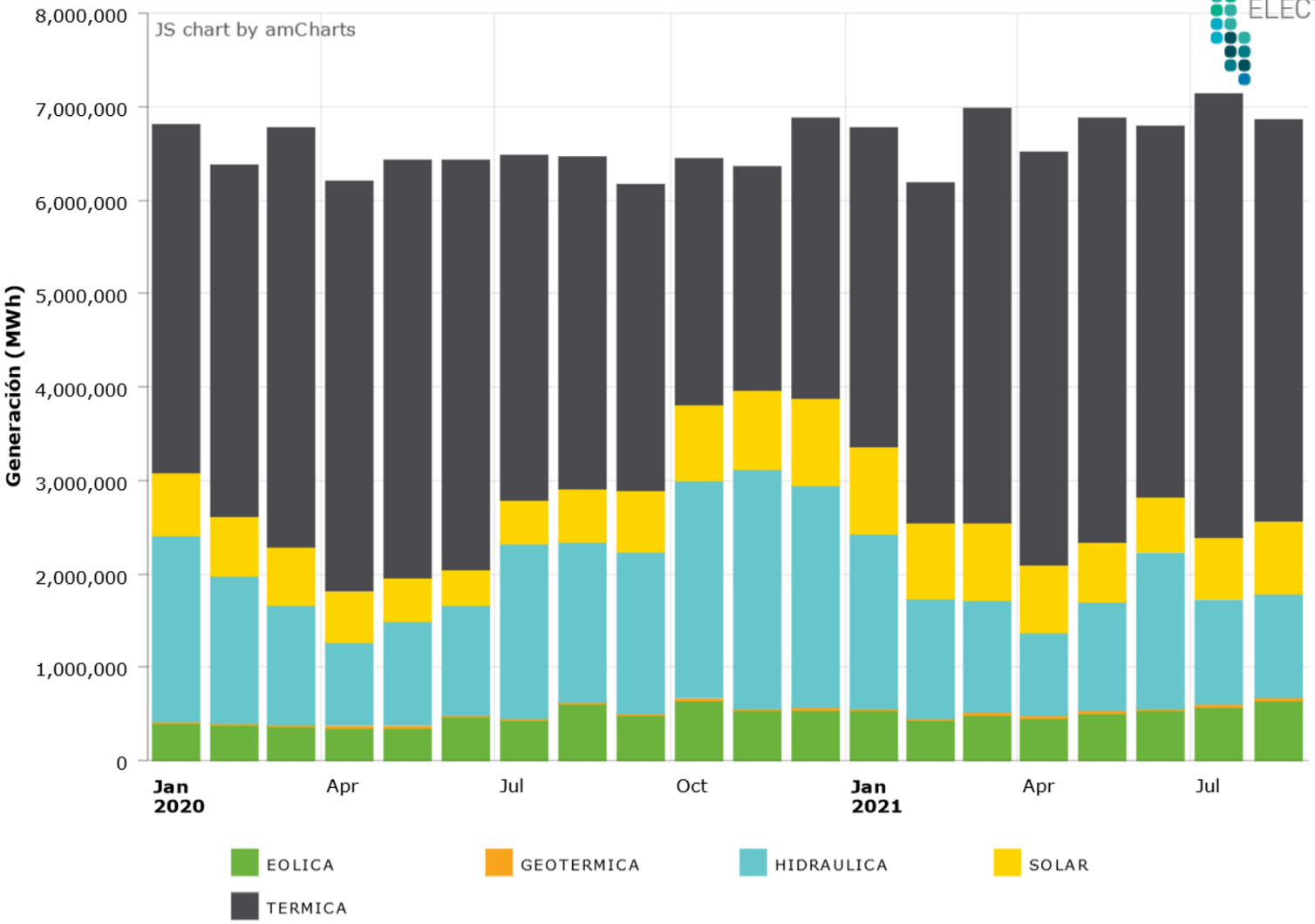
43.433,5
GWh
Ventas a Cliente Final
a julio 2021

Sistema Eléctrico Nacional Chile 2021

NEOSECURE
SABEMOS DE SEGURIDAD



Generación acumulada Mensual por Tecnología 2020 - 2021



Política Energética de Chile 2050

NEOSECURE
SABEMOS DE SEGURIDAD

ENERGÍA 2050
POLÍTICA ENERGÉTICA DE CHILE

PRINCIPALES METAS 2050

1 La indisponibilidad de suministro eléctrico promedio, sin considerar fuerza mayor, **no supera a una hora/año en cualquier localidad del país.**

2 **Las emisiones de GEI del sector energético chileno** son coherentes con los límites definidos por la ciencia a nivel global y con la correspondiente meta nacional de reducción, haciendo una contribución relevante hacia una economía baja en carbono.

3 **Asegurar acceso universal y equitativo** a servicios energéticos modernos, confiables y asequibles a toda la población.

4 **Los instrumentos de planificación y ordenamiento** territorial regional y comunal incorporan los lineamientos de la Política Energética.

5 **Chile se encuentra entre los 3 países OCDE** con menores precios promedio de suministro eléctrico, a nivel residencial e industrial.

6 **Al menos el 70% de la generación eléctrica nacional** proviene de energías renovables.

7 **El crecimiento del consumo energético** está desacoplado del crecimiento del producto interno bruto.

8 **El 100% de las edificaciones nuevas cuentan con estándares OCDE** de construcción eficiente, y cuentan con sistemas de control y gestión inteligente de la energía.

9 **El 100% de las principales categorías de artefactos** y equipos que se venden en el mercado corresponden a equipos energéticamente eficientes.

10 **La cultura energética está instalada en todos los niveles de la sociedad,** incluyendo los productores, comercializadores, consumidores y usuarios.

Descarbonización Matriz Generación

NEOSECURE
SABEMOS DE SEGURIDAD

COORDINADOR ELÉCTRICO NACIONAL

Julio - 2021

Juan Carlos Olmedo: "para alcanzar la descarbonización es fundamental seguir fortaleciendo el proceso de transformación del sistema eléctrico"

Según el presidente del Coordinador Eléctrico Nacional, "esperamos que se activen todos los proyectos de generación de energía renovable y de infraestructura de transmisión"

(30 de julio de 2021) Todos los actores que forman parte del mercado eléctrico nacional, es decir, generadores, transmisores y distribuidores, han demostrado un óptimo desempeño a pesar de los nuevos y grandes desafíos que ha impuesto la pandemia para el despliegue de sus operaciones. Un logro que obedece al esfuerzo permanente desarrollado por la industria, que pretende seguir creciendo vigorosamente y consolidándose a corto, mediano y largo plazo.

Así lo subrayó el presidente del ***Coordinador Eléctrico Nacional***, Juan Carlos Olmedo, en el marco de una entrevista a Diario Financiero, oportunidad en la que recalcó que, pese a todas las adversidades que ha debido enfrentar nuestro país, el sistema ha mantenido la continuidad operacional sin mayores contratiempos.

Un desempeño que, a su juicio, reafirma todo el trabajo desarrollado con el propósito de fortalecer al sector.

'Desde el punto de vista del consumo, si comparamos el período enero-junio de 2020 con el mismo del presente año observamos un crecimiento de la demanda de 3,5%. Un positivo registro que esperamos que continúe incrementándose a futuro', enfatiza.

En un eventual escenario pospandemia, el mercado eléctrico espera seguir consolidándose e implementando nuevos proyecto objetivo es trabajar en el desarrollo de las redes de transmisión, ya que para alcanzar la descarbonización es fundamental seg fortaleciendo el proceso de transformación del sistema eléctrico.

'Tenemos que desarrollar acciones para que este proceso transformacional sea exitoso y dispongamos de un suministro eléctr resiliente, confiable, seguro y costo-efectivo. Todo para que esa transición llegue a todos y, lo más importante, sea justa', puntu Olmedo.

En lo que respecta a proyecciones, el profesional enfatiza que están comenzando a advertir una recuperación de la demanda e Una señal de un mayor dinamismo que también refleja un cambio en el funcionamiento de la economía del país y sus activida asociadas.

'Esperamos que se activen todos los proyectos de generación de energía renovable y de infraestructura de transmisión. Esas serán las principales fuentes de inversión en el sector, además de la relevante meta fijada por el Ministerio de Energía de tener 5.000 Megawatts en plantas de hidrógeno verde al año 2025. Necesitamos nueva infraestructura y el mundo entero está requiriendo proyectos como los últimos mencionados', anticipa el experto.

Se trata de una serie de proyectos e inversiones claves para impulsar el desarrollo y el crecimiento del sector eléctrico, un objetivo para el que todos los actores del sistema ya están trabajando.

Fuente: **Diario Financiero**

Proyectos de Energía Renovable
Para el 2025 Plantas de Hidrogeno Verde con capacidad de generación de 5.000 MW

Agenda

- Sistema Eléctrico Nacional
- Estándar de Ciberseguridad
- Ciberseguridad en Industrial Control System “ICS”
  - Desafíos, Riesgos, Amenazas ICS
  - Modelo y Soluciones

Estándar Ciberseguridad - SEN

El Coordinador Eléctrico Nacional Presenta el Estándar de Ciberseguridad para el Sector Eléctrico Nacional

COORDINADOR ELÉCTRICO NACIONAL

ESTÁNDAR DE CIBERSEGURIDAD PARA EL SECTOR ELÉCTRICO

Octubre 2020

Julio - 2020

Coordinador presentó Estándar de Ciberseguridad para el Sector Eléctrico Nacional

El documento establece requisitos y medidas de control para el resguardo de la seguridad cibernética aplicables al sector eléctrico con el fin de proteger las instalaciones eléctricas y activos informáticos contra amenazas que puedan poner en riesgo la seguridad y continuidad del servicio del Sistema Eléctrico Nacional.

(Santiago, 27 de julio de 2020) La creciente interconectividad y la dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente la exposición al riesgo de los gobiernos, las empresas y las personas, a una gran variedad de actos relacionados con la delincuencia, el espionaje y la ciberseguridad. Los gobiernos y las empresas reconocen la necesidad de tener políticas y estrategias nacionales de ciberseguridad, cultura en ciberseguridad, educación, formación y competencias en seguridad, marcos jurídicos, reglamentos, normativas y estándares, así como contar con la cooperación e intercambio de información.

Los incidentes que han ocurrido en los últimos años han ocasionado que tanto los gobiernos, como las instituciones y organizaciones sean más conscientes de la necesidad de adoptar medidas para controlar los riesgos de ciberseguridad. En la medida que la industria se desarrolla e incrementa sus niveles de transformación, la ciberseguridad toma mayor relevancia.

Es por este motivo, y de acuerdo a lo instruido por los oficios N°3377 del 25 de junio de 2018 y N°11508 del 3 de junio de 2019 emitidos por la Superintendencia de Electricidad y Combustible (SEC), que el Coordinador publicó esta semana el ***Estándar de Ciberseguridad para el Sector Eléctrico***.

Este documento establece requisitos y medidas de control para el resguardo de la seguridad cibernética con el fin de proteger las instalaciones eléctricas y activos informáticos contra amenazas que puedan poner en riesgo la seguridad y continuidad del servicio del Sistema Eléctrico Nacional.

En su elaboración, se analizaron exhaustivamente las diferentes normativas internacionales existentes en materia de ciberseguridad para el sector eléctrico, y junto al apoyo especializado de CAISO (California Independent System Operator), el Coordinador ha definido adoptar el estándar CIP (Critical Infrastructure Protection) de NERC (North American Electric Reliability Corporation), en adelante "NERC-CIP.

Las consultas que puedan existir en esta materia, deben ser dirigidas a seguridadSEN@coordinador.cl

Estándar Ciberseguridad - SEN

NEOSECURE
SABEMOS DE SEGURIDAD

COORDINADOR
ELÉCTRICO NACIONAL

CIP-002: Ciber Seguridad - Categorización de Ciber Sistemas SEN
CIP-003: Ciber Seguridad – Controles de Gestión de la Seguridad
CIP-004: Ciber Seguridad – Personal y Capacitación
CIP-005: Ciber Seguridad – Perímetro de Seguridad Electrónica (PSE)
CIP-006: Ciber Seguridad – Seguridad Física de Ciber Sistemas SEN
CIP-007: Ciber Seguridad – Gestión de la Seguridad de Sistemas
CIP-008: Ciber Seguridad – Reporte de Incidentes y Planes de Respuesta
CIP-009: Ciber Seguridad – Planes de Recuperación para Ciber Sistemas SEN
CIP-010: Ciber Seguridad – Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades
CIP-011: Ciber Seguridad – Protección de Información
CIP-012: Ciber Seguridad – Comunicaciones entre Centros de Control
CIP-013: Ciber Seguridad – Gestión de Riesgos en la Cadena de Suministros
CIP-014: Ciber Seguridad – Seguridad Física

CIP-001-1 — Sabotage Reporting
Purpose: Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

Estándar Ciberseguridad - SEN

NEOSECURE
SABEMOS DE SEGURIDAD

COORDINADOR
ELÉCTRICO NACIONAL

CIP-003: Ciber Seguridad – Controles de Gestión de la Seguridad

7.2.3. Requerimientos (R) y Medidas de Control (M)

R1. Cada Entidad Responsable deberá revisar y obtener aprobación del Encargado CIP, al menos una vez cada 15 meses calendario, de una o más políticas de ciberseguridad documentadas que en su conjunto aborden los siguientes aspectos:

a) Para Ciber Sistemas SEN de Impacto Alto y Medio:

- Personal y capacitación (CIP-004);
- Perímetro(s) de Seguridad Electrónica (CIP-005), incluyendo Acceso Remoto Interactivo;
- Seguridad Física de Ciber Sistemas SEN Críticos (CIP-006);
- Gestión de Seguridad del Sistema (CIP-007);
- Reportes de Incidentes y Planes de Respuesta (CIP-008);
- Planes de Recuperación para Ciber Sistemas Críticos (CIP-009);
- Gestión de Cambio de Configuraciones y Evaluación de Vulnerabilidades (CIP-010);
- Protección de la Información (CIP-011);
- Seguridad Física (CIP-014); y
- Declaración y respuesta a Circunstancias Excepcionales CIP

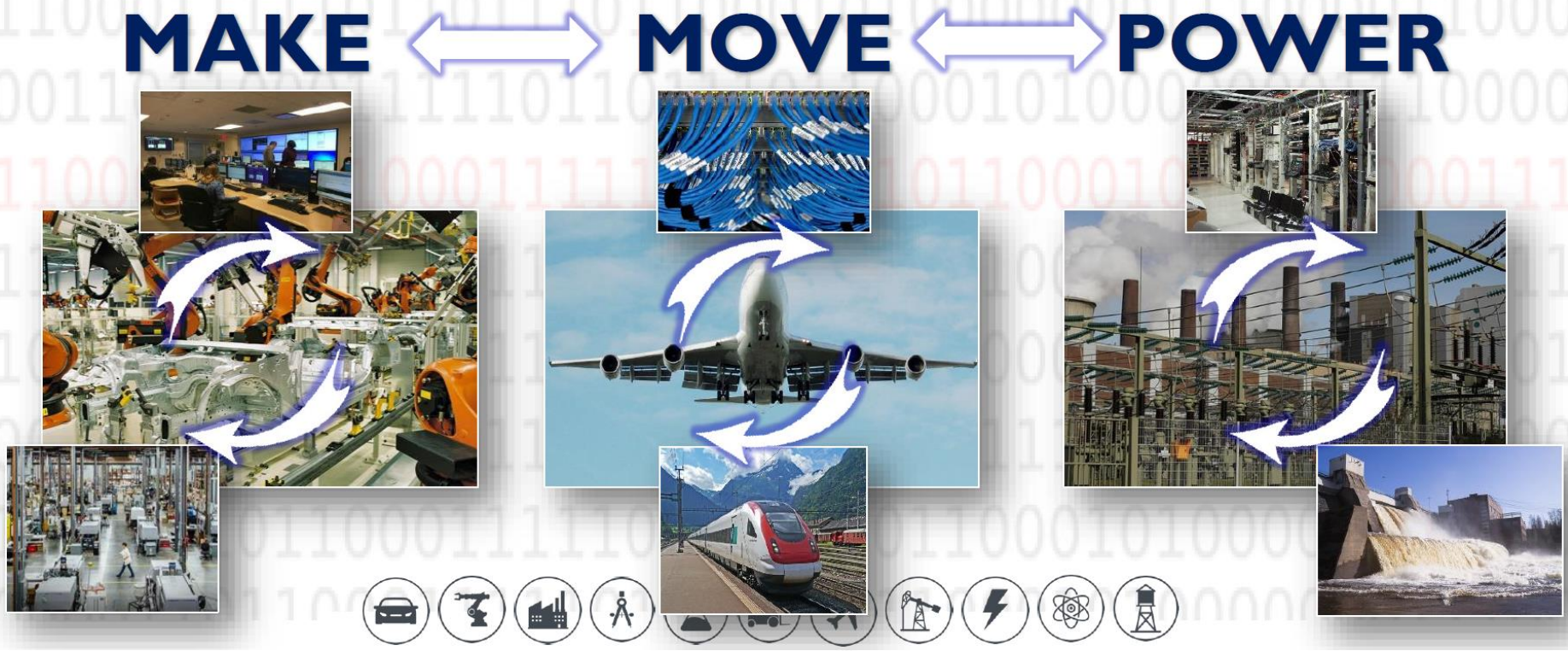
Agenda

- Sistema Eléctrico Nacional
- Estándar de Ciberseguridad
- Ciberseguridad en Industrial Control System “ICS”
  - Desafíos, Riesgos, Amenazas ICS
  - Modelo y Soluciones

Historia de la Industria

NEOSECURE
SABEMOS DE SEGURIDAD

Digitalización Industrial “Industria 4.0”



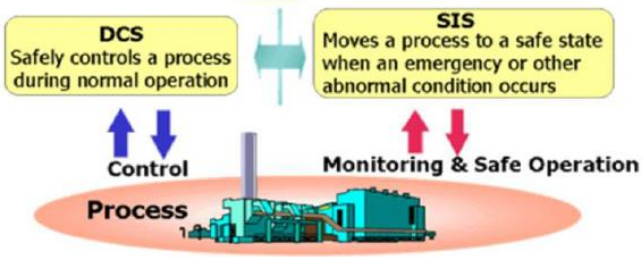
Aparición de los Sistemas de Control Industrial Control System “ICS”

NEOSECURE
SABEMOS DE SEGURIDAD

Supervisory Control And Data Acquisition (SCADA)


Process Control Systems (PCS)


Distributed Control Systems (DCS) & Safety Instrumented System (SIS)

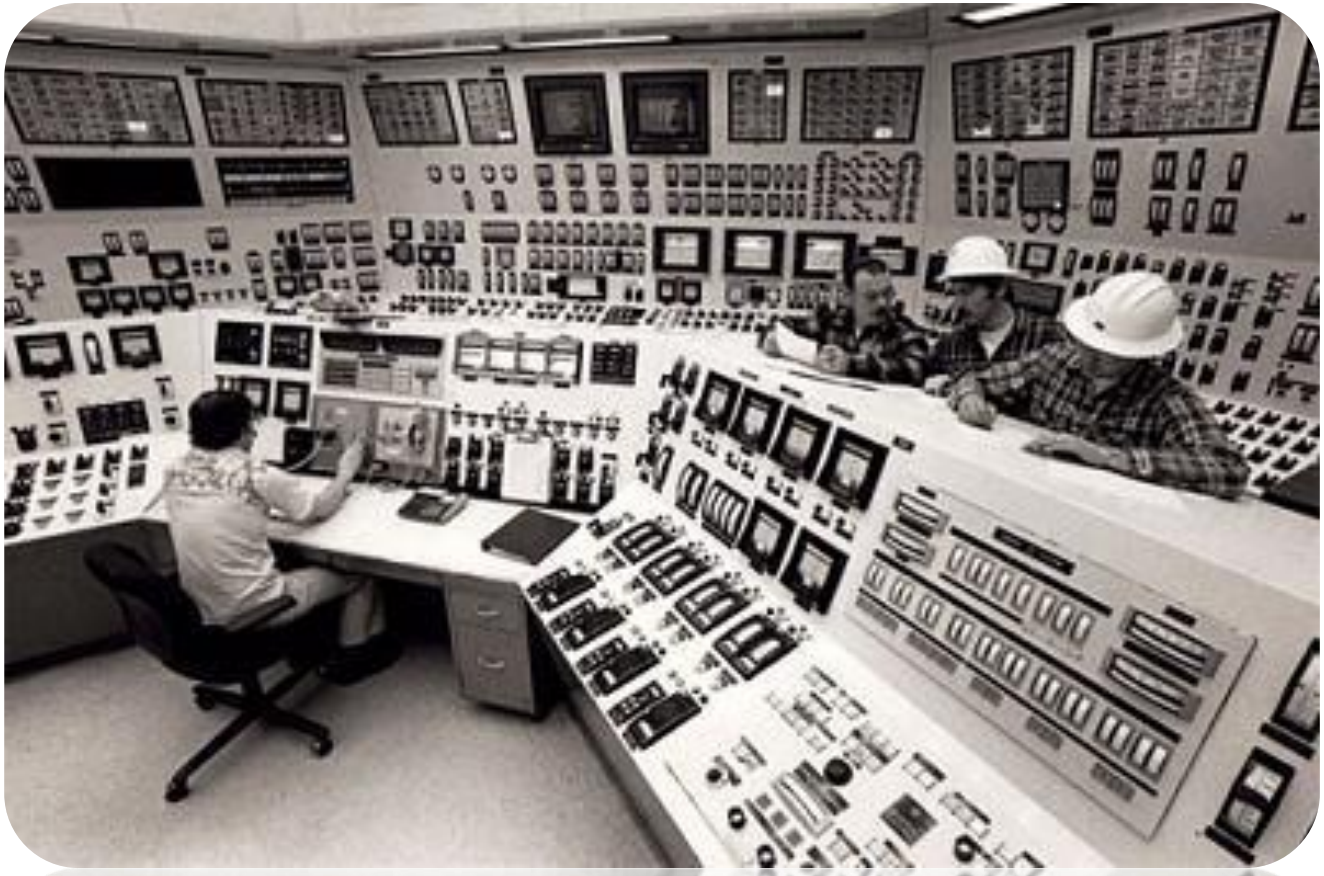


Automation Systems


Porque la Seguridad en Sistemas de Control Industrial ICS

NEOSECURE
SABEMOS DE SEGURIDAD

Este es un centro de Control de las generaciones anteriores



Porque la Seguridad en Sistemas de Control Industrial ICS

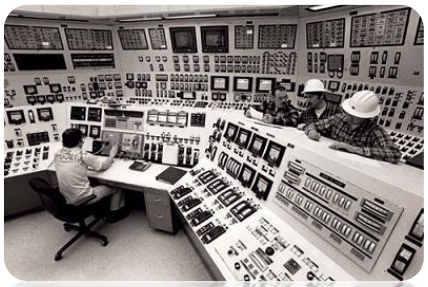
NEOSECURE
SABEMOS DE SEGURIDAD

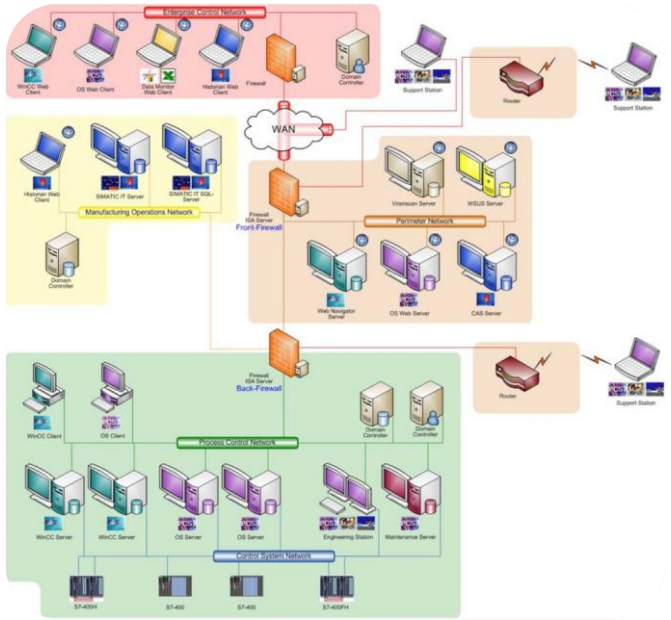
Estos son los centros de Control Actuales

Seguridad por “Air Gap” en ICS

NEOSECURE
SABEMOS DE SEGURIDAD

Los sistemas de control están aislados por “Air Gap” de los demás sistemas

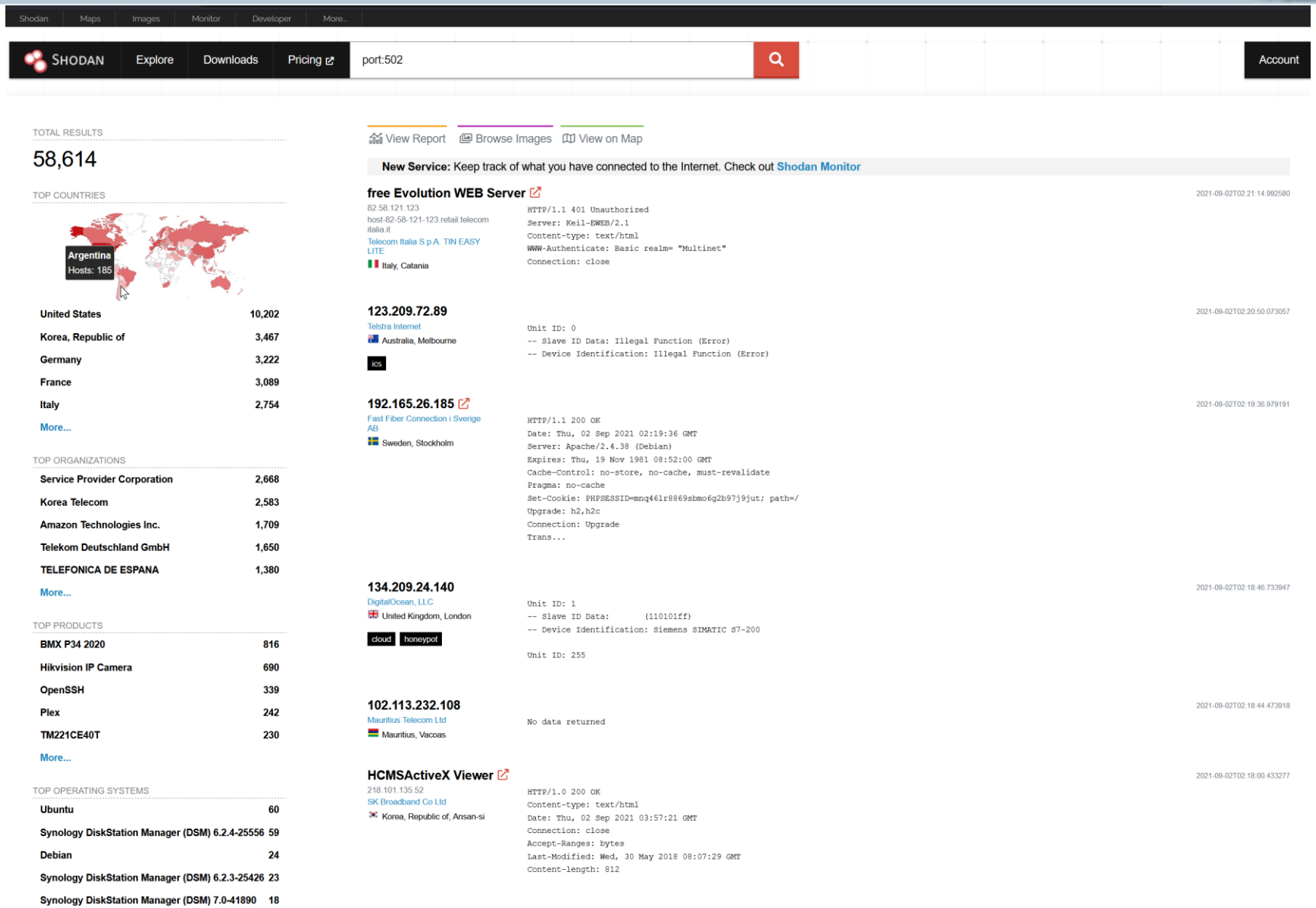




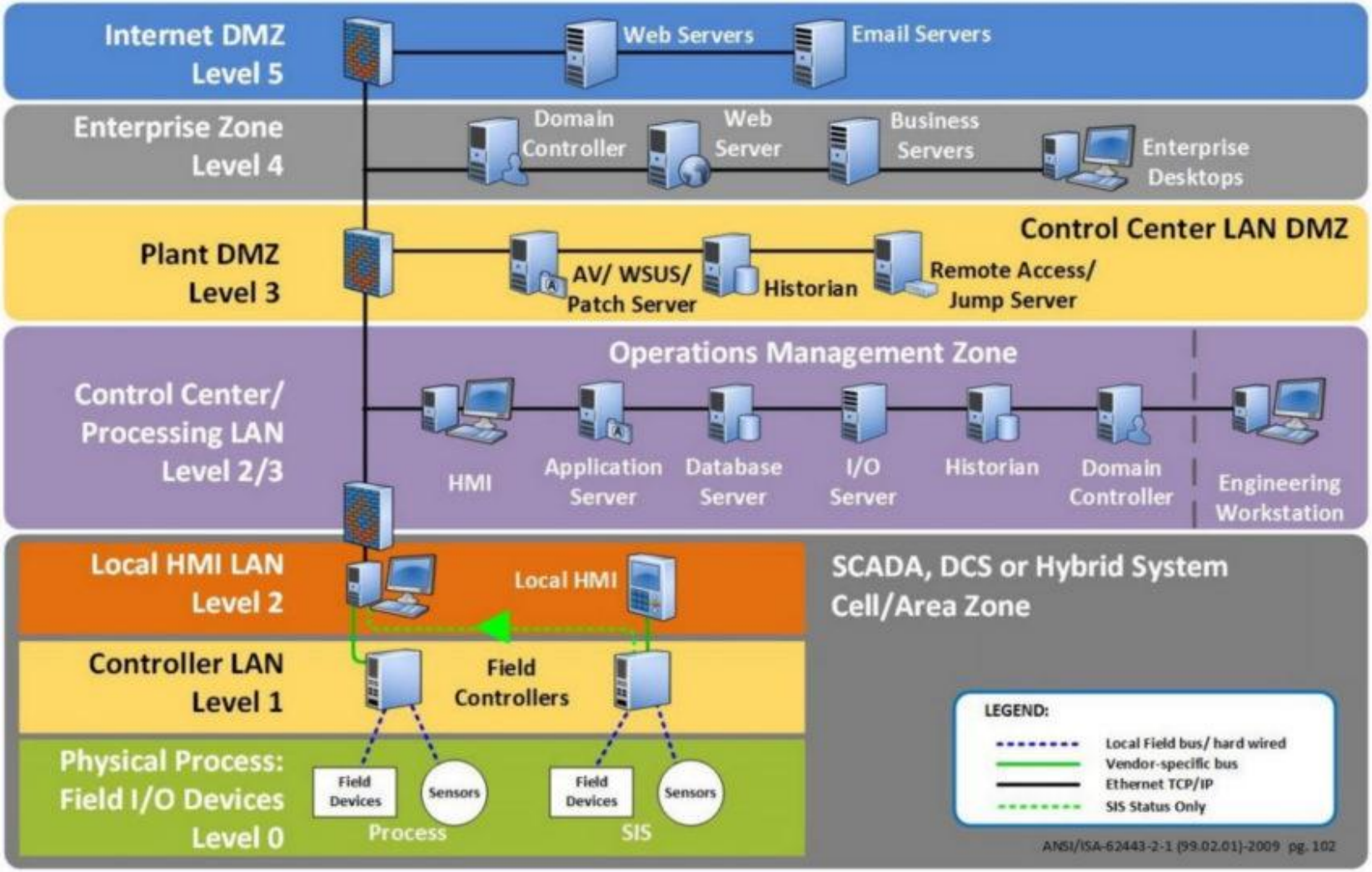
Los sistemas de control hoy NO están aislados de los demás sistemas por “air gap”, eso es historia

Acceso a ICS visibles de Internet

NEOSECURE
SABEMOS DE SEGURIDAD



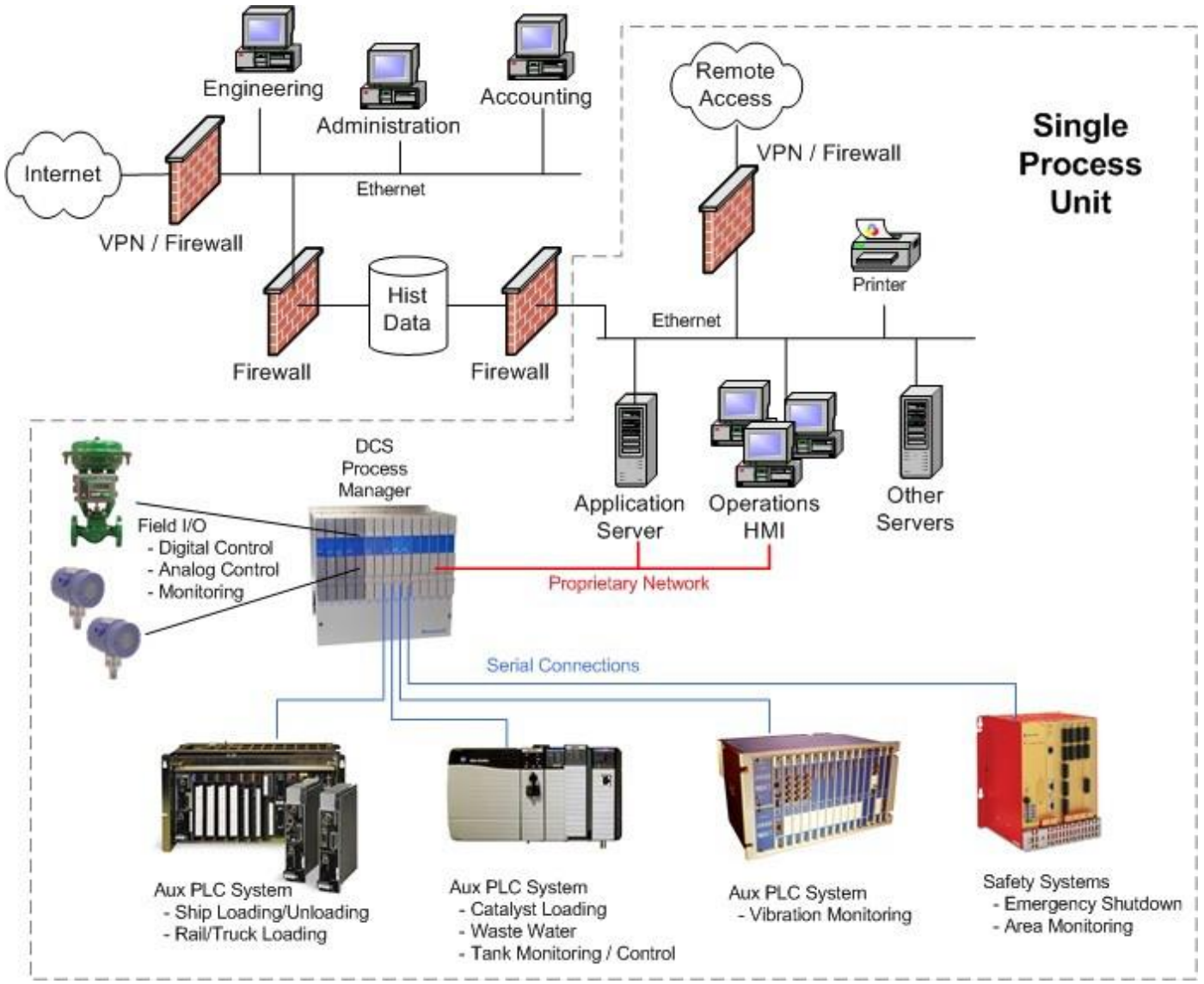
Modelo Purdue
ISA/IEC 62443 - Actualidad



Purdue Enterprise Reference Architecture (PERA) is a 1990s reference model for enterprise architecture, developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.

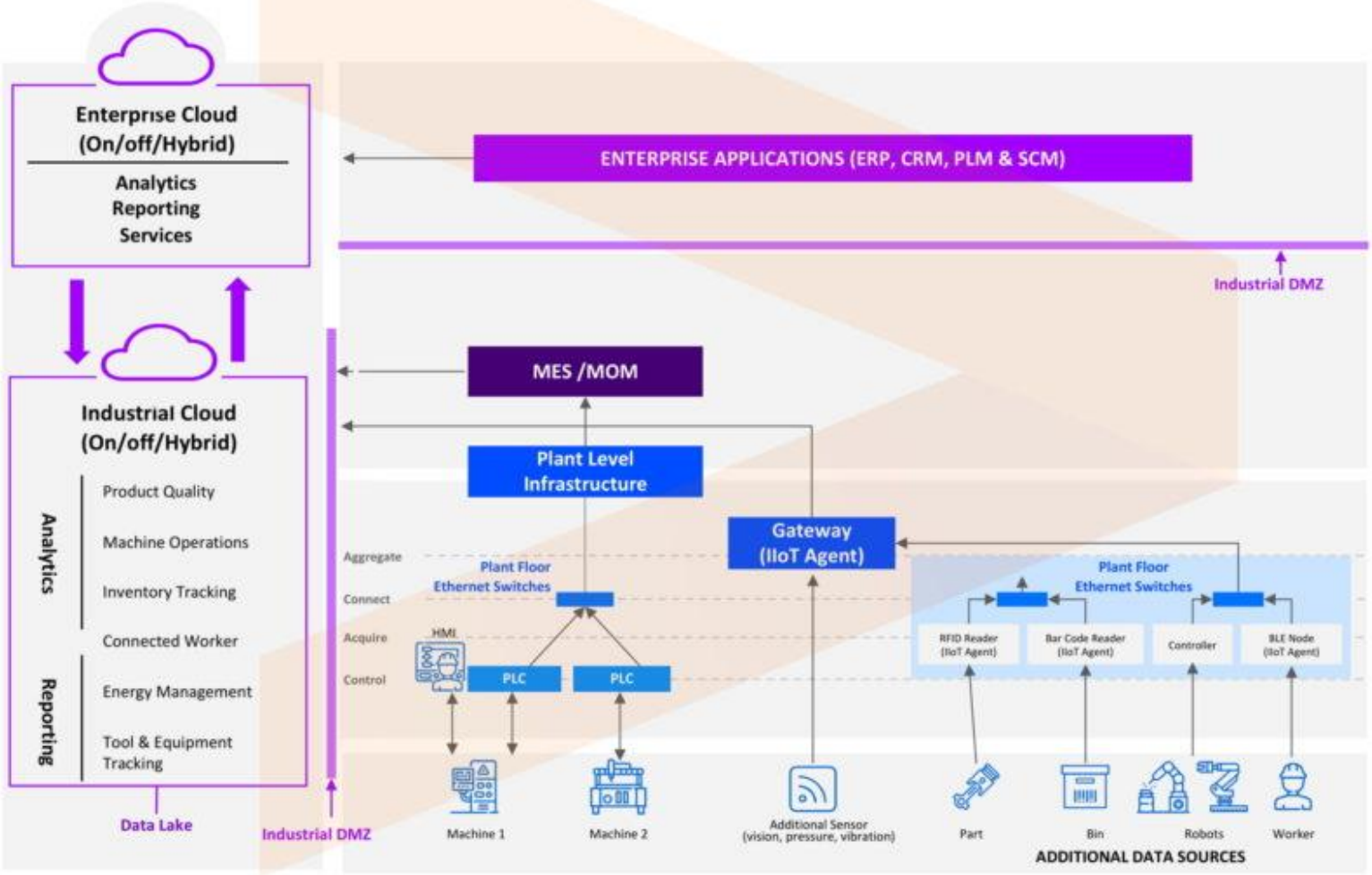
Arquitectura ICS

Implementación Básica



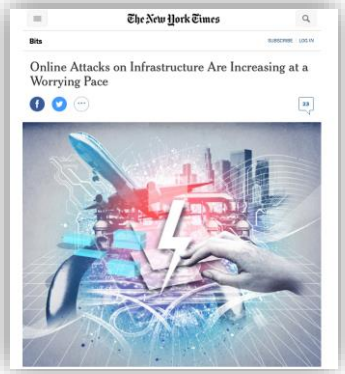
Modelo ICS CLOUD-ORIENTED “Uso IIoT” (Industrial IoT) “Nuevo Desafío”

NEOSECURE
SABEMOS DE SEGURIDAD



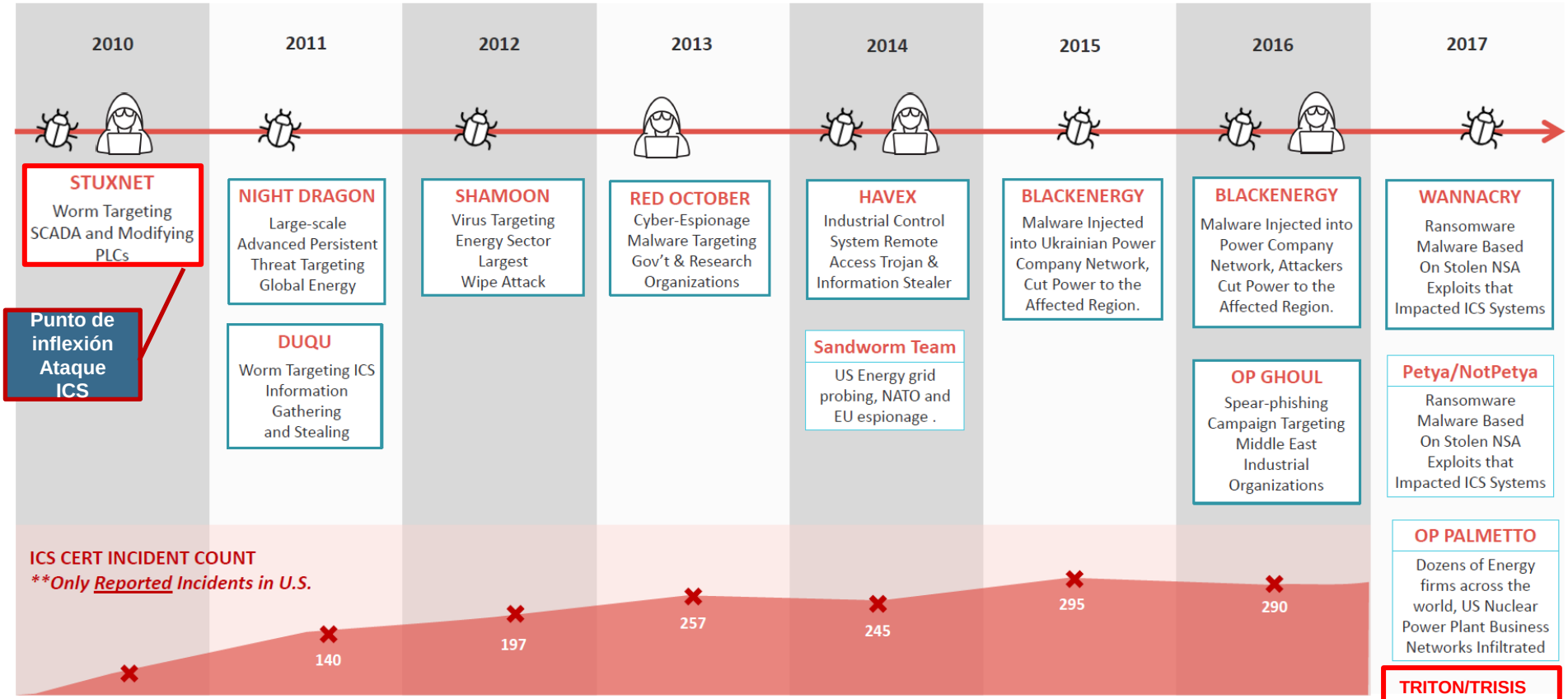
Escenario de Amenazas

NEOSECURE
SABEMOS DE SEGURIDAD

Estados	Insiders	Terroristas	Hacktivistas	Ciber Criminales
				
Ataques a infraestructura crítica	Empleados disconformes o Herramienta de huelgas y negociaciones	Acciones para atemorizar	Acciones frente a proyectos o empresas	Extorsión con Ransomware

La Infraestructura ICS bajo Continuo Ataque

NEOSECURE
SABEMOS DE SEGURIDAD



Los 10 peores incidentes de Ciberseguridad en 2020

- SolarWinds, FireEye, otras
- Vacunas contra el COVID-19
- Ransomware Principal amenaza 2020
- Contraseñas Filtradas {275 Millones}
- Phishing “aún seguimos picando”
- Hackeo a Twitter
- El código Fuente de Windows XP filtrado
- Correo Electrónico {7 de cada 10 amenazas llegan por esa vía}
- Dispositivos desprotegidos y teletrabajo {37 de cada 100}
- Cafeteras Hackeadas ¿El IoT se nos ha ido de las manos?

Referencia: https://www.muycomputer.com/2020/12/30/ciberseguridad-en-2020/

Ataque Ransomware

NEOSECURE
SABEMOS DE SEGURIDAD

El “**ciberataque” de Colonial Pipeline**

Tuvo lugar entre el jueves 6 de mayo y el viernes 7 de mayo de 2021

Ataque de malware que los obligó a cerrar su sistema.

El ataque detuvo todas las operaciones del oleoducto.

Colonial Pipeline dijo que el ataque afectó a algunos de sus sistemas de información.

El presidente Joe Biden declaró el estado de emergencia el domingo 9 de mayo.

Una fuente dijo que el ataque fue llevado a cabo por una empresa criminal de ransomware llamada DarkSide

Se cree que el mismo grupo robó 100 gigabytes de datos de los servidores de la empresa el día antes del ataque de malware.

El ataque a Colonial Pipeline se originó con el robo de una sola contraseña

La cuenta VPN que fue comprometida, y que ya fue desactivada, no usaba, además, autenticación multifactor.

Estados Unidos ha recuperado parte de los **4,4 millones de dólares** pagados por Colonial Pipeline al grupo de piratas informáticos **DarkSide** tras haber sido objeto de un **ataque de *ransomware***. Así lo ha confirmado **Paul Abbate**, subdirector del FBI. Un profesional que ha precisado que se han recuperado **63,7 *bitcoins*** (unos **2,3 millones de dólares**) de los 75 pagados.

Ataques de Ransomware

NEOSECURE
SABEMOS DE SEGURIDAD

Los ataques de 'ransomware', al alza

Los casos de Colonial Pipeline y, posteriormente, la empresa cárnica JBS han generado preocupación en la Casa Blanca. Al respecto, **Gina Raimondo**, secretaria de Comercio de Estados Unidos, ha asegurado que «**los ataques de *ransomware* han llegado para quedarse y es lógico pensar que se intensificarán**».

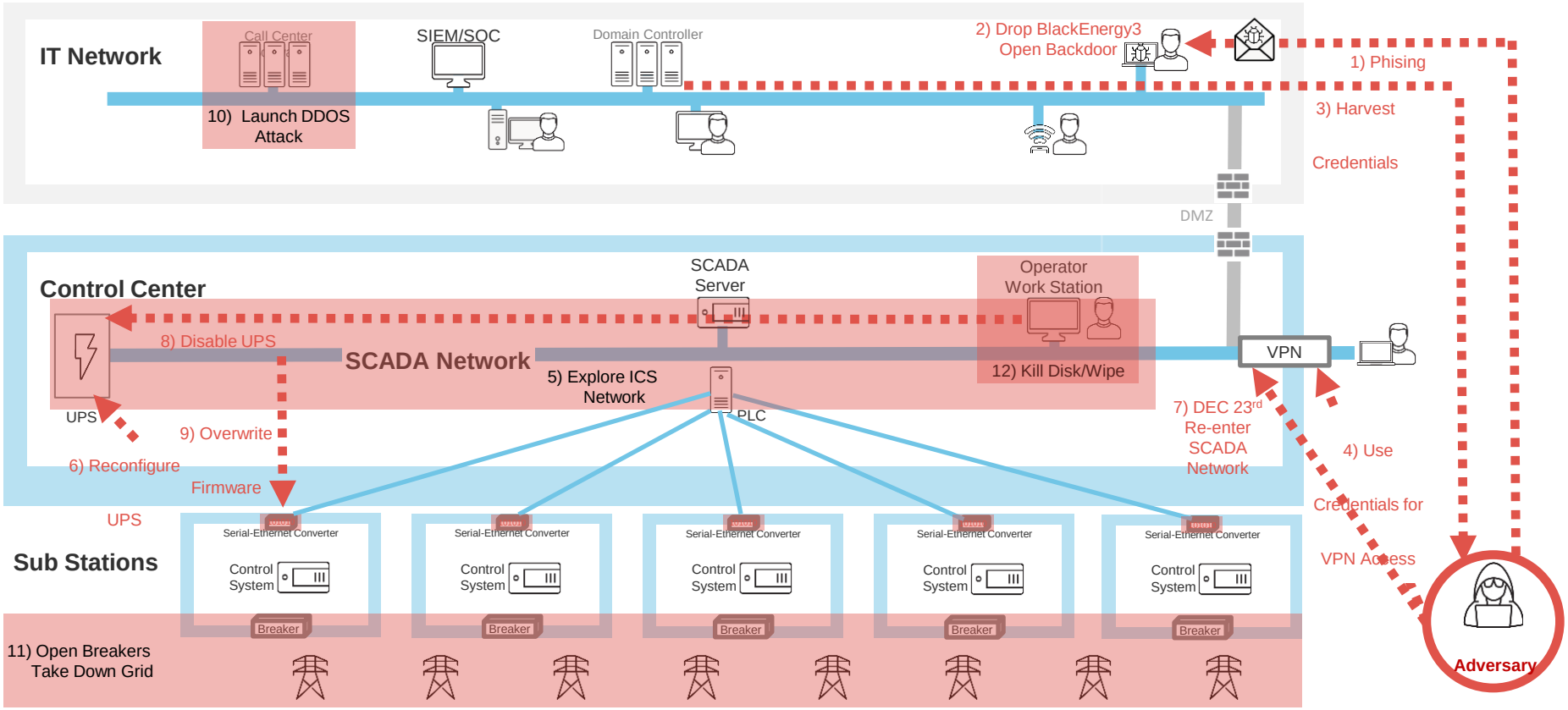
Por otra parte, un reciente estudio de ciberseguridad realizado por los investigadores de **Check Point** pone de manifiesto que **los ataques de *ransomware* han aumentado un 56 por ciento** a nivel mundial desde principios de año.

Ataque Real en Ucrania “Red de Distribución Eléctrica” Diciembre 2015

LOS ATACANTES Y SUS MOTIVOS AUN NO SON CONOCIDOS

Ataque en Ucrania “Electric Grid” Dic. 2015

NEOSECURE
SABEMOS DE SEGURIDAD



Actividad Maliciosa en Internet

Muestra Algunos Grupos Activos Ataques a ICS

NEOSECURE
SABEMOS DE SEGURIDAD

THREAT ACTIVITY GROUPS

HEXANE

PARISITE

MAGNALLIUM

WASSONITE

XENOTIME

DYMALLOY

ALLANITE

CHRYSENE

RASPITE

ELECTRUM

COVELLITE

ELECTRUM

ELECTRUM IS RESPONSIBLE FOR THE CRASHOVERRIDE MALWARE ATTACK WHICH SUCCESSFULLY BLACKED OUT PORTIONS OF KIEV, UKRAINE IN DECEMBER 2016. IT IS ASSOCIATED WITH THE SANDWORM GROUP.[50]

CRASHOVERRIDE: The Malware That Attacks Power Grids

Dymalloy, Electrum, and Xenotime Hacking Groups Set Their Targets on US Energy Sector

Algunos Grupos de Ataques a los ICS (15)

NEOSECURE
SABEMOS DE SEGURIDAD

MAGNALIO

DESDE 2017

Red de TI limitada, recopilación de información contra organizaciones industriales

RASPITE

DESDE 2017

Red de TI limitada, recopilación de información sobre servicios eléctricos con algunas similitudes con CRISENO

HEXANO

DESDE 2018

Compromiso de TI y recopilación de información contra entidades de ICS

PARISITA

DESDE 2017

Compromiso VPN de las redes de TI para realizar reconocimientos

WASSONITE

DESDE 2018

Compromiso de TI y recopilación de información

ALANITA

DESDE 2017

Watering-hole y phishing que conducen al reconocimiento ICS y la recopilación de capturas de pantalla

CRISENO

DESDE 2017

Compromiso de TI, recopilación de información y reconocimiento contra organizaciones industriales

Algunos Casos de Ataques & Costos

NEOSECURE
SABEMOS DE SEGURIDAD

2016

Duke Energy
Electric Power C

CYBER COMPL
Failure to Meet
Cyber Security S

COST
$10 million

Basados en su plan de respuesta a incidentes de ciberseguridad, lograron recuperar su plataforma afectada de 4.000 Servidores, 45.000 PC y 2.500 aplicaciones en solo 10 días.

Maersk had to undertake an almost complete infrastructure overhaul. They reinstalled 4,000 servers, 45,000 PCs and 2,500 applications over the course of ten days, a process that would normally have taken six months to implement.[4]

2017

A.P. Moller Maersk
Shipping and Logistics

CYBER INCIDENT
Ransomware: NotPetya

COST
$300 million

2019

Norsk Hydro
Metals and Mining

CYBER INCIDENT
Ransomware: LockerGoga

COST
$70 million

Desafíos de Redes Industriales

NEOSECURE
SABEMOS DE SEGURIDAD

Inseguras Inherentemente

- Redes planas
- Autenticación débil
- No cifrado
- Protocoles ICS inseguros
- Dificultad de parchar
- Tecnología antigua

Aumento de la conectividad

- Accesos remotos del Vendor equipos OT
- Visibilidad de Información de “Piso de Planta” para la organización
- Programas de analíticos
- Integración a Cadena de Produccion

Falta de colaboración

- Equipos de Planta vs. Seguridad TI
- No hay vista común del ambiente IT/OT
- No hay herramientas de colaboración IT/OT
- Gaps o conflictos de Gobernabilidad

Visibilidad y Seguridad Insuficiente

- No hay visibilidad redes ICS
- Eventos de configuración de red no detectados
- No hay monitoreo de amenazas
- Bajo control del acceso remoto y contraseñas

a ataques básicos

Objetivos de Seguridad OT v/s IT

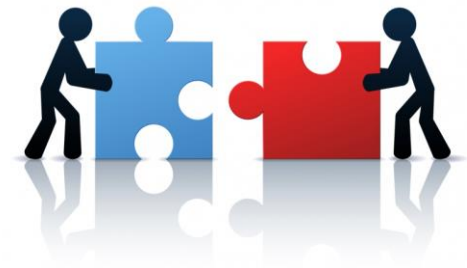
NEOSECURE
SABEMOS DE SEGURIDAD

Operational Technologies “OT”		Information Technologies “IT”
Industrial Automation & Control Systems		General Purpose Information Technology Systems
Availability	Priority	**C**onfidentiality
Integrity		**I**ntegrity
Confidentiality		**A**vailability

Comparison of Objectives

Qué se pide para una solución en ambientes OT

- Específica al Ambiente OT
- Baja Intrusividad
- Controles de Impacto Inmediato
- Protección Continua

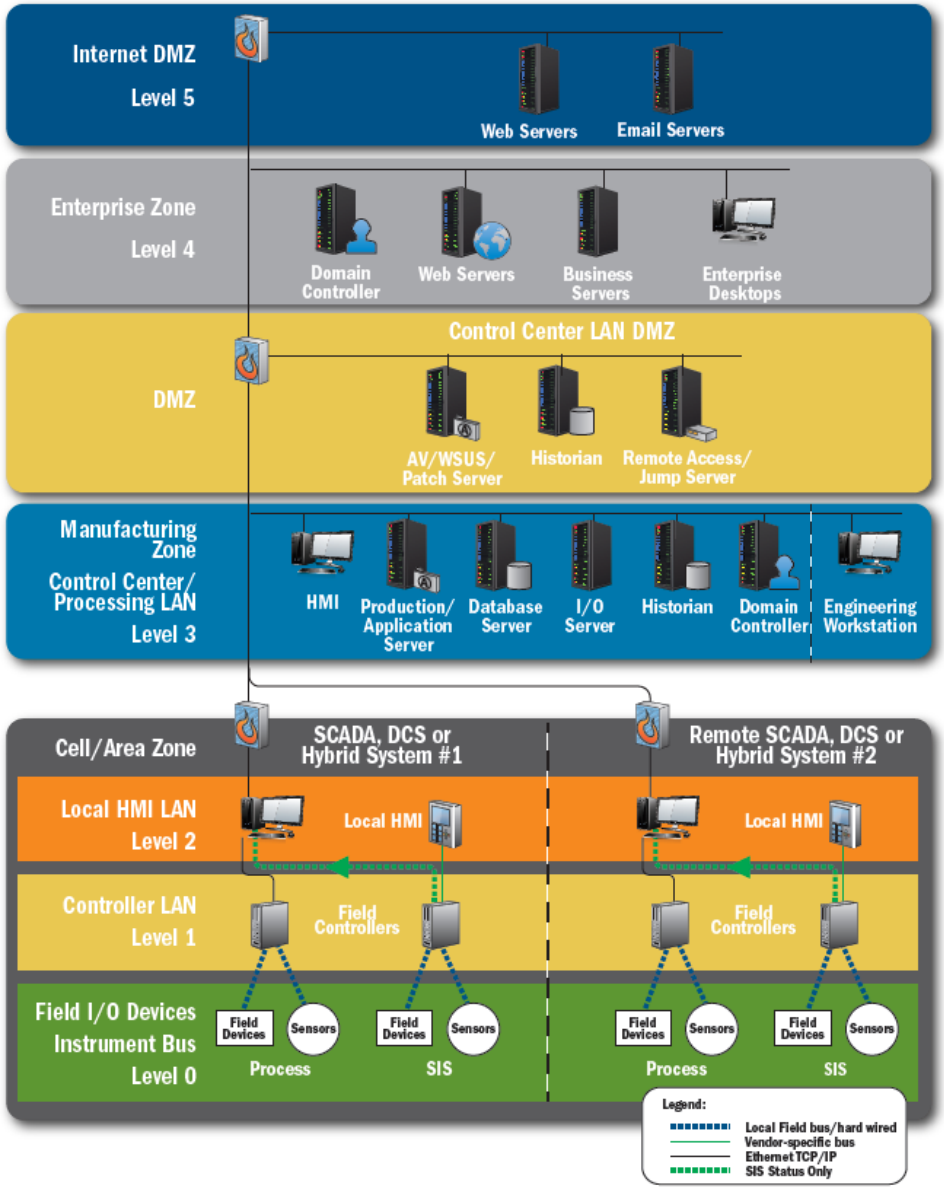


Agenda

- **Ciberseguridad en Industrial Control System “ICS”**
  - **Desafíos, Riesgos, Amenazas ICS**
  - **Modelo y Soluciones**

Estrategia de Protección

- Visibilidad en la Red Industrial
- Controlar los Perímetros
- Controlar Acceso Usuarios
- Detección y prevención de ataques
- Plan de Contingencia
- Implementación ISA/IEC 62443 u otra
  - Bloqueo Trafico Saliente
  - Listas Blancas
  - No uso de Mail en Red OT



Modelo

Seguridad de Neosecure Para Redes Industrial ICS - OT

NEOSECURE
SABEMOS DE SEGURIDAD

Anticipar

- Evaluación Buenas Practicas y estándares
- Inventario Redes Industriales
- Inteligencia de la Amenaza

Prevenir

- Separación & Segregación Red OT de IT
- Segmentación Red OT
- Accesos Usuarios
- Control Accesos Red
- Manejo de Credenciales
- Malware

Detectar

- Monitorear Trafico Red
- Detección Anomalías
- Monitorear Cambios y Nuevos Dispositivos
- Ataques

Responder

- Orquestar Respuestas
- Análisis Forense

Servicios & Soluciones

Seguridad de Neosecure Para Redes Industrial ICS - OT

NEOSECURE
SABEMOS DE SEGURIDAD

Anticipar

- Evaluación Redes OT
- Monitoreo Oper & Seg
- Inteligencia de la amenaza

Prevenir

- Unidirectional Gateways
- Firewall Next Generation
- Control Accesos
- Control EndPoint
- Monitoreo Operación y Seguridad

Detectar

- Monitoreo Operación y Seguridad

Responder

- Monitoreo Operación y Seguridad
- Equipo Respuestas Incidentes

Evaluación de Redes OT

NEOSECURE
SABEMOS DE SEGURIDAD

Evaluación Buenas Practicas y Estándares de Seguridad ICS

- International Society for Automation (ISA 99)
- International Electrotechnical Commission (ISA/IEC 62443)
- National Institute for Standards and Technology (NIST SP800-82)
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- The North American Electrical Reliability Corporation (NERC-CIP)
- Otros especificas a la Industria

Levantamiento Ambiente

- Mapa e Información de Dispositivos
- Mapa de tráfico de red entre Dispositivos

Alcance

- Controles físicos
- Controles de red
- Controles de plataforma
- Controles de aplicaciones
- Mejores prácticas
- Continuidad operativa
- Mapa e Información de Dispositivos
- Mapa de tráfico de red entre Dispositivos

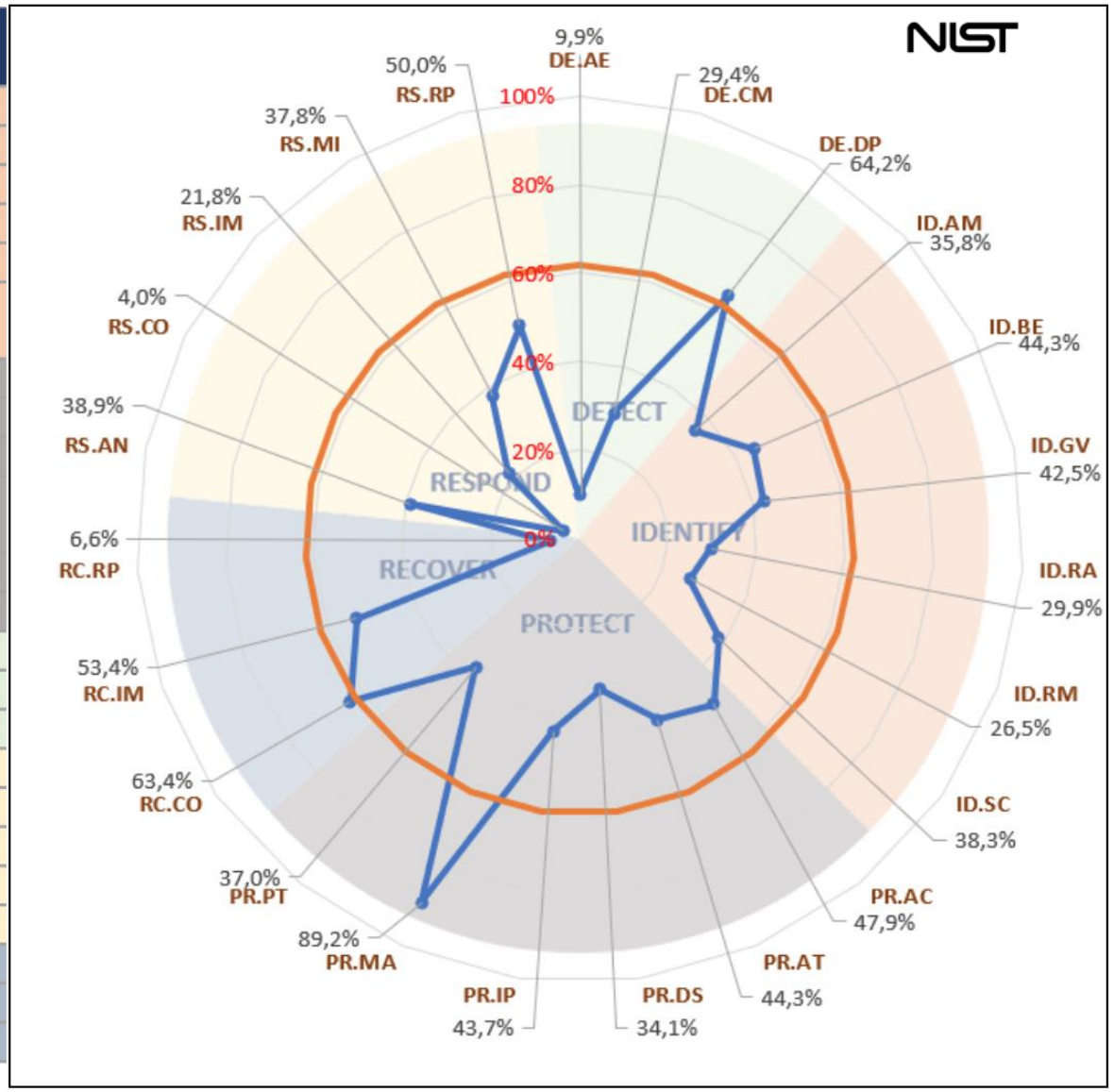
Entregables

- Informe Levantamiento
- Plan de mejoras

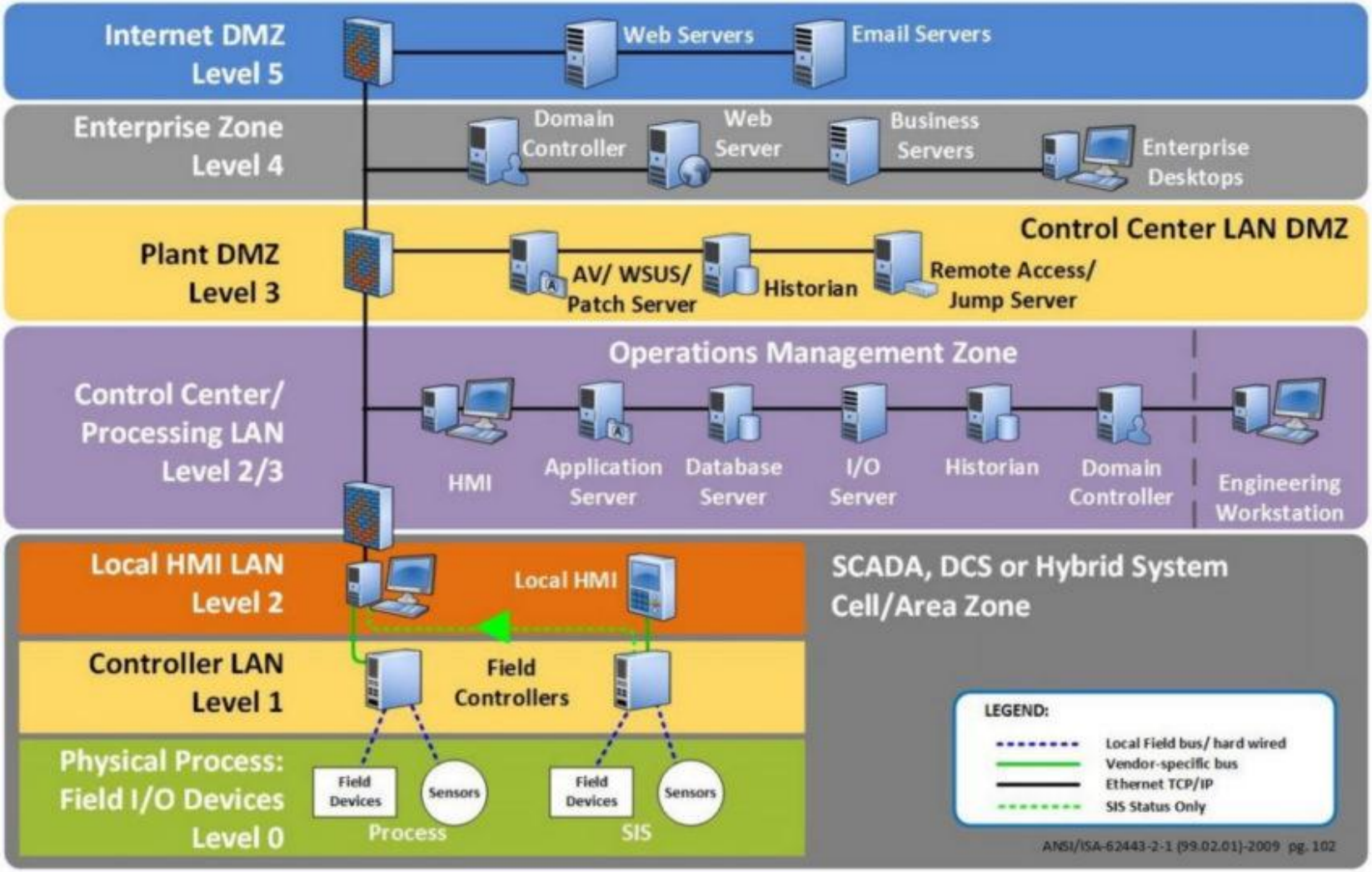
Evaluación de Redes OT - Ejemplo: NIST-800: National Institute of Standards and Technology

NEOSECURE
SABEMOS DE SEGURIDAD

NIST ID	Categoría
ID.AM	Gestión de Activos
ID.BE	Ambiente de Negocio
ID.GV	Governance
ID.RA	Evaluación de Riesgos
ID.RM	Estrategia de gestión de riesgos
ID.SC	Gestión de Riesgos de la Cadena de suministro
PR.AC	Control de Acceso
PR.AT	Sensibllización y Entrenamiento
PR.DS	Seguridad de Datos
PR.IP	Procesos y Procedimientos de Protección de Información
PR.MA	Mantención
PR.PT	Tecnología de Protección
DE.AE	Anomalias y Eventos
DE.DP	Procesos de Detección
DE.CM	Monitoreo continuo de Seguridad
RS.AN	Análisis
RS.CO	Comunicaciones
RS.IM	Mejoras
RS.MI	Mitigación
RS.RP	Planificación de la Respuesta
RC.CO	Comunicaciones
RC.IM	Mejoras
RC.RP	Planificación de la Recuperación



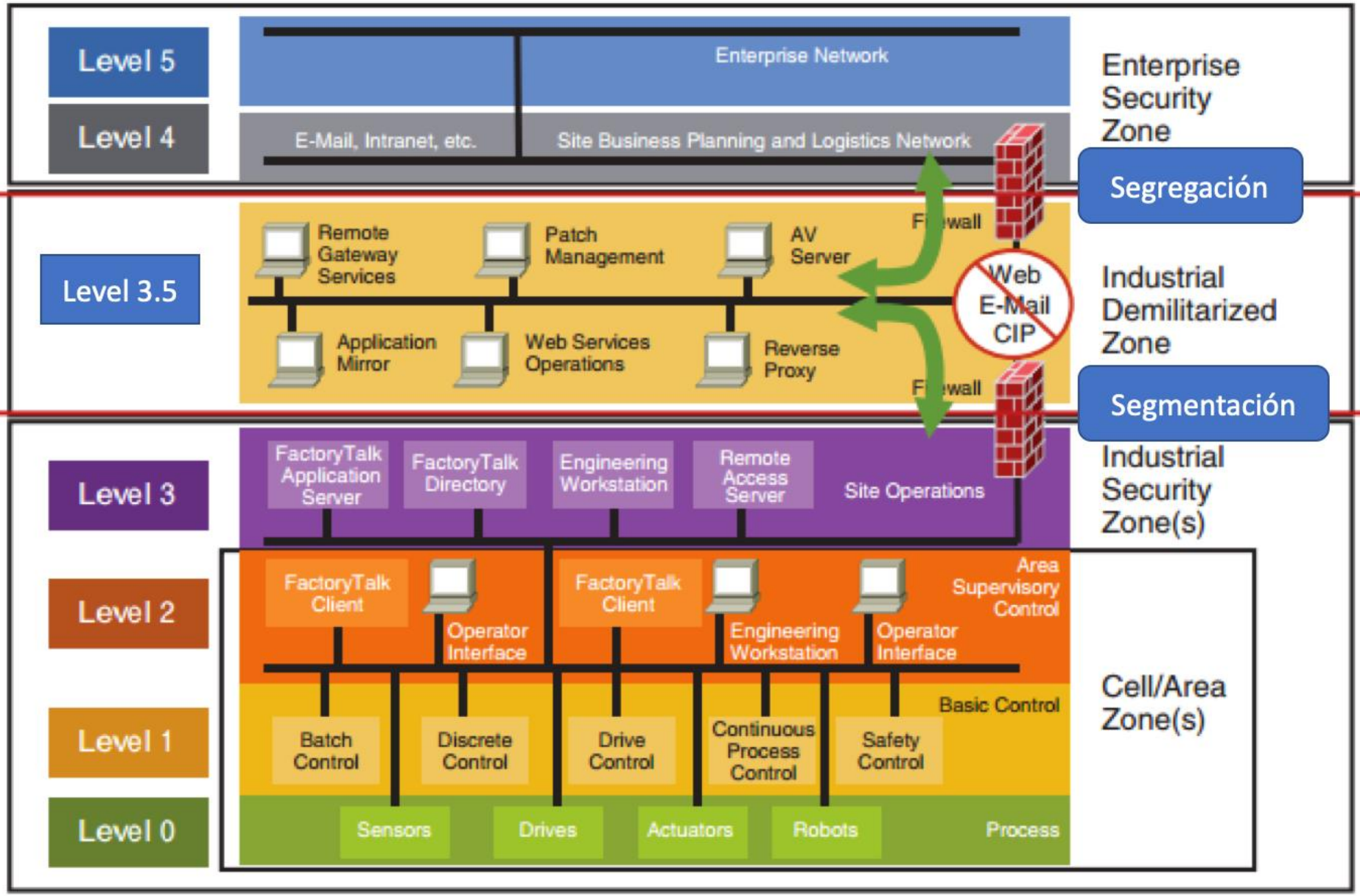
Modelo Purdue
ISA/IEC 62443 - Actualidad



Purdue Enterprise Reference Architecture (PERA) is a 1990s reference model for enterprise architecture, developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.

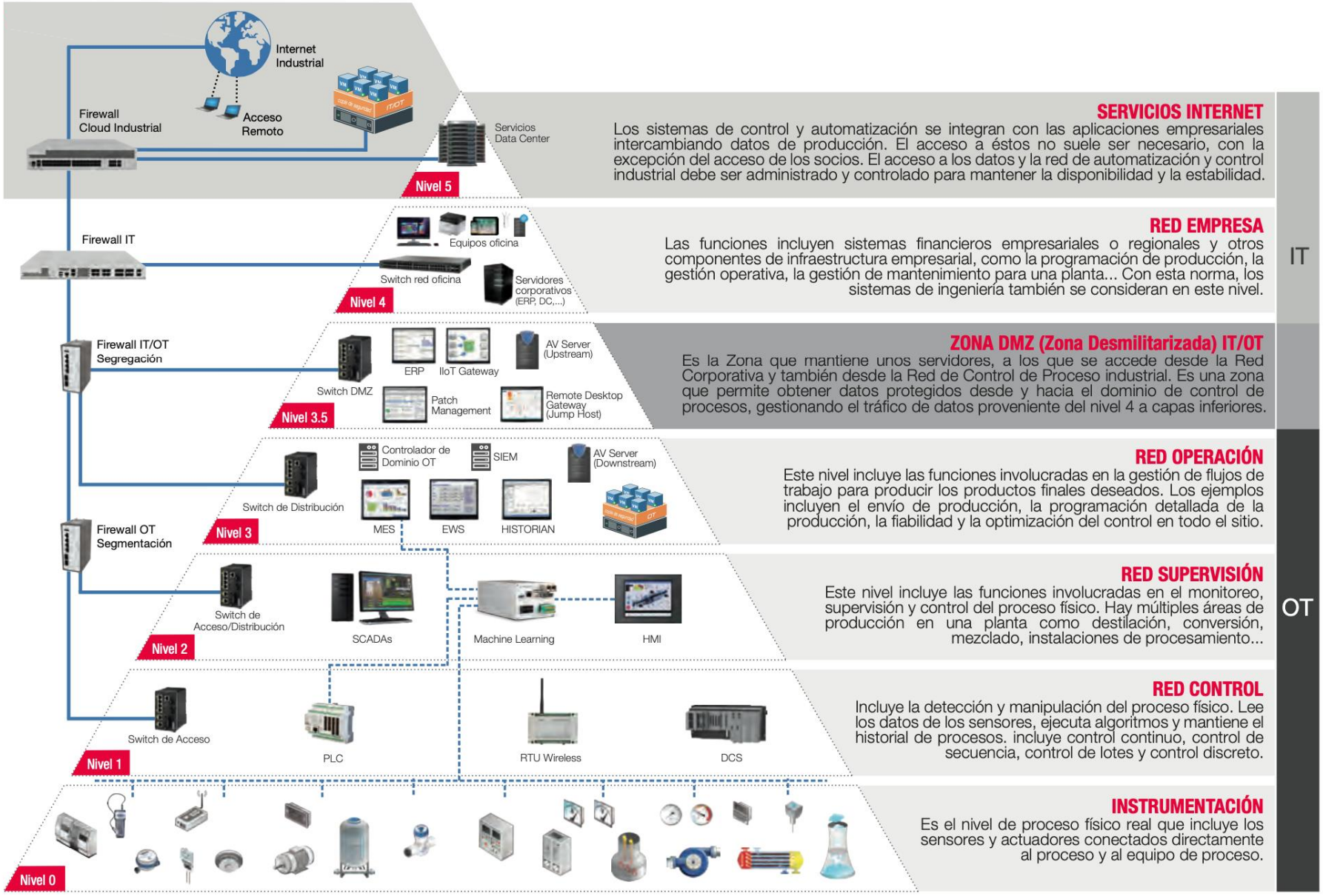
Next Generation Firewall
Segregación & Segmentación

NEOSECURE
SABEMOS DE SEGURIDAD



Segregación & Segmentación

NEOSECURE
SABEMOS DE SEGURIDAD



SERVICIOS INTERNET
Los sistemas de control y automatización se integran con las aplicaciones empresariales intercambiando datos de producción. El acceso a éstos no suele ser necesario, con la excepción del acceso de los socios. El acceso a los datos y la red de automatización y control industrial debe ser administrado y controlado para mantener la disponibilidad y la estabilidad.

RED EMPRESA
Las funciones incluyen sistemas financieros empresariales o regionales y otros componentes de infraestructura empresarial, como la programación de producción, la gestión operativa, la gestión de mantenimiento para una planta... Con esta norma, los sistemas de ingeniería también se consideran en este nivel.

IT

ZONA DMZ (Zona Desmilitarizada) IT/OT
Es la Zona que mantiene unos servidores, a los que se accede desde la Red Corporativa y también desde la Red de Control de Proceso industrial. Es una zona que permite obtener datos protegidos desde y hacia el dominio de control de procesos, gestionando el tráfico de datos proveniente del nivel 4 a capas inferiores.

RED OPERACIÓN
Este nivel incluye las funciones involucradas en la gestión de flujos de trabajo para producir los productos finales deseados. Los ejemplos incluyen el envío de producción, la programación detallada de la producción, la fiabilidad y la optimización del control en todo el sitio.

RED SUPERVISIÓN
Este nivel incluye las funciones involucradas en el monitoreo, supervisión y control del proceso físico. Hay múltiples áreas de producción en una planta como destilación, conversión, mezclado, instalaciones de procesamiento...

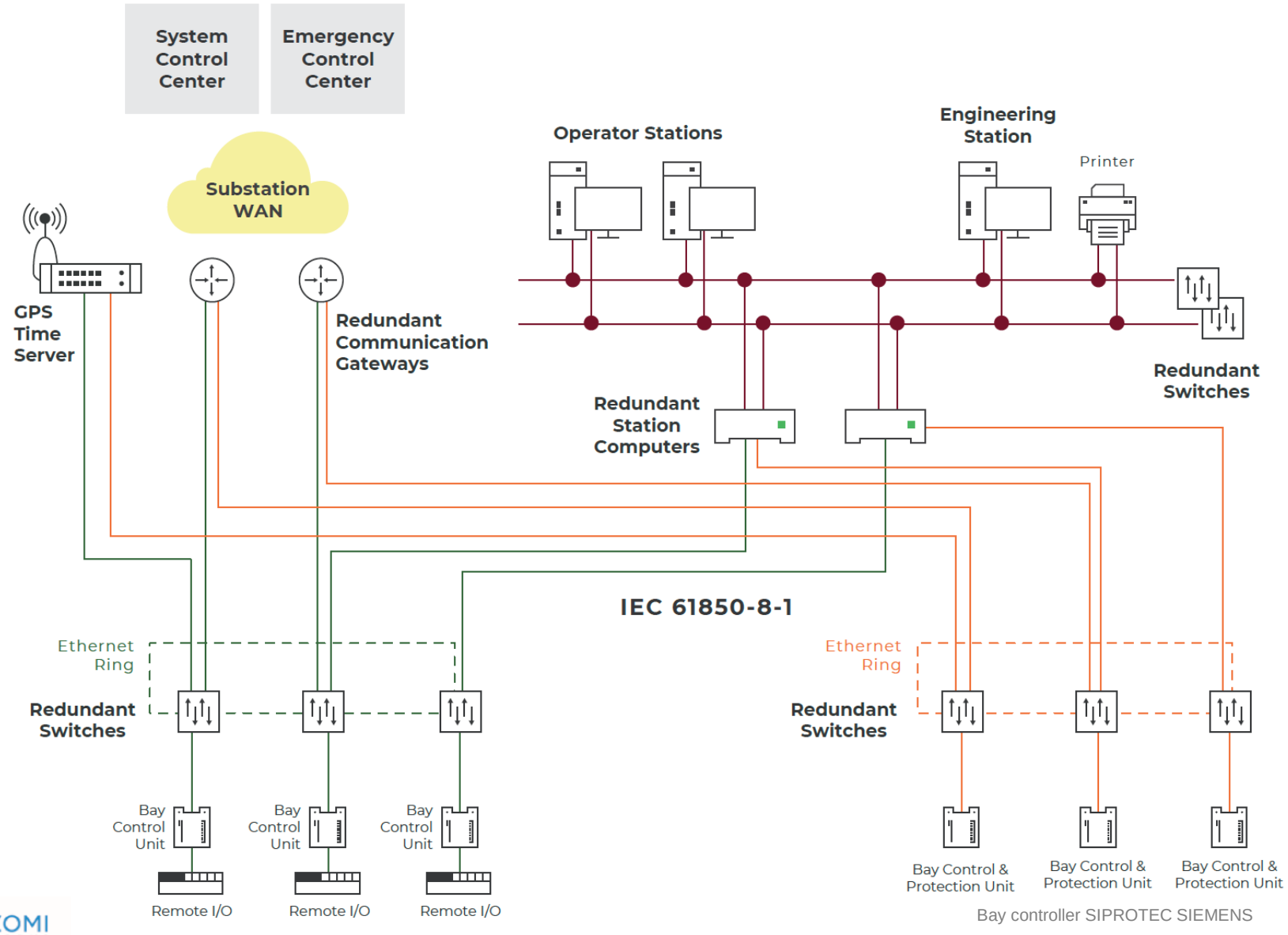
RED CONTROL
Incluye la detección y manipulación del proceso físico. Lee los datos de los sensores, ejecuta algoritmos y mantiene el historial de procesos. incluye control continuo, control de secuencia, control de lotes y control discreto.

OT

INSTRUMENTACIÓN
Es el nivel de proceso físico real que incluye los sensores y actuadores conectados directamente al proceso y al equipo de proceso.

Monitoreo de Operación y Seguridad
Ejemplo Arquitectura Solución – Industria Transmisión Eléctrica

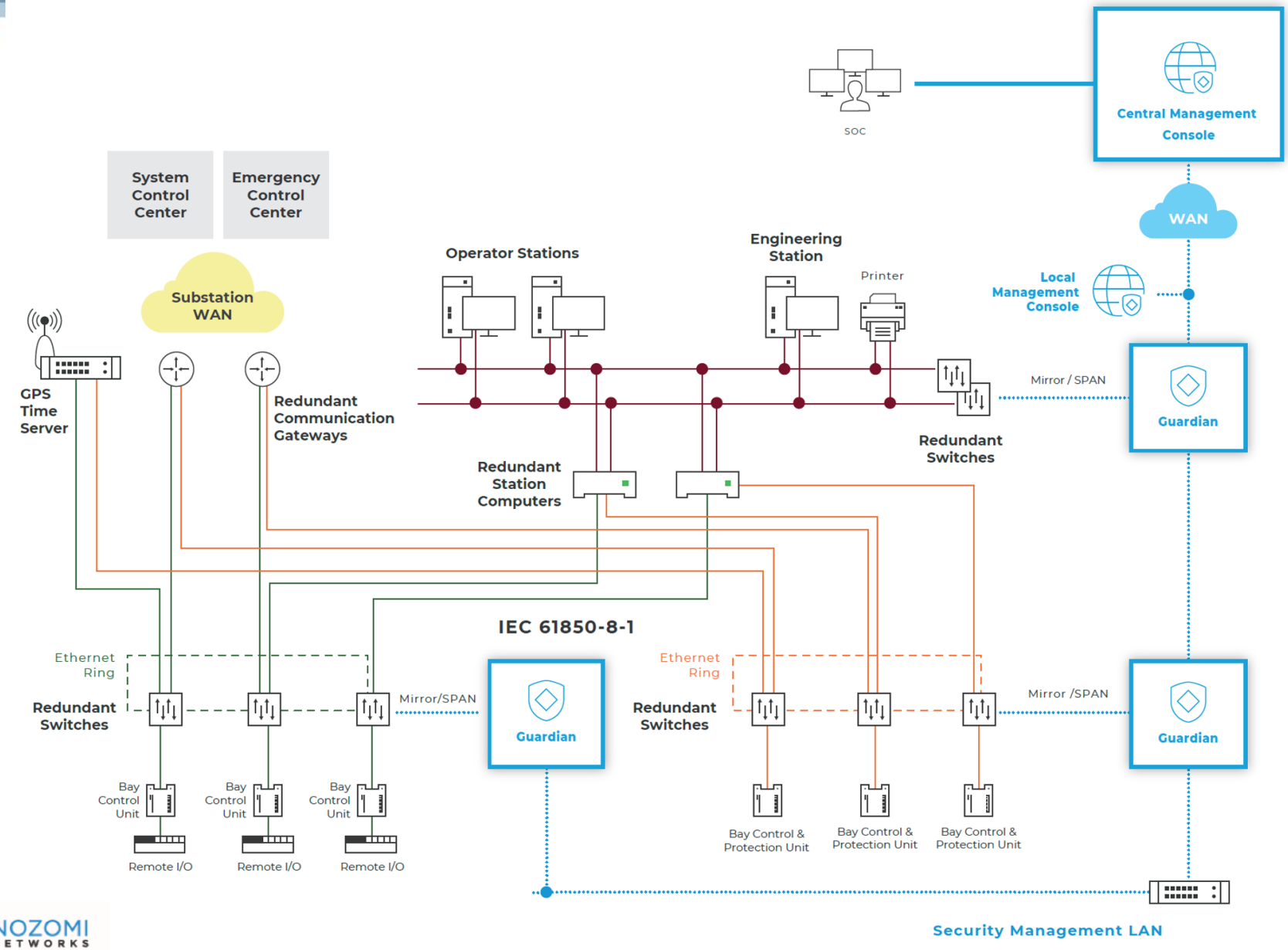
NEOSECURE
SABEMOS DE SEGURIDAD



NOZOMI NETWORKS

Monitoreo de Operación y Seguridad

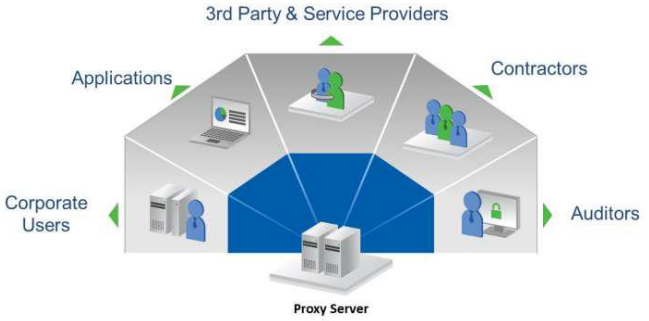
Ejemplo Arquitectura Solución – Industria Transmisión Eléctrica

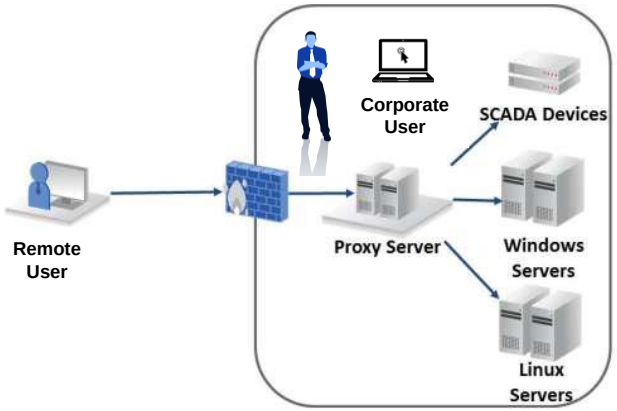


Control Accesos Usuarios

Control Acceso Usuarios

- Accesos Usuarios
  - Usuarios Corporativos
  - Terceros (Ej.: Vendor ICS)
  - Segundo Factor de Autenticación
  - NAC & VPN
- Descubrimiento cuentas
- Almacenamiento seguro de claves
- Control de cambio de claves
- Claves para accesos temporales
- Proxy de sesión
- Grabación de sesión
- Auditoría por usuario
- Administración Centralizada





Seguridad Endpoint de Nueva Generación

Next Generation Antivirus AV

- Protege contra Malware Conocido/Desconocido
- Detecta y previene ataques de día cero
- Protección para Ransomware
- Detección no basada en firmas
- Detección de ataques que no utilizan malware

Endpoint Detection and Response (EDR)

- Investigación de actividad actual e histórica en segundos
- Visibilidad total de ataques apoya la respuesta a incidente
- Minimiza el tiempo de remediación al entender como opera los ataques
- Apoya la detección de lo que no es evidente (ej. Fileless)
- La detección es en base a comportamiento

Roadmap Recomendado de Implementación Seguridad Redes OT

Fase 1

- Evaluación Redes OT
- Segregación de redes OT e IT
- Monitoreo Redes OT
- Control Accesos de Usuarios

Fase 2

- Segmentación Red OT
- Controles End_Point
- Control de Accesos NAC
- Aplicación Programa Mejoras Postura Seguridad

Servicios Gestionados
+ Inteligencia de la Amenaza

NEOSECURE
SABEMOS DE SEGURIDAD

MUCHAS GRACIAS

Presencia Local en:

- Argentina
- Chile
- Colombia
- Perú
- Brasil