FORTINET

Ciberseguridad para TO en Energía y Utilities

LATAM – OTCI

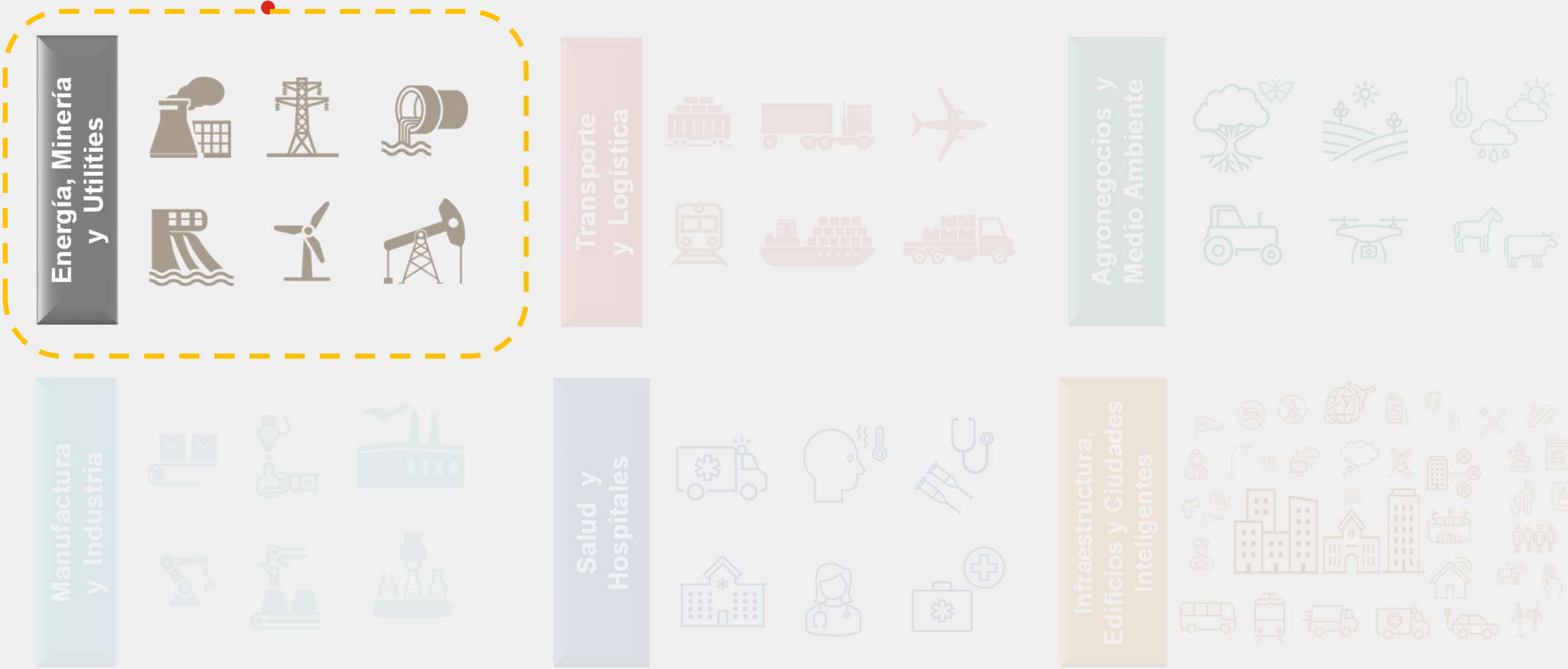
Ivo Faria

Conceptos de Seguridad TO Visión General

Protección de OT

Tecnología Operativa (TO):

Más que una tecnología, TO no és un segmento… és un conjunto de verticales



Energía, Minería y Utilities

Transporte y Logística

Agronegocios y Medio Ambiente

Manufactura y Industria

Salud y Hospitales

Infraestructura, Edificios y Ciudades Inteligentes

TI y TO Tienen Perspectivas Distintas

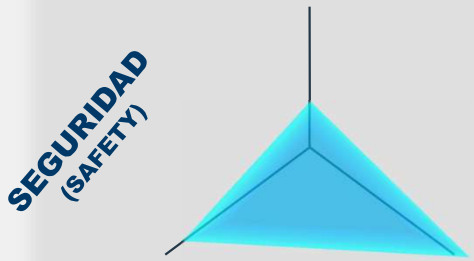
Prioridades

Normas

Connectividad

Protocolos y Equipos

TO



Confidencialidad

SEGURIDAD (SAFETY)

Integridad

Disponibilidad

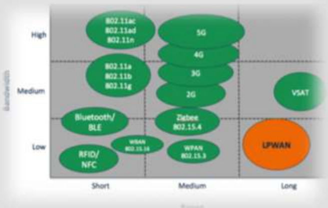
NERC CIP

NIST

ISA

IEC

Purdue Model



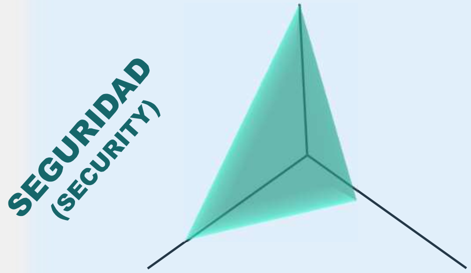
Satélite / RF PmP / LTE / 5G / LPWAN

Modbus

BACnet

PLC / SCADA
HMI / DCS

TI



Confidencialidad

SEGURIDAD (SECURITY)

Integridad

Disponibilidad

ISO

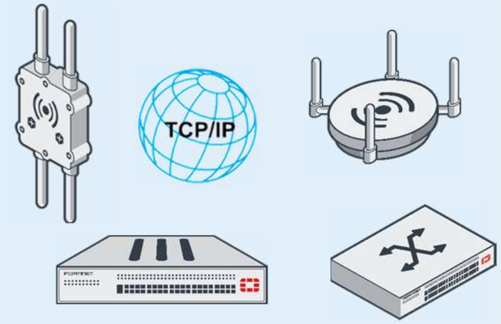
ISO 20000
IT SERVICE MANAGEMENT SYSTEM

GDPR

ISO 27001

OSI Model

WiFi™



Infraestructura inteligente para TO

Smart Infrastructures – Infraestructura crítica inteligente

Infraestructuras Críticas y Inteligentes

RENEWABLE ENERGY

MICROGRID

SELF HEALING

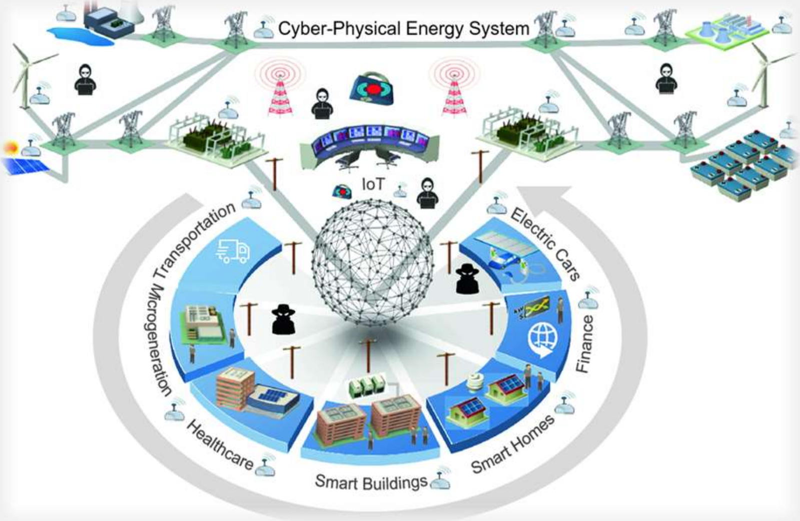
ELECTRIC VEHICLES

SMART ASSETS Mgt

SMART METERING

ENERGY MKT

COMMUNICATION



© 2020 | Probabilistic Reliability Analysis of Power Systems ©Springer Nature

AUTOMATION

PEAK-SHAVING

DIST. GENERAT + BATTERY

SMART CITIES

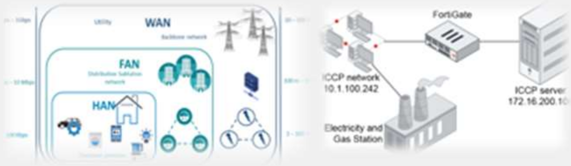
SMART OPERATION

SMART COMPUTING

SMART IoT SENSORS

Solar Generation
UTILITY GRIDS
Smart Homes
UTILITY MICROGRIDS
COMMUNITY MICROGRIDS
Smart Grid
BUILDING MICROGRIDS
Smart Communities/Cities
Solar Generation

Infraestructura Tecnológica/Comunicación



Sistemas y Seguridad

SMART METER

COMMUNICATION

AMI SYSTEMS (MDC + MDM)

INTEGRATION

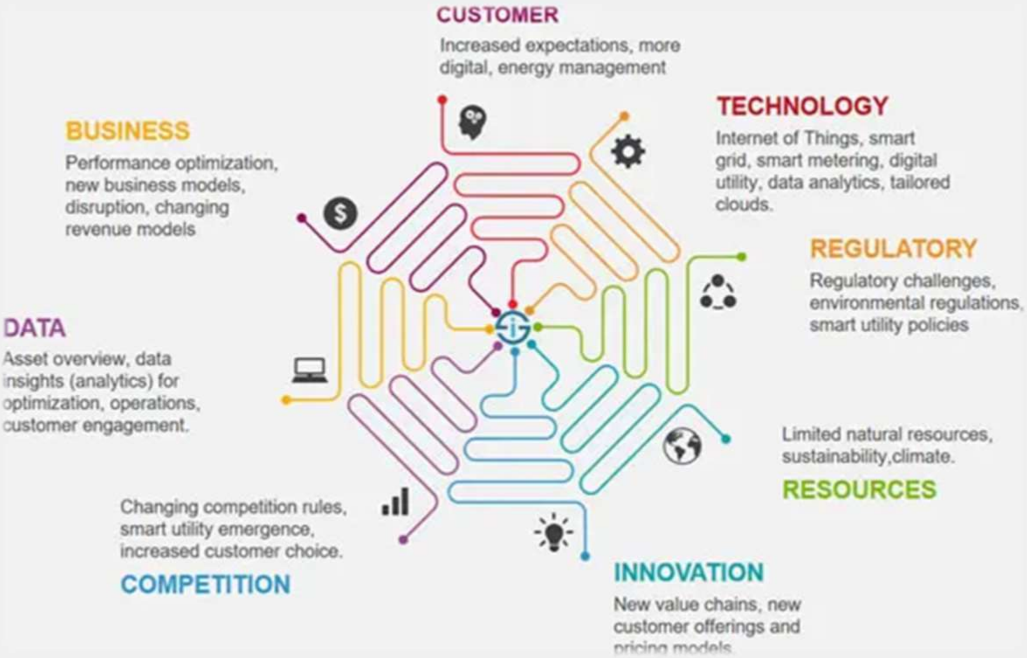
Dispositivos y Equipos

Comunicación

Sistemas de Control/Gestión

Entrenamiento de Personal

Energía: el paradigma esta cambiando



CUSTOMER
Increased expectations, more digital, energy management

TECHNOLOGY
Internet of Things, smart grid, smart metering, digital utility, data analytics, tailored clouds.

REGULATORY
Regulatory challenges, environmental regulations, smart utility policies

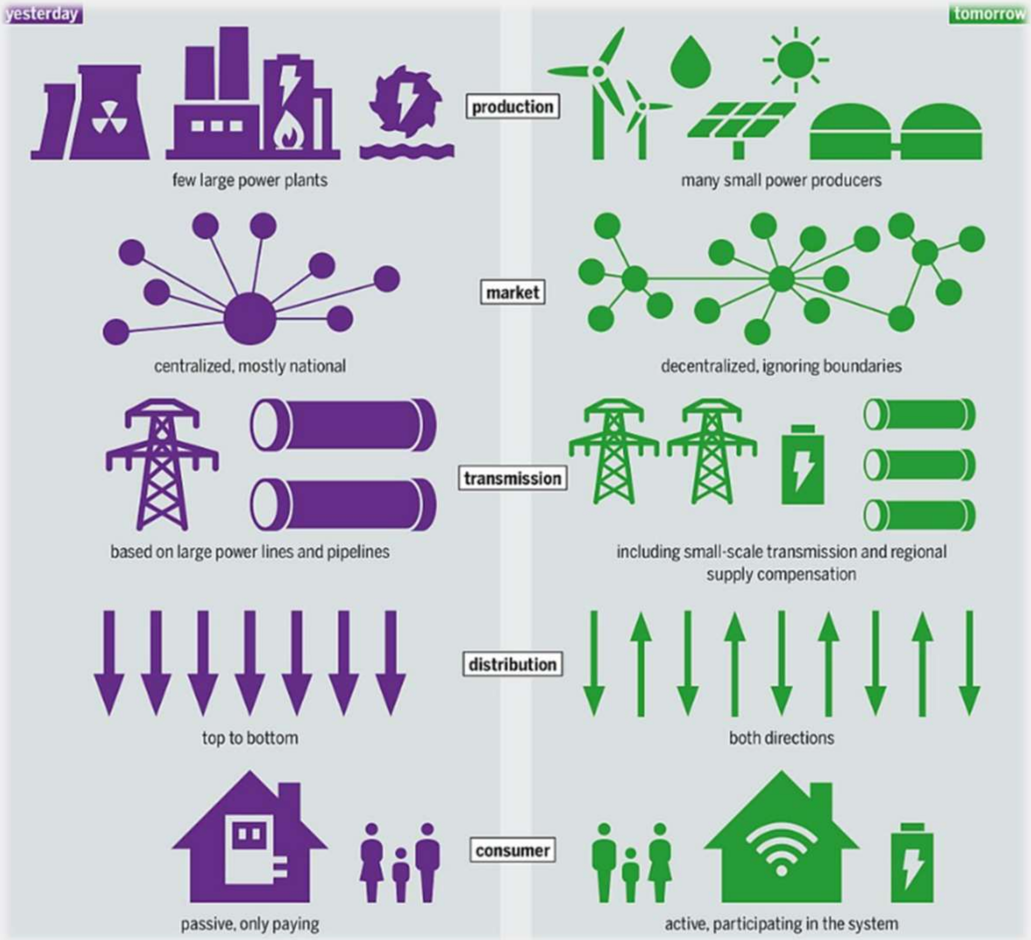
RESOURCES
Limited natural resources, sustainability,climate.

INNOVATION
New value chains, new customer offerings and pricing models

COMPETITION
Changing competition rules, smart utility emergence, increased customer choice.

DATA
Asset overview, data insights (analytics) for optimization, operations, customer engagement.

BUSINESS
Performance optimization, new business models, disruption, changing revenue models


yesterday
tomorrow
production
few large power plants
many small power producers
market
centralized, mostly national
decentralized, ignoring boundaries
transmission
based on large power lines and pipelines
including small-scale transmission and regional supply compensation
distribution
top to bottom
both directions
consumer
passive, only paying
active, participating in the system

Smart Grids - Arquitecturas

Comunicación de redes inteligentes y arquitecturas en capas

E. Ancillotti et al. / Computer Communications 36 (2013) 1665–1697

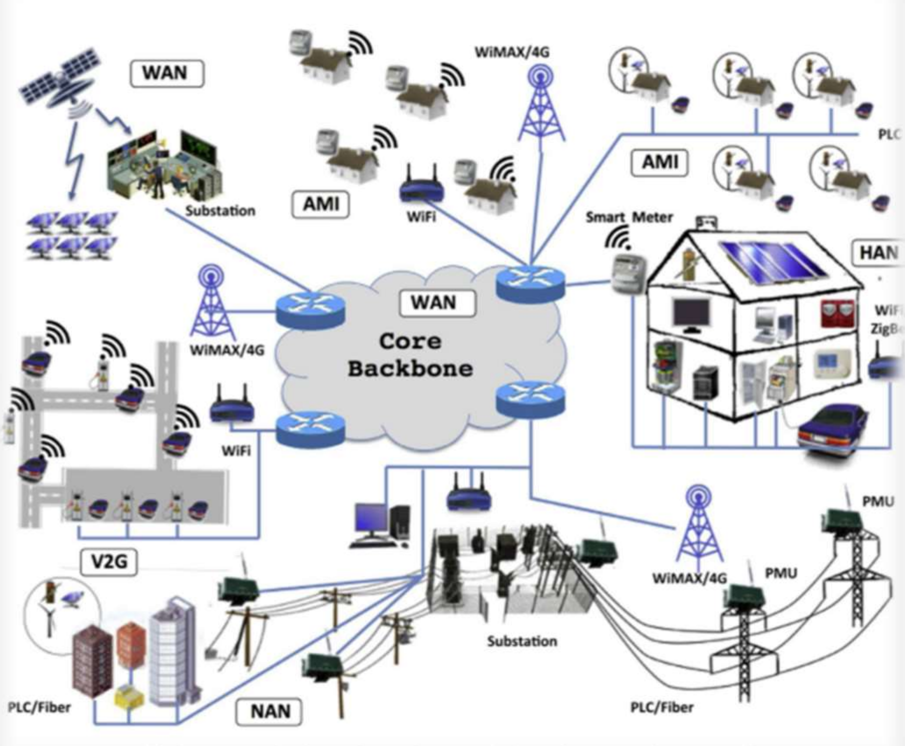
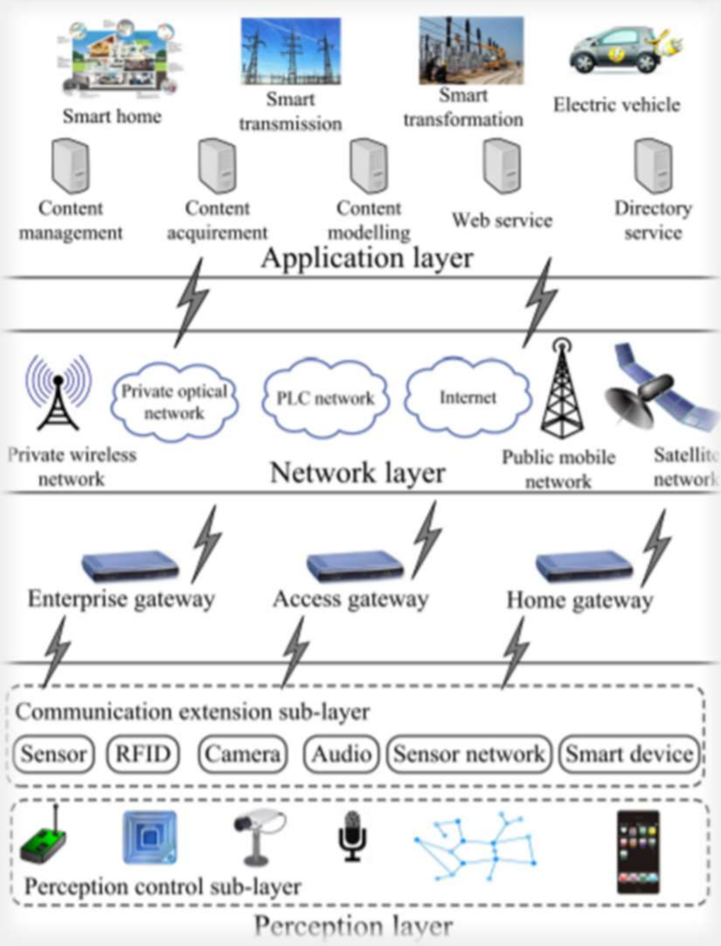
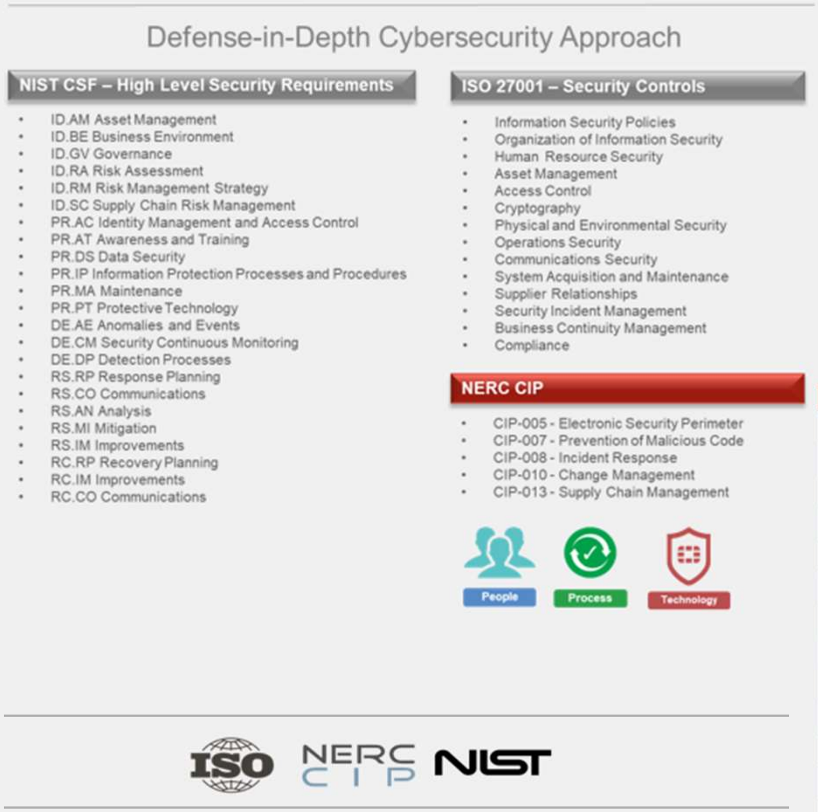


Fig. 5. An example of an end-to-end communication infrastructure for smart grids.



Smart Grids – Arquitecturas y Estándares



Defense-in-Depth Cybersecurity Approach

NIST CSF – High Level Security Requirements

- ID.AM Asset Management
- ID.BE Business Environment
- ID.GV Governance
- ID.RA Risk Assessment
- ID.RM Risk Management Strategy
- ID.SC Supply Chain Risk Management
- PR.AC Identity Management and Access Control
- PR.AT Awareness and Training
- PR.DS Data Security
- PR.IP Information Protection Processes and Procedures
- PR.MA Maintenance
- PR.PT Protective Technology
- DE.AE Anomalies and Events
- DE.CM Security Continuous Monitoring
- DE.DP Detection Processes
- RS.RP Response Planning
- RS.CO Communications
- RS.AN Analysis
- RS.MI Mitigation
- RS.IM Improvements
- RC.RP Recovery Planning
- RC.IM Improvements
- RC.CO Communications

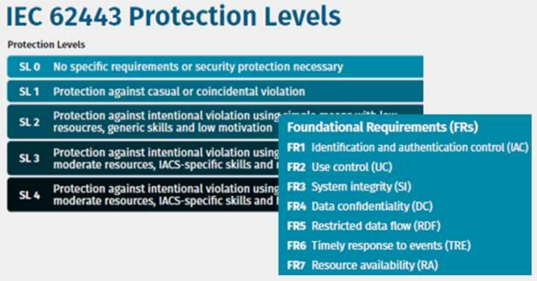
ISO 27001 – Security Controls

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition and Maintenance
- Supplier Relationships
- Security Incident Management
- Business Continuity Management
- Compliance

NERC CIP

- CIP-005 - Electronic Security Perimeter
- CIP-007 - Prevention of Malicious Code
- CIP-008 - Incident Response
- CIP-010 - Change Management
- CIP-013 - Supply Chain Management

People
Process
Technology
ISO
NERC CIP
NIST



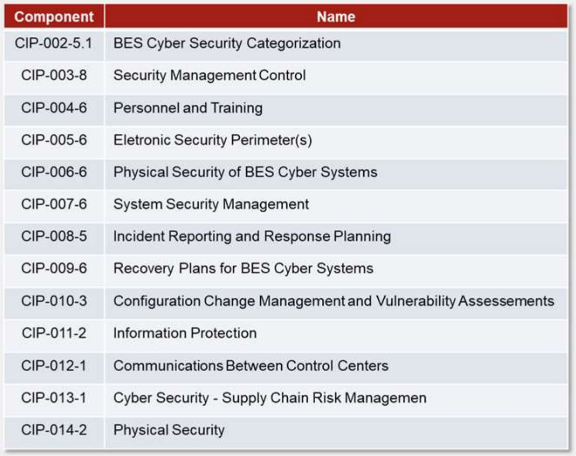
IEC 62443 Protection Levels

Protection Levels

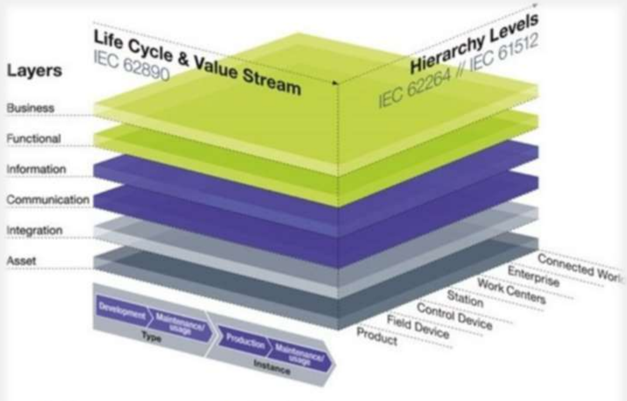
- SL 0 No specific requirements or security protection necessary
- SL 1 Protection against casual or coincidental violation
- SL 2 Protection against intentional violation using resoucres, generic skills and low motivation
- SL 3 Protection against intentional violation using moderate resources, IACS-specific skills and
- SL 4 Protection against intentional violation using moderate resources, IACS-specific skills and

Foundational Requirements (FRs)

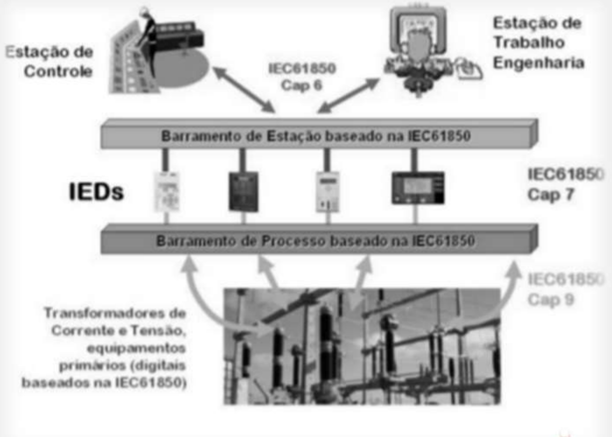
- FR1 Identification and authentication control (IAC)
- FR2 Use control (UC)
- FR3 System integrity (SI)
- FR4 Data confidentiality (DC)
- FR5 Restricted data flow (RDF)
- FR6 Timely response to events (TRE)
- FR7 Resource availability (RA)



Component	Name
CIP-002-5.1	BES Cyber Security Categorization
CIP-003-8	Security Management Control
CIP-004-6	Personnel and Training
CIP-005-6	Eletronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management and Vulnerability Assessements
CIP-011-2	Information Protection
CIP-012-1	Communications Between Control Centers
CIP-013-1	Cyber Security - Supply Chain Risk Managemen
CIP-014-2	Physical Security



ːAMI 4.0 (Reference Architecture Model I4.0) by ZVEI [75].

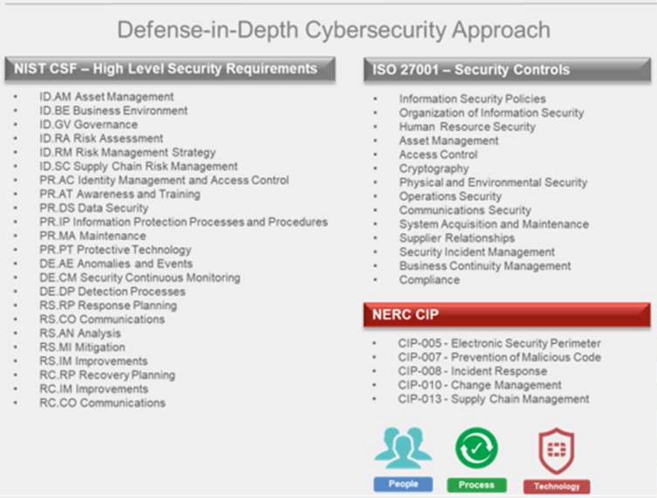


Estação de Controle
Estação de Trabalho Engenharia
IEC61850 Cap 6
Barramento de Estação baseado na IEC61850
IEDs
IEC61850 Cap 7
Barramento de Processo baseado na IEC61850
IEC61850 Cap 9
Transformadores de Corrente e Tensão, equipamentos primários (digitais baseados na IEC61850)

Figura 2: SAS conforme a IEC 61850

https://www.scirp.org/journal/paperinformation.aspx?paperid=91158

Arquitecturas y Estándares



Defense-in-Depth Cybersecurity Approach

NIST CSF – High Level Security Requirements

- ID.AM Asset Management
- ID.BE Business Environment
- ID.GV Governance
- ID.RA Risk Assessment
- ID.RM Risk Management Strategy
- ID.SC Supply Chain Risk Management
- PR.AC Identity Management and Access Control
- PR.AT Awareness and Training
- PR.DS Data Security
- PR.IP Information Protection Processes and Procedures
- PR.MA Maintenance
- PR.PT Protective Technology
- DE.AE Anomalies and Events
- DE.CM Security Continuous Monitoring
- DE.DP Detection Processes
- RS.RP Response Planning
- RS.CO Communications
- RS.AN Analysis
- RS.MI Mitigation
- RS.IM Improvements
- RC.RP Recovery Planning
- RC.IM Improvements
- RC.CO Communications

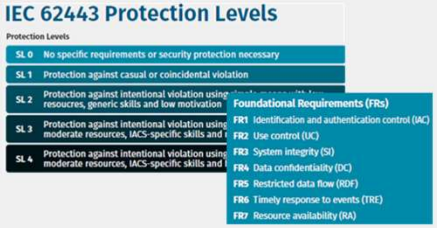
ISO 27001 – Security Controls

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition and Maintenance
- Supplier Relationships
- Security Incident Management
- Business Continuity Management
- Compliance

NERC CIP

- CIP-005 - Electronic Security Perimeter
- CIP-007 - Prevention of Malicious Code
- CIP-008 - Incident Response
- CIP-010 - Change Management
- CIP-013 - Supply Chain Management

People
Process
Technology



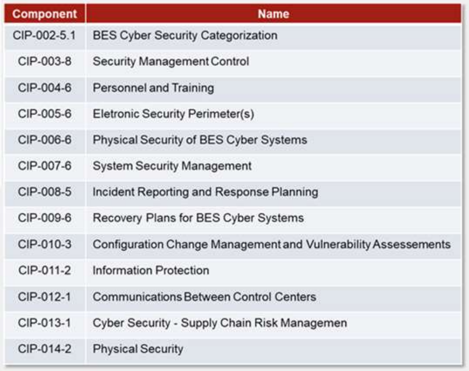
IEC 62443 Protection Levels

Protection Levels

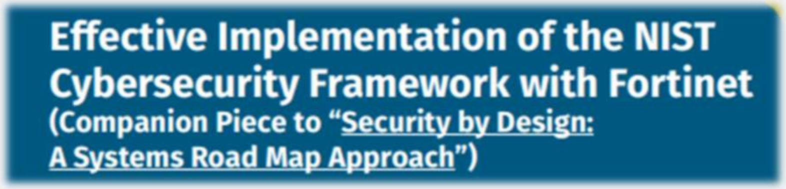
SL 0	No specific requirements or security protection necessary
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using resoucres, generic skills and low motivation
SL 3	Protection against intentional violation using moderate resources, IACS-specific skills and
SL 4	Protection against intentional violation using moderate resources, IACS-specific skills and

Foundational Requirements (FRs)

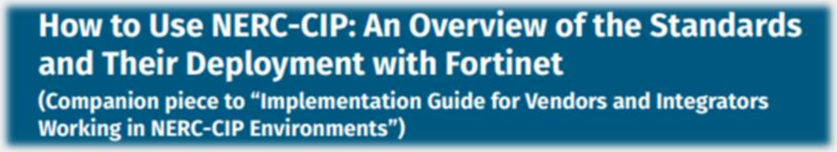
FR1	Identification and authentication control (IAC)
FR2	Use control (UC)
FR3	System integrity (SI)
FR4	Data confidentiality (DC)
FR5	Restricted data flow (RDF)
FR6	Timely response to events (TRE)
FR7	Resource availability (RA)



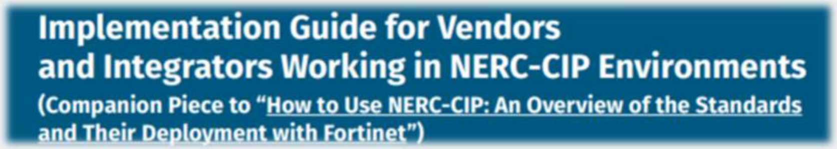
Component	Name
CIP-002-5.1	BES Cyber Security Categorization
CIP-003-8	Security Management Control
CIP-004-6	Personnel and Training
CIP-005-6	Eletronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management and Vulnerability Assessements
CIP-011-2	Information Protection
CIP-012-1	Communications Between Control Centers
CIP-013-1	Cyber Security - Supply Chain Risk Managemen
CIP-014-2	Physical Security



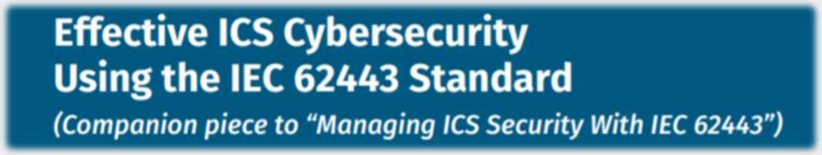
Effective Implementation of the NIST Cybersecurity Framework with Fortinet
(Companion Piece to "Security by Design: A Systems Road Map Approach")



How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet
(Companion piece to "Implementation Guide for Vendors and Integrators Working in NERC-CIP Environments")



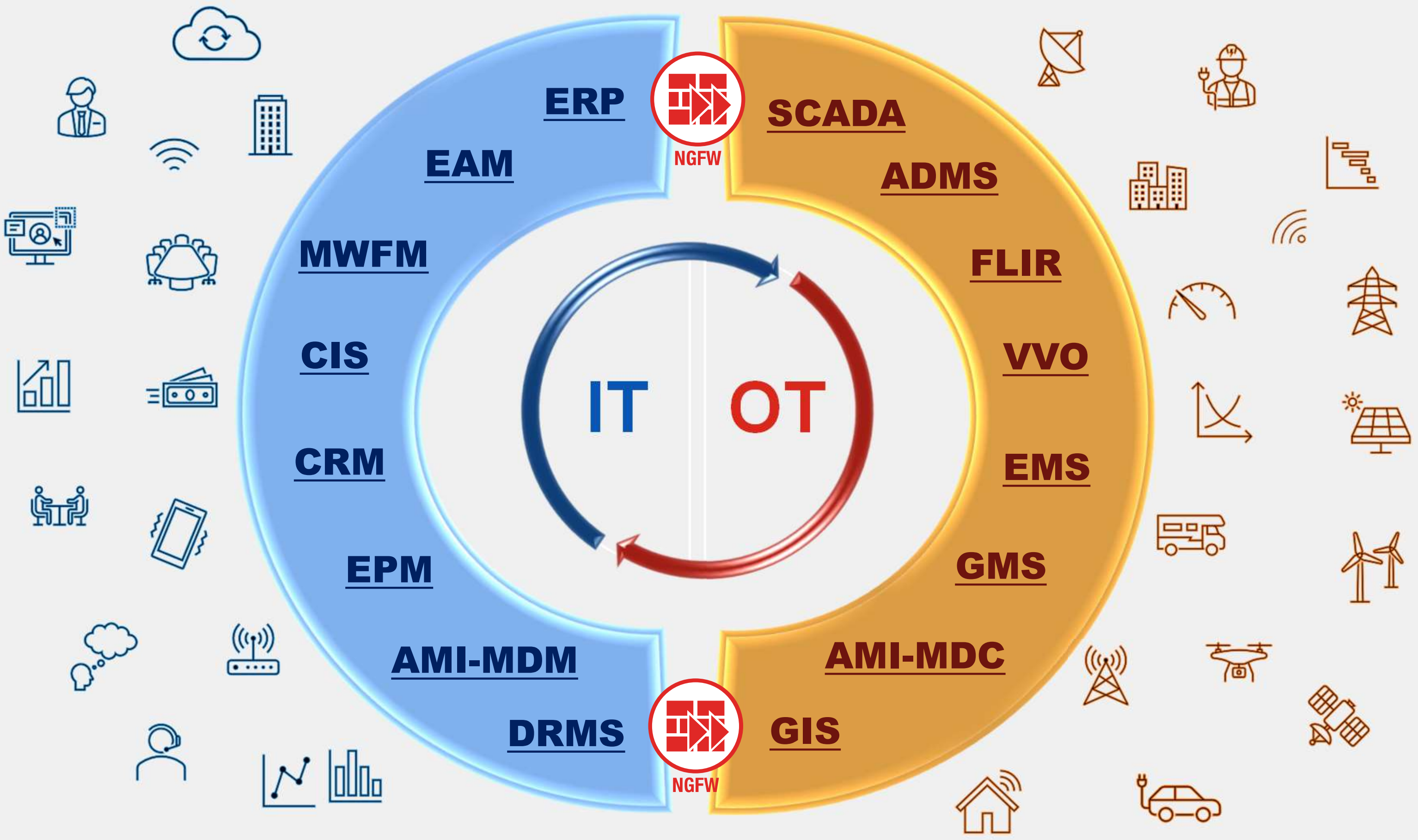
Implementation Guide for Vendors and Integrators Working in NERC-CIP Environments
(Companion Piece to "How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet")



Effective ICS Cybersecurity Using the IEC 62443 Standard
(Companion piece to "Managing ICS Security With IEC 62443")

https://www.scirp.org/journal/paperinformation.aspx?paperid=91158

OTCI – Convergencia IT x OT



¿ Por qué ciberseguridad para OT y IoT?

Tendencias de comunicación y cumplimiento de OT/IoT

Intrusiones: parte del nuevo normal

Y afectan la productividad, los ingresos y la seguridad física

FORTINET
2022 State of Operational Technology and Cybersecurity Report

9 out of 10

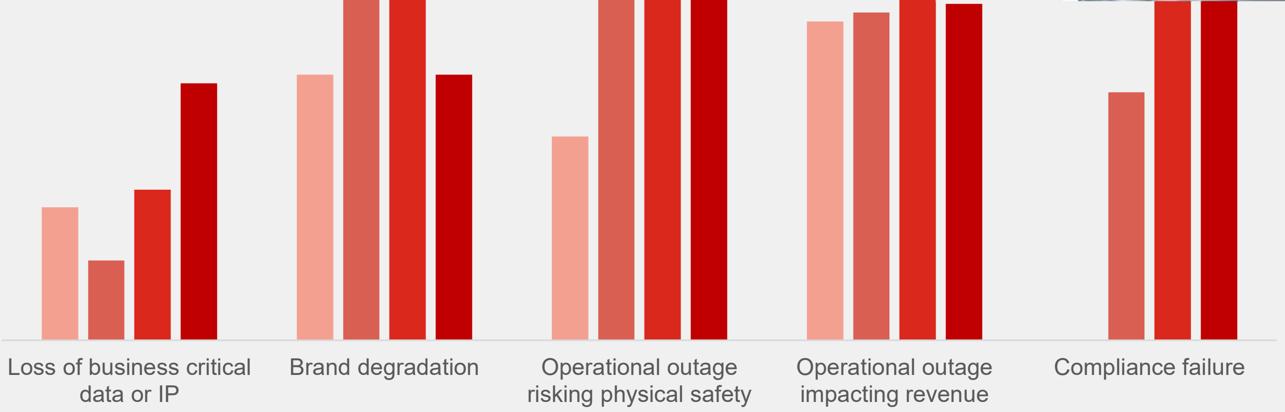
OT organizations experienced at least one intrusion in the past year and **78% had 3 or more intrusions**, which is up from the results in 2021.

61 % de las intrusiones afectaron a los sistemas de TO

90 % de las intrusiones tardaron horas o más para restablecer el servicio

Impact on organization

🟥 2019 🟥 2020 🟥 2021 🟥 2022



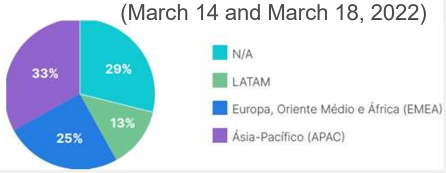
Top-tier organizations are…

…likely to have centralized visibility, use **network access control** and have **security tracking and reporting** in place.

32% **more likely** to have their SOC **monitor and track OT security**.

Data is from Fortinet's **2022 State of Operational Technology and Cybersecurity Report**

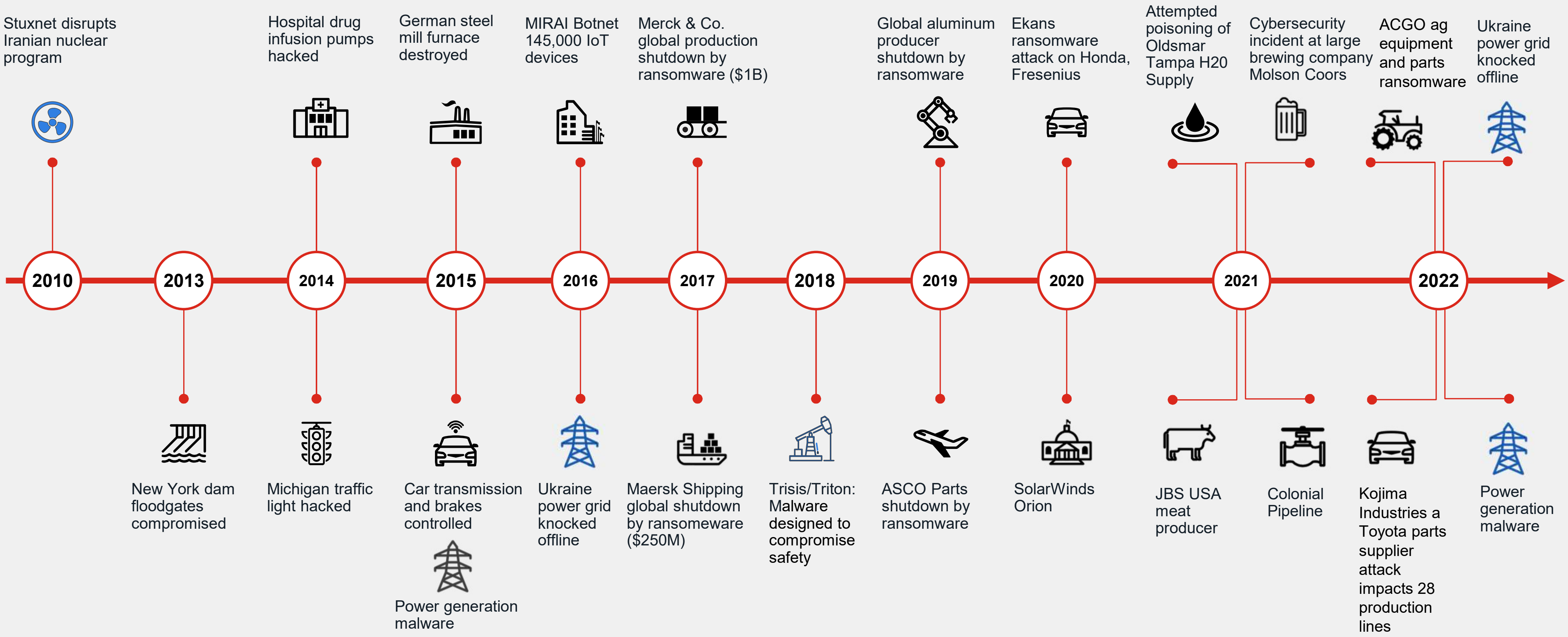
More than 500 OT professionals (March 14 and March 18, 2022)



Source: Fortinet's 2022 State of Operational Technology and Cybersecurity Report

Ataques a la Infraestructura OT & IoT

El Riesgo es Real



2010

Stuxnet disrupts Iranian nuclear program

2013

New York dam floodgates compromised

2014

Hospital drug infusion pumps hacked

Michigan traffic light hacked

2015

German steel mill furnace destroyed

Car transmission and brakes controlled

Power generation malware

2016

MIRAI Botnet 145,000 IoT devices

Ukraine power grid knocked offline

2017

Merck & Co. global production shutdown by ransomware ($1B)

Maersk Shipping global shutdown by ransomware ($250M)

2018

Trisis/Triton: Malware designed to compromise safety

2019

Global aluminum producer shutdown by ransomware

ASCO Parts shutdown by ransomware

2020

Ekans ransomware attack on Honda, Fresenius

SolarWinds Orion

2021

Attempted poisoning of Oldsmar Tampa H20 Supply

Cybersecurity incident at large brewing company Molson Coors

JBS USA meat producer

Colonial Pipeline

2022

ACGO ag equipment and parts ransomware

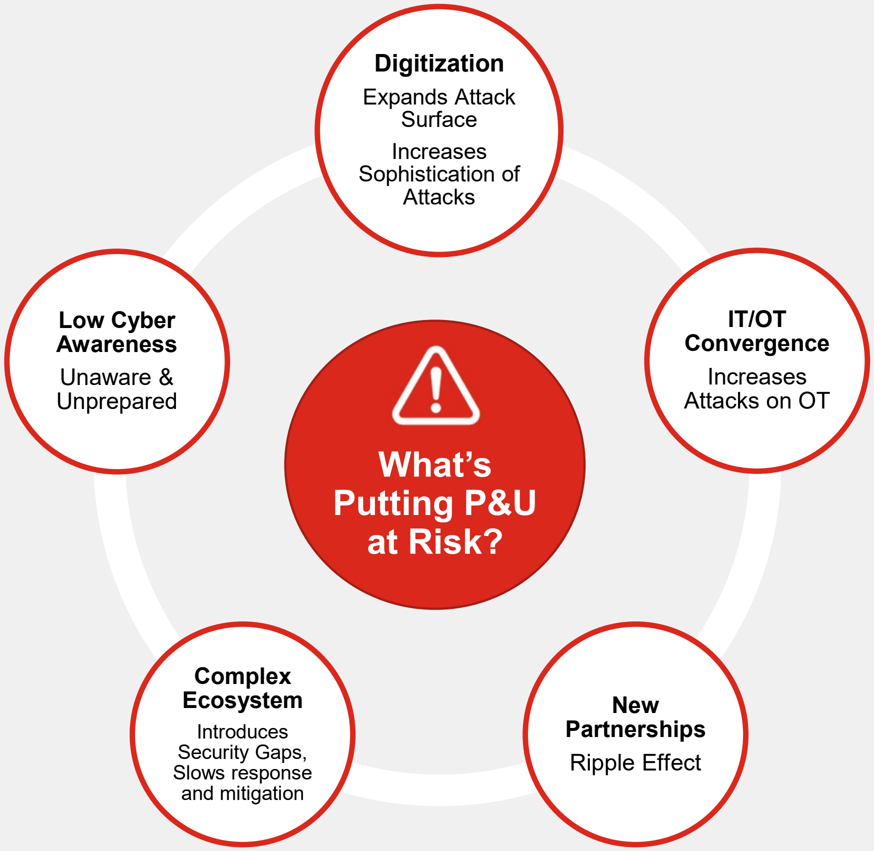
Ukraine power grid knocked offline

Kojima Industries a Toyota parts supplier attack impacts 28 production lines

Power generation malware

OT targeted attacks

Aumento de los ataques cibernéticos



Digitization

Expands Attack Surface

Increases Sophistication of Attacks

IT/OT Convergence

Increases Attacks on OT

New Partnerships

Ripple Effect

Complex Ecosystem

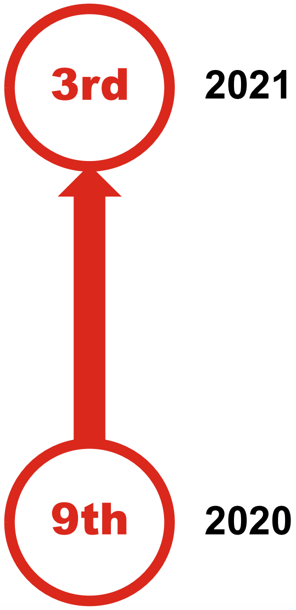
Introduces Security Gaps, Slows response and mitigation

Low Cyber Awareness

Unaware & Unprepared

What's Putting P&U at Risk?

Industria más atacada



3rd **2021**

9th **2020**

Energia saltó del noveno lugar en 2020 al **3er lugar en 2021**, lo que subraya que los atacantes se centran en las industrias de OT conectadas.

April 2021

The U.S. government announces a new effort to protect power and utilities and in particular their industrial control systems (ICS), from cyberattacks.

Desafío: Protección de la Tecnología Operativa

Habilitando la convergencia de TO y TI

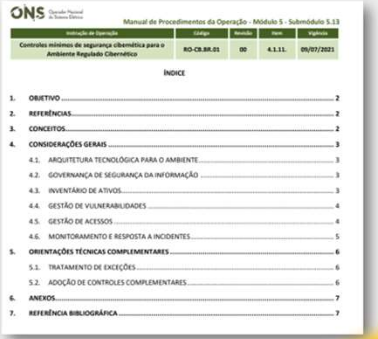
- La **superficie de ataque** para los activos cibernéticos se está **expandiendo** a medida que disminuye la dependencia de la protección de espacios aéreos con las iniciativas de transformación digital que impulsan la **convergencia** de la red de TI y TO.
- Requisitos de **acceso remoto** para terceros y empleados que causan **riesgos adicionales**.
- La mayoría de los sistemas de control industrial carecen de **seguridad por diseño**.
- Aumento de la adopción de **nuevas tecnologías**, como 5G, IoT y la nube.
- La **confianza** de los propietarios de activos en los OEMs y los SIs **expone** los sistemas críticos a riesgos adicionales.

Marco Regulatorio - Ciber Securidad en LATAM

¿Existe un marco regulatorio o regulación específica para servicios críticos o sector eléctrico en Uruguay ?

Brasil – RO.CB.BR.01

- Publicado en la primera semana de julio de 2021;
- Entrada en vigor el 7 de julio de 2021
- Más simple que NERC-CIP
- 3 olas definidas para la implementación



ONS Operador Nacional do Sistema Elétrico

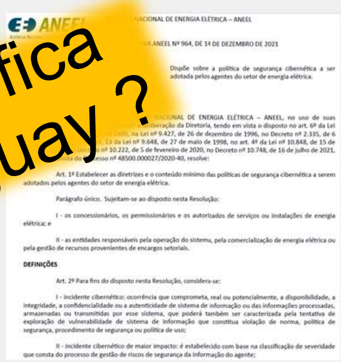
Manual de Procedimentos da Operação - Módulo 5 - Submódulo 5.13

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	RO-CB.BR.01	00	4.1.11.	09/07/2021

ÍNDICE

Brasil – REN2021_964

- Publicado a mediados de dicie de 2021
- Entra en vigor
- Estab ctrico
- O.CB.BR01-ONS



ANEEL

NACIONAL DE ENERGIA ELÉTRICA – ANEEL

ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021

Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

NACIONAL DE ENERGIA ELÉTRICA – ANEEL, no uso de suas deliberação da Diretoria, tendo em vista o disposto no art. 6º da Lei 1995, na Lei nº 9.427, de 26 de dezembro de 1996, no Decreto nº 2.335, de 6 art. 13 da Lei nº 9.648, de 27 de maio de 1998, no art. 4º da Lei nº 10.848, de 15 de Decreto nº 10.222, de 5 de fevereiro de 2020, no Decreto nº 10.748, de 16 de julho de 2021, consta do Processo nº 48500.000027/2020-40, resolve:

Art. 1º Estabelecer as diretrizes e o conteúdo mínimo das políticas de segurança cibernética a serem adotados pelos agentes do setor de energia elétrica.

Parágrafo único. Sujeitam-se ao disposto nesta Resolução:

I - os concessionários, os permissionários e os autorizados de serviços ou instalações de energia elétrica; e

II - as entidades responsáveis pela operação do sistema, pela comercialização de energia elétrica ou pela gestão de recursos provenientes de encargos setoriais.

DEFINIÇÕES

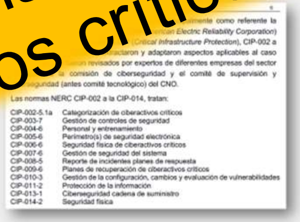
Art. 2º Para fins do disposto nesta Resolução, considera-se:

I - incidente cibernético: ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

II - incidente cibernético de maior impacto: é estabelecido com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do agente;

Colombia – CNO 1347

- Basado e artícul
- Implen e con diferente a diferentes artículos
- Algunos artículos se retrasaron debido a la pandemia de COVID-19



mente como referente la Electric Reliability Corporation) (Critical Infrastructure Protection), CIP-002 a extractaron y adaptaron aspectos aplicables al caso revisados por expertos de diferentes empresas del sector la comisión de ciberseguridad y el comité de supervisión y seguridad (antes comité tecnológico) del CNO.

Las normas NERC CIP-002 a la CIP-014, tratan:

CIP-002-5.1a	Categorización de ciberactivos críticos
CIP-003-7	Gestión de controles de seguridad
CIP-004-6	Personal y entrenamiento
CIP-005-6	Perímetro(s) de seguridad electrónica
CIP-006-6	Seguridad física de ciberactivos críticos
CIP-007-6	Gestión de seguridad del sistema
CIP-008-5	Reporte de incidentes planes de respuesta
CIP-009-6	Planes de recuperación de ciberactivos críticos
CIP-010-3	Gestión de la configuración, cambios y evaluación de vulnerabilidades
CIP-011-2	Protección de la información
CIP-013-1	Ciberseguridad cadena de suministro
CIP-014-2	Seguridad física

Que el Comité de Supervisión y Ciberseguridad en la reunión 26 del 9 de septiembre de 2020 recomendó la expedición del presente Acuerdo, en el que se amplían los plazos de las siguientes actividades a partir del 1 de octubre de 2019, así:

Ampliación plazo de 12 a 18 meses

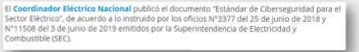
- Actualización de inventario de ciberactivos.
- Actualización de análisis de riesgos y vulnerabilidades.
- Actualización del nivel de gestión de ciberseguridad.
- Definición de los perímetros de seguridad electrónica para los ciberactivos.

Ampliación plazo de 18 a 24 meses

- Plan de seguridad electrónica de ciberactivos.
- Plan de seguridad física para ciberactivos.

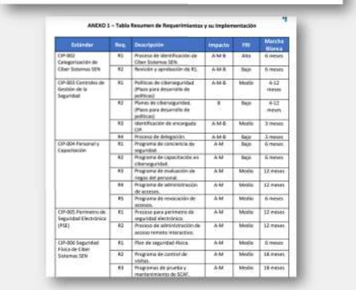
Source: https://www.cno.org.co/content/acuerdo-1347-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad

Chile – Oficios 3377 and 11508



El Coordinador Eléctrico Nacional publicó el documento "Estándar de Ciberseguridad para el Sector Eléctrico", 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).

- También basado en NERC-CIP
- Publicado en julio de 2020
- Utiliza el artículo 12 de NERC-CIP, que ni siquiera se aplicó en América del Norte



ANEXO 1 – Tabla Resumen de Requerimientos y su Implementación

Estándar	Req.	Descripción	Impacto	FRI	Marcha Blanca
CIP-002 Categorización de Ciber Sistemas SEN	R1	Proceso de identificación de Ciber Sistemas SEN.	A-M-B	Alto	6 meses
	R2	Revisión y aprobación de R1.	A-M-B	Bajo	6 meses
CIP-003 Controles de Gestión de la Seguridad	R1	Políticas de ciberseguridad (Plazo para desarrollo de políticas)	A-M-B	Medio	4-12 meses
	R2	Planes de ciberseguridad (Plazo para desarrollo de políticas)	B	Bajo	4-12 meses
	R3	Identificación de encargado CIP.	A-M-B	Medio	3 meses
	R4	Proceso de delegación.	A-M-B	Bajo	3 meses
CIP-004 Personal y Capacitación	R1	Programa de conciencia de seguridad.	A-M	Bajo	6 meses
	R2	Programa de capacitación en ciberseguridad.	A-M	Bajo	6 meses
	R3	Programa de evaluación de riesgos del personal.	A-M	Medio	12 meses
	R4	Programa de administración de accesos.	A-M	Medio	12 meses
	R5	Programa de revocación de accesos.	A-M	Medio	6 meses
CIP-005 Perímetro de Seguridad Electrónica (PSE)	R1	Proceso para perímetro de seguridad electrónica.	A-M	Medio	12 meses
	R2	Proceso de administración de acceso remoto interactivo.	A-M	Medio	12 meses
CIP-006 Seguridad Física de Ciber Sistemas SEN	R1	Plan de seguridad física.	A-M	Medio	6 meses
	R2	Programa de control de visitas.	A-M	Medio	18 meses
	R3	Programas de prueba y mantenimiento de SCAF.	A-M	Medio	18 meses

Source: https://www.guiachileenergia.cl/coordinador-presento-estandar-de-ciberseguridad-para-el-sector-electrico-nacional/

El enfoque de Fortinet para ciberseguridad TO

Fortinet Security Fabric

AMPLIO

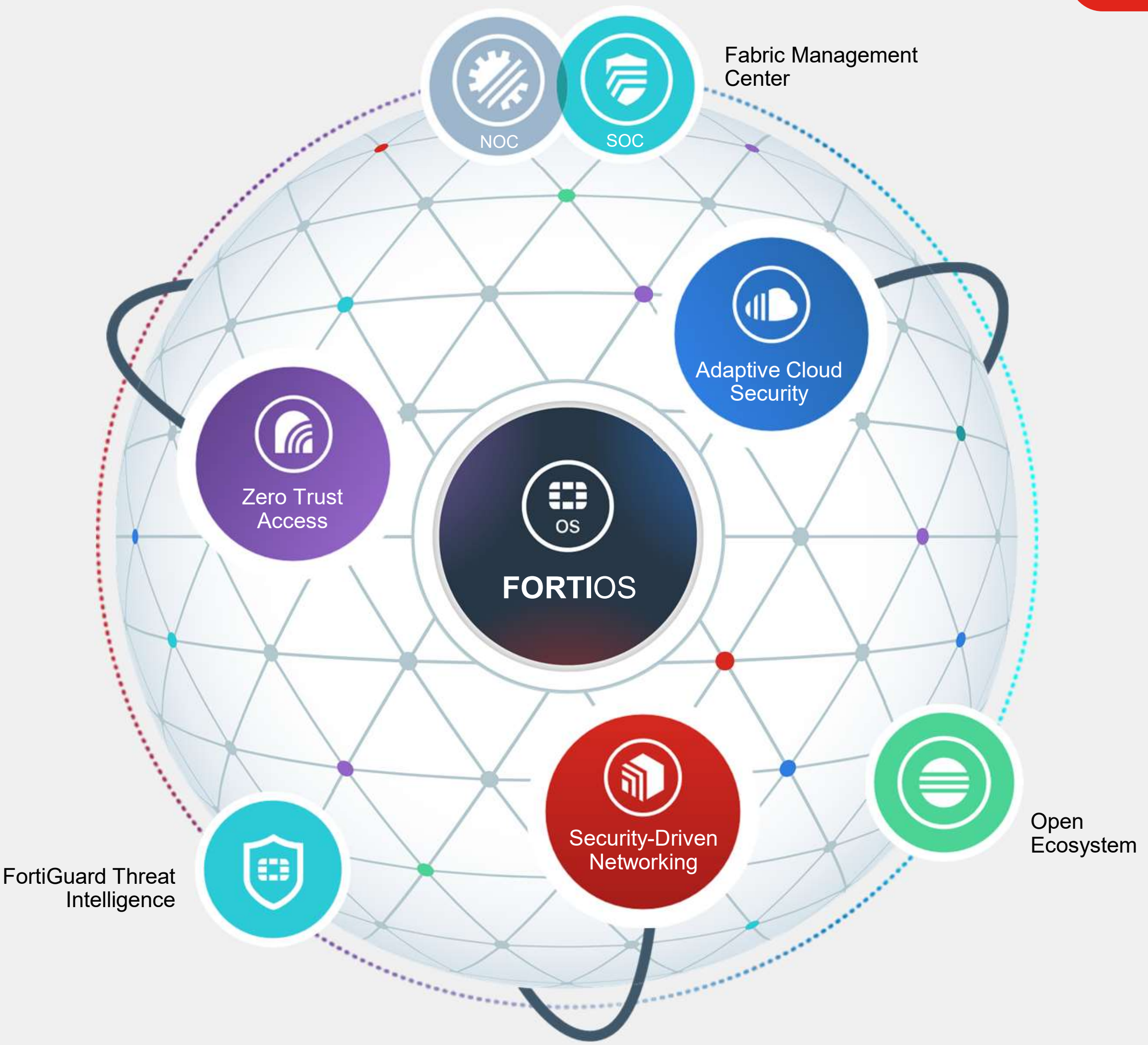
Visibilidad de toda la superficie de ataque digital para mejor manejo del riesgo

INTEGRADO

Soluciones que reducen la complexidad de gestión y comparten inteligencia sobre las amenazas

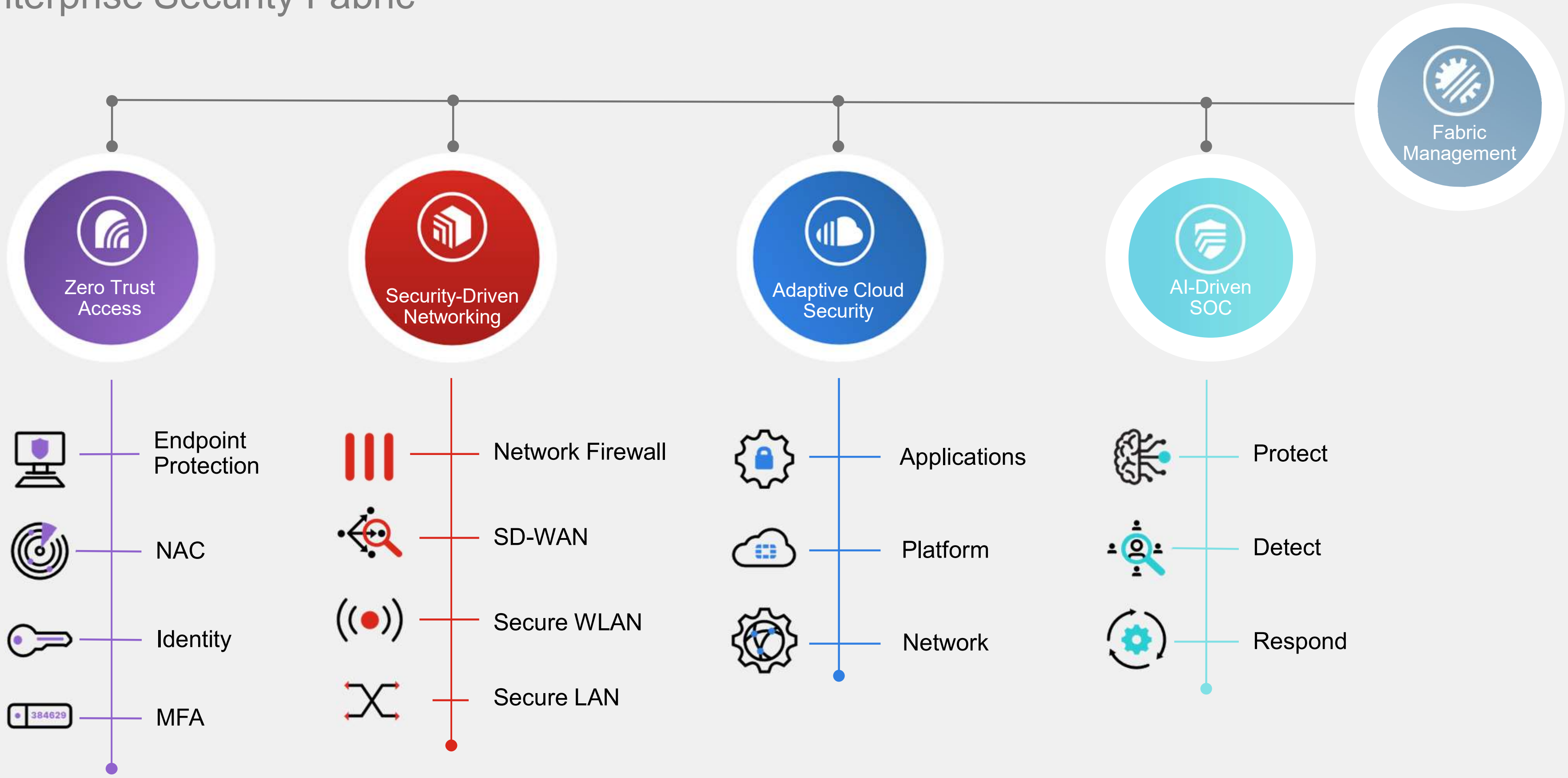
AUTOMATIZADO

Operaciones y respuesta impulsadas por *Machine Learning* para operaciones eficientes y ágiles



Plataforma Fortinet de Ciberseguridad

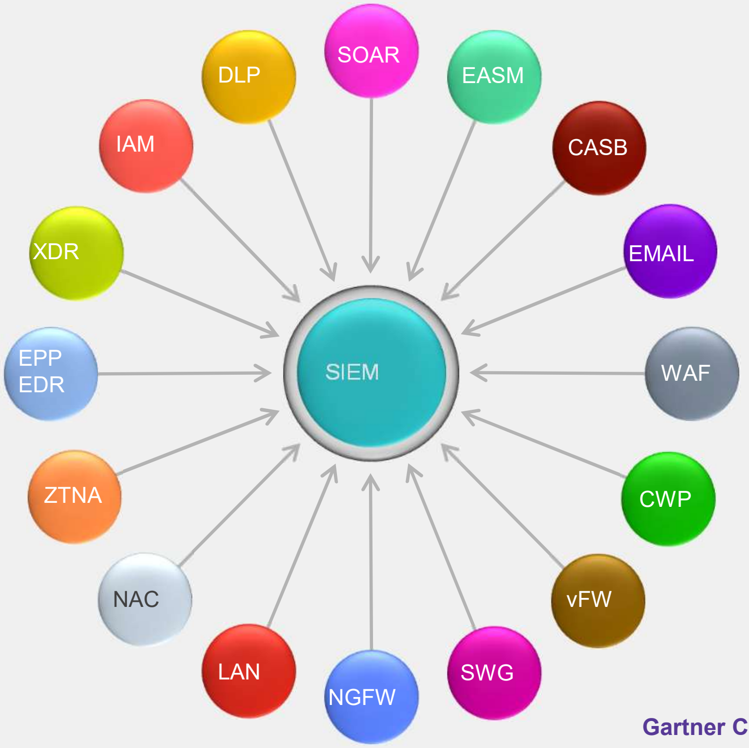
Enterprise Security Fabric



Centralización de Controles y Transparencia en la seguridad TI y TO

Gartner

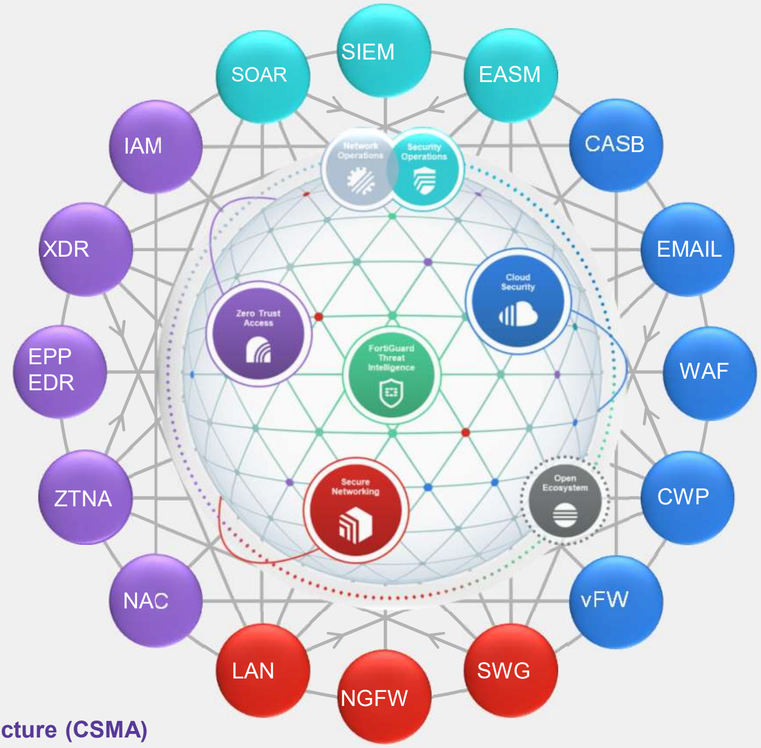
Cyberseguridad con Soluciones puntuales



20 Vendors

FORTINET

Propuesta de Plataformas de Ciberseguridad



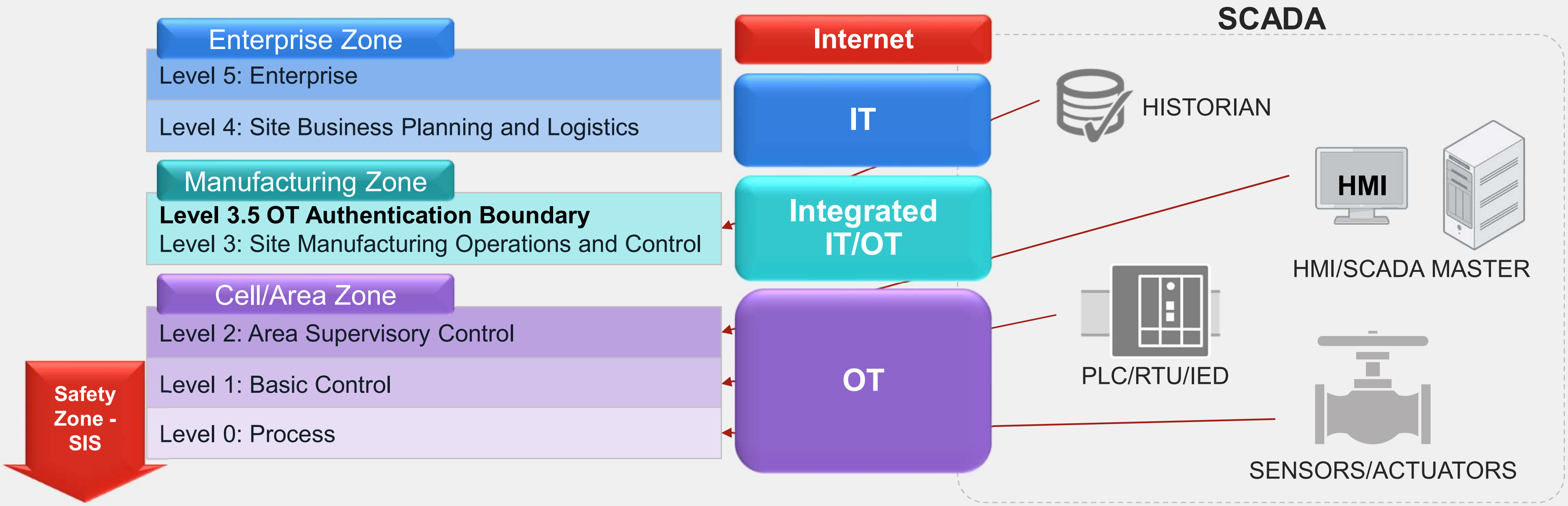
Gartner Cybersecurity Mesh Architecture (CSMA)

4-6 Platforms

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Modelo Purdue para Jerarquía de Control Industrial

- Marco estándar de la industria para la ciberseguridad de OT
- Segmenta los activos de OT en zonas y conductos de seguridad
- Aumento de los niveles de seguridad para mejorar la postura de seguridad
- Controles de seguridad validados para proteger los activos de OT



Enterprise Zone

Level 5: Enterprise

Level 4: Site Business Planning and Logistics

Manufacturing Zone

Level 3.5 OT Authentication Boundary

Level 3: Site Manufacturing Operations and Control

Cell/Area Zone

Level 2: Area Supervisory Control

Level 1: Basic Control

Level 0: Process

Safety Zone - SIS

Internet

IT

Integrated IT/OT

OT

SCADA

HISTORIAN

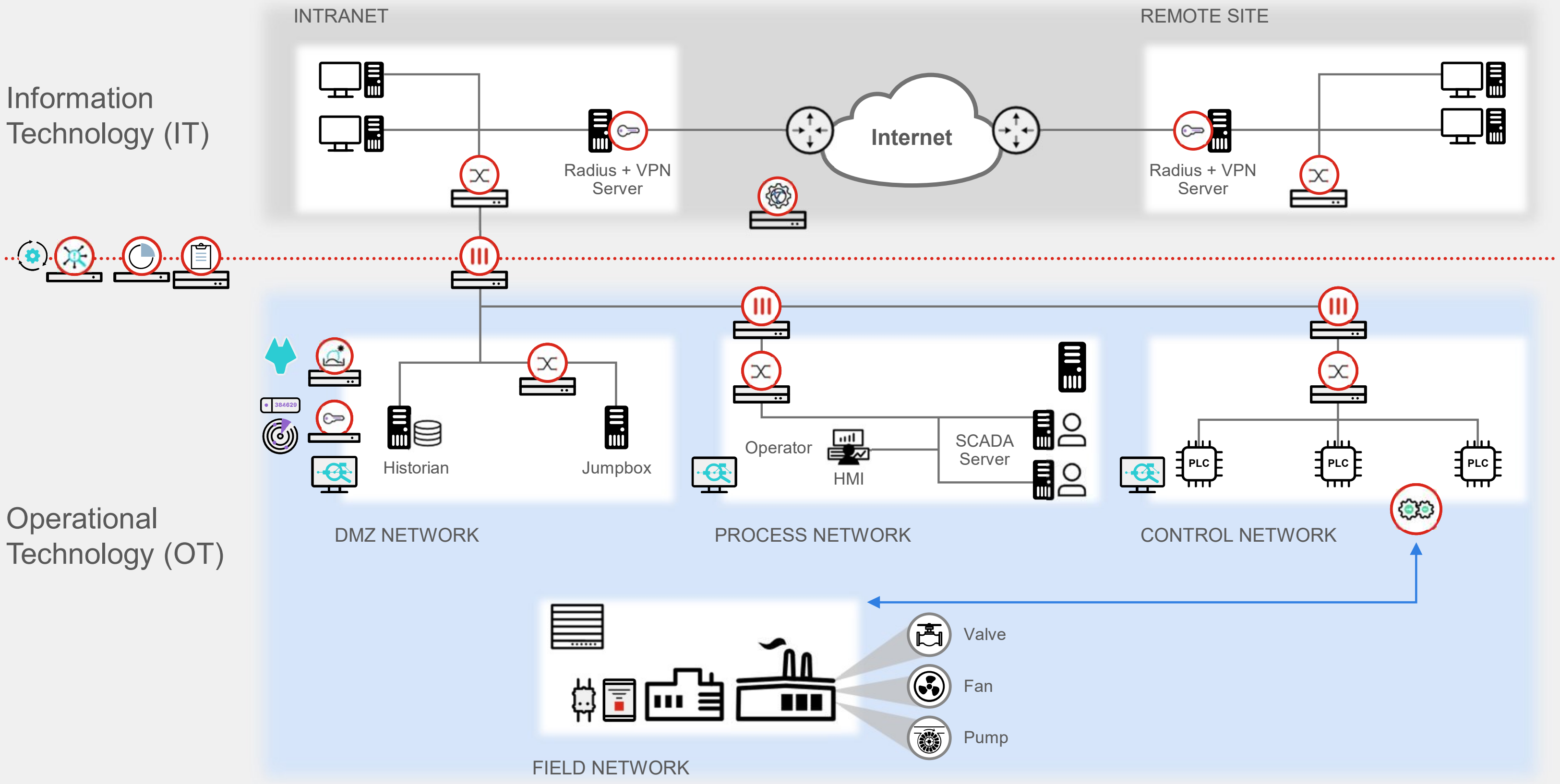
HMI

HMI/SCADA MASTER

PLC/RTU/IED

SENSORS/ACTUATORS

Casos de Uso Típicos – Defensa en Profundidad



- Zonas y conductos
- Conectividad remota segura
- Visibilidad profunda de OT
- Control de acceso basado en roles
- Asegurar endpoints críticos
- Centralizar la gestión de seguridad
- Amenaza Persistente Avanzada

Soluciones Fortinet Específicas para OT

Hardware Especializado

FortiGate Rugged 60F

FortiSwitch Rugged

FortiAP IPS-rated

- Firewalls robustecido para ambientes industriales
- Switches robustecido para ambientes industriales
- Puntos de acceso inalámbricos de uso exterior con evaluación IP

Información Especializada

- Servicios de control industrial
- Protocolos OT específicos
- Vulnerabilidades específicas de OT
- 1800+ firmas IPS y Control de Aplicaciones
- Soporte a los principales fabricantes de ICS

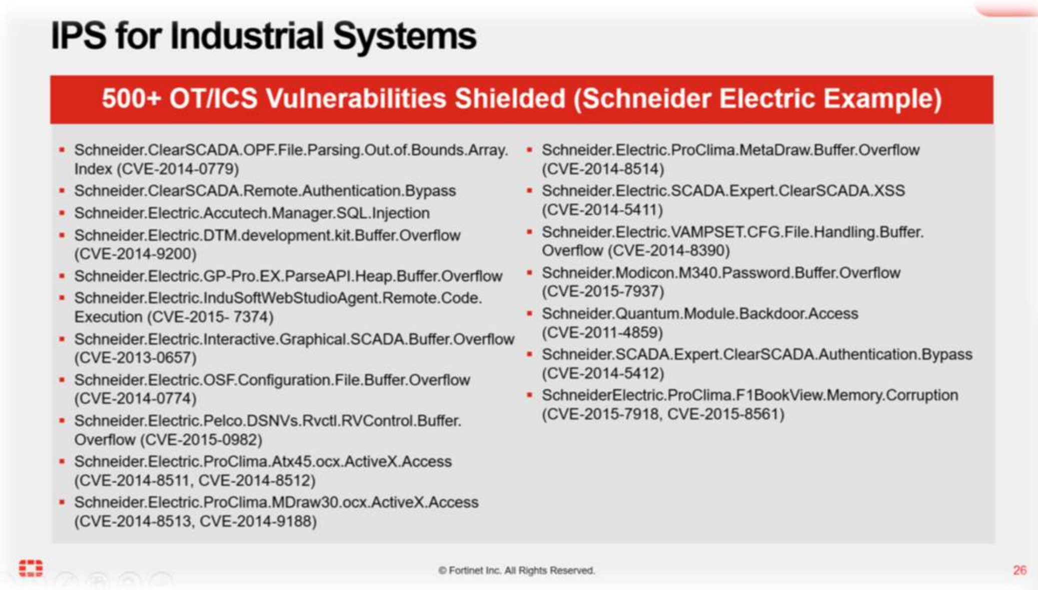
Equipo Especializado

- Soluciones referenciadas
- Profesionales experimentados para lo sector de OT
- Décadas en la industria
- Décadas de clientes

Ecosistema

- Expandir la plataforma a través de la integración
- Integración de más de 400 ecosistemas de Security Fabric
- Estrechas integraciones con los principales socios de seguridad de OT

La Mayor Cantidad de Vulnerabilidades y Aplicaciones Protegidas



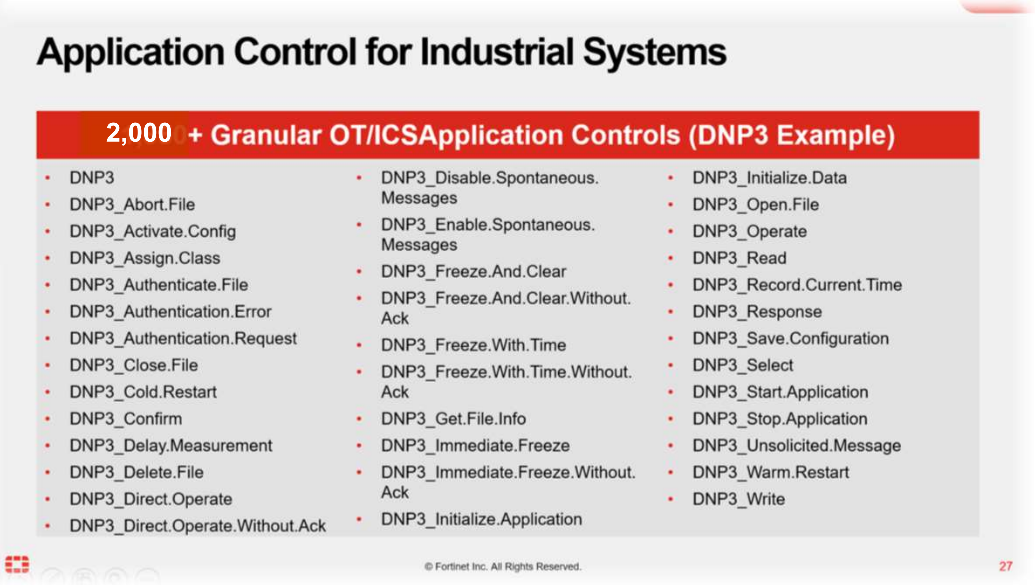
IPS for Industrial Systems

500+ OT/ICS Vulnerabilities Shielded (Schneider Electric Example)

- Schneider.ClearSCADA.OPF.File.Parsing.Out.of.Bounds.Array. Index (CVE-2014-0779)
- Schneider.ClearSCADA.Remote.Authentication.Bypass
- Schneider.Electric.Accutech.Manager.SQL.Injection
- Schneider.Electric.DTM.development.kit.Buffer.Overflow (CVE-2014-9200)
- Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow
- Schneider.Electric.InduSoftWebStudioAgent.Remote.Code. Execution (CVE-2015- 7374)
- Schneider.Electric.Interactive.Graphical.SCADA.Buffer.Overflow (CVE-2013-0657)
- Schneider.Electric.OSF.Configuration.File.Buffer.Overflow (CVE-2014-0774)
- Schneider.Electric.Pelco.DSNVs.Rvctl.RVControl.Buffer. Overflow (CVE-2015-0982)
- Schneider.Electric.ProClima.Atx45.ocx.ActiveX.Access (CVE-2014-8511, CVE-2014-8512)
- Schneider.Electric.ProClima.MDraw30.ocx.ActiveX.Access (CVE-2014-8513, CVE-2014-9188)
- Schneider.Electric.ProClima.MetaDraw.Buffer.Overflow (CVE-2014-8514)
- Schneider.Electric.SCADA.Expert.ClearSCADA.XSS (CVE-2014-5411)
- Schneider.Electric.VAMPSET.CFG.File.Handling.Buffer. Overflow (CVE-2014-8390)
- Schneider.Modicon.M340.Password.Buffer.Overflow (CVE-2015-7937)
- Schneider.Quantum.Module.Backdoor.Access (CVE-2011-4859)
- Schneider.SCADA.Expert.ClearSCADA.Authentication.Bypass (CVE-2014-5412)
- SchneiderElectric.ProClima.F1BookView.Memory.Corruption (CVE-2015-7918, CVE-2015-8561)

© Fortinet Inc. All Rights Reserved.

26



Application Control for Industrial Systems

2,000+ Granular OT/ICSApplication Controls (DNP3 Example)

- DNP3
- DNP3_Abort.File
- DNP3_Activate.Config
- DNP3_Assign.Class
- DNP3_Authenticate.File
- DNP3_Authentication.Error
- DNP3_Authentication.Request
- DNP3_Close.File
- DNP3_Cold.Restart
- DNP3_Confirm
- DNP3_Delay.Measurement
- DNP3_Delete.File
- DNP3_Direct.Operate
- DNP3_Direct.Operate.Without.Ack
- DNP3_Disable.Spontaneous. Messages
- DNP3_Enable.Spontaneous. Messages
- DNP3_Freeze.And.Clear
- DNP3_Freeze.And.Clear.Without. Ack
- DNP3_Freeze.With.Time
- DNP3_Freeze.With.Time.Without. Ack
- DNP3_Get.File.Info
- DNP3_Immediate.Freeze
- DNP3_Immediate.Freeze.Without. Ack
- DNP3_Initialize.Application
- DNP3_Initialize.Data
- DNP3_Open.File
- DNP3_Operate
- DNP3_Read
- DNP3_Record.Current.Time
- DNP3_Response
- DNP3_Save.Configuration
- DNP3_Select
- DNP3_Start.Application
- DNP3_Stop.Application
- DNP3_Unsolicited.Message
- DNP3_Warm.Restart
- DNP3_Write

© Fortinet Inc. All Rights Reserved.

27

Ecosistema y Alianzas Globales

Soluciones integradas para una amplia protección

FORTINET FABRIC-READY

OT TECHNOLOGY PARTNERS

Visibility and Threat Intelligence

- CLAROTY
- NOZOMI NETWORKS
- DRAGOS
- ordr
- np network perception
- CYBERX
- SCADAfence
- INDUSTRIAL DEFENDER
- tenable

Operations, Orchestration Automation

- OTORIO
- splunk>
- tdi
- rubrik
- BACKBOX
- SKYBOX SECURITY
- servicenow

Other

- SIEMENS RUGGEDCOM
- FORESCOUT
- radiflow
- OWL Cyber Defense
- DARKTRACE
- RAD

SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Control Vendors

- Schneider Electric
- ABB
- SIEMENS Ingenuity for life
- HITACHI Inspire the Next
- YOKOGAWA
- EMERSON
- Rockwell Automation
- SEL SCHWEITZER ENGINEERING LABORATORIES
- HIRSCHMANN A BELDEN BRAND
- Honeywell
- GE

Global System Integration

- Hewlett Packard Enterprise
- IBM
- Capgemini
- Orange Cyberdefense
- Atos
- LOGICALIS Architects of Change
- NTT
- accenture
- HCL

Other(s)

- Baker Hughes
- T-Systems
- Johnson Controls
- Eleven Paths
- World Wide Technology, Inc.

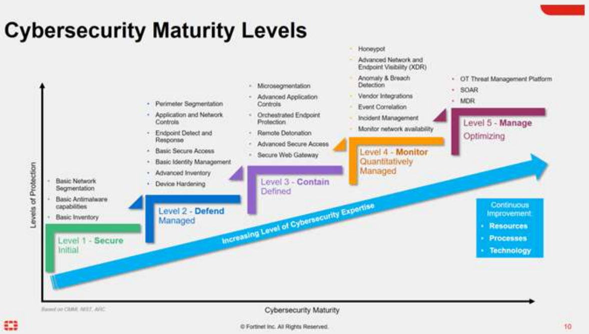
© Fortinet Inc. All Rights Reserved.

Note: Logos are a representative subset of the Security Fabric Ecosystem

Escala Madurez de Ciberseguridad de Fortinet

Adaptados a la Jornada de Cada Organización

1. **Iniciando la Jornada**



Cybersecurity Maturity Levels

- Basic Network Segmentation
- Basic Antimalware capabilities
- Basic Inventory

Level 1 - **Secure**
Initial

- Perimeter Segmentation
- Application and Network Controls
- Endpoint Detect and Response
- Basic Secure Access
- Basic Identity Management
- Advanced Inventory
- Device Hardening

Level 2 - **Defend**
Managed

- Microsegmentation
- Advanced Application Controls
- Orchestrated Endpoint Protection
- Remote Detonation
- Advanced Secure Access
- Secure Web Gateway

Level 3 - **Contain**
Defined

- Honeypot
- Advanced Network and Endpoint Visibility (XDR)
- Anomaly & Breach Detection
- Vendor Integrations
- Event Correlation
- Incident Management
- Monitor network availability

Level 4 - **Monitor**
Quantitatively Managed

- OT Threat Management Platform
- SOAR
- MDR

Level 5 - **Manage**
Optimizing

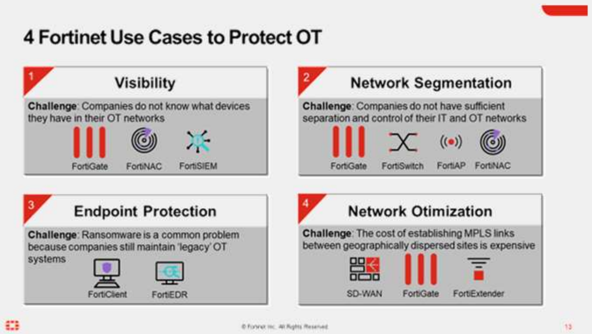
Continuous Improvement:

- **Resources**
- **Processes**
- **Technology**

Based on CMMI, NIST, ARC

© Fortinet Inc. All Rights Reserved. 10

2. **Casos de Uso Específicos**



4 Fortinet Use Cases to Protect OT

1 **Visibility**

Challenge: Companies do not know what devices they have in their OT networks

FortiGate FortiNAC FortiSIEM

2 **Network Segmentation**

Challenge: Companies do not have sufficient separation and control of their IT and OT networks

FortiGate FortiSwitch FortiAP FortiNAC

3 **Endpoint Protection**

Challenge: Ransomware is a common problem because companies still maintain 'legacy' OT systems

FortiClient FortiEDR

4 **Network Otimization**

Challenge: The cost of establishing MPLS links between geographically dispersed sites is expensive

SD-WAN FortiGate FortiExtender

© Fortinet Inc. All Rights Reserved. 13

3. **Desafío de Cumplir con Marcos Regulatorios y/o Políticas Internas**

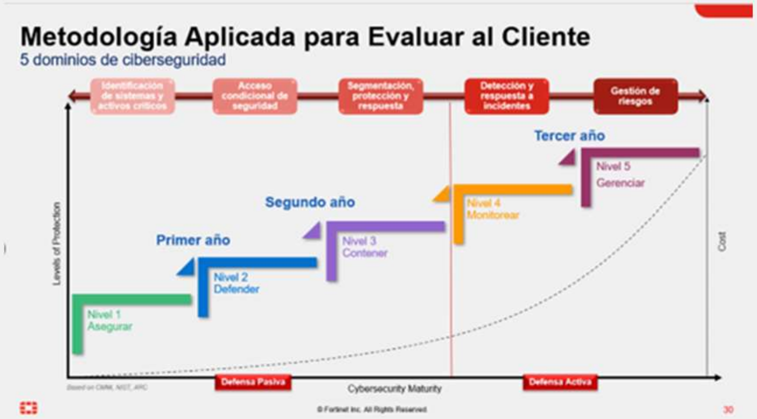
Effective Implementation of the NIST Cybersecurity Framework with Fortinet
(Companion Piece to "Security by Design: A Systems Road Map Approach")

How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet
(Companion piece to "Implementation Guide for Vendors and Integrators Working in NERC-CIP Environments")

Effective ICS Cybersecurity Using the IEC 62443 Standard
(Companion piece to "Managing ICS Security With IEC 62443")

Modelo de Evaluación de Madurez Cibernética

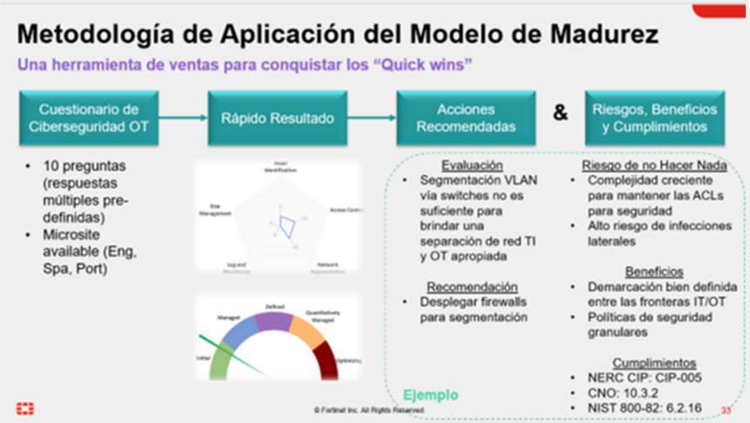
1



Metodología Aplicada para Evaluar al Cliente

5 dominios de ciberseguridad

2



Metodología de Aplicación del Modelo de Madurez

Una herramienta de ventas para conquistar los "Quick wins"

Cuestionario de Ciberseguridad OT → Rápido Resultado → Acciones Recomendadas & Riesgos, Beneficios y Cumplimientos

- 10 preguntas (respuestas múltiples pre-definidas)
- Microsite available (Eng, Spa, Port)

Evaluación
- Segmentación VLAN vía switches no es suficiente para brindar una separación de red TI y OT apropiada

Recomendación
- Desplegar firewalls para segmentación

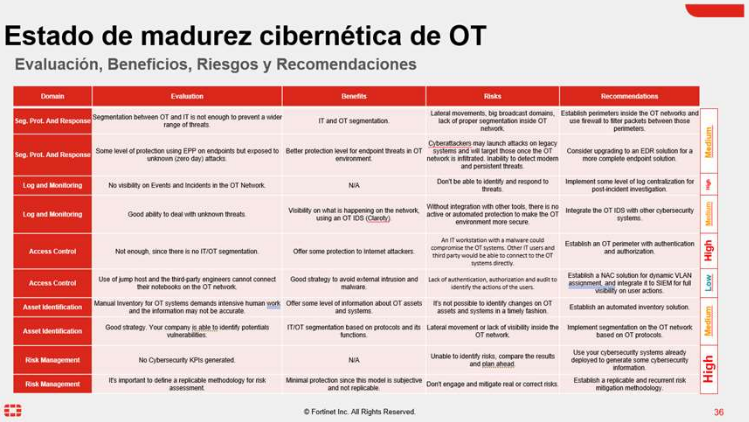
Riesgo de no Hacer Nada
- Complejidad creciente para mantener las ACLs para seguridad
- Alto riesgo de infecciones laterales

Beneficios
- Demarcación bien definida entre las fronteras IT/OT
- Políticas de seguridad granulares

Cumplimientos
- NERC CIP: CIP-005
- CNO: 10.3.2
- NIST 800-82: 6.2.16

Ejemplo

3

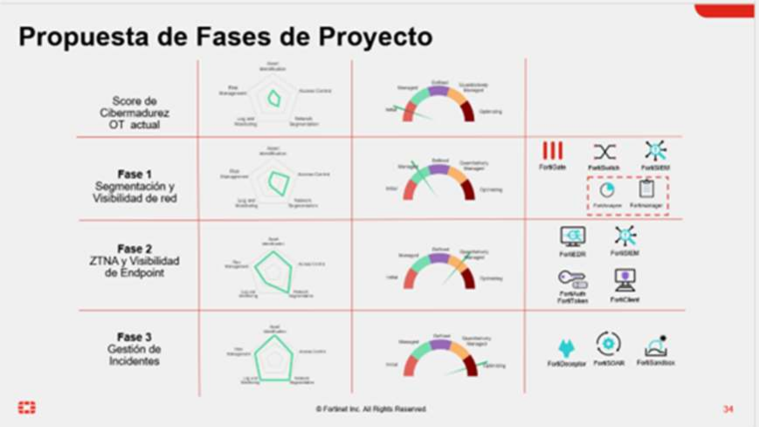


Estado de madurez cibernética de OT

Evaluación, Beneficios, Riesgos y Recomendaciones

Domain	Evaluation	Benefits	Risks	Recommendations	
Seg. Prot. And Response	Segmentation between OT and IT is not enough to prevent a wider range of threats.	IT and OT segmentation.	Lateral movements, big broadcast domains, lack of proper segmentation inside OT network.	Establish perimeters inside the OT networks and use firewall to filter packets between those perimeters.	Medium
Seg. Prot. And Response	Some level of protection using EPP on endpoints but exposed to unknown (zero day) attacks.	Better protection level for endpoint threats in OT environment.	Cyberattackers may launch attacks on legacy systems and will target those once the OT network is infiltrated. Inability to detect modern and persistent threats.	Consider upgrading to an EDR solution for a more complete endpoint solution.	
Log and Monitoring	No visibility on Events and Incidents in the OT Network.	N/A	Don't be able to identify and respond to threats.	Implement some level of log centralization for post-incident investigation.	High
Log and Monitoring	Good ability to deal with unknown threats.	Visibility on what is happening on the network, using an OT IDS (Claroty).	Without integration with other tools, there is no active or automated protection to make the OT environment more secure.	Integrate the OT IDS with other cybersecurity systems.	Medium
Access Control	Not enough, since there is no IT/OT segmentation.	Offer some protection to internet attackers.	An IT workstation with a malware could compromise the OT systems. Other IT users and third party would be able to connect to the OT systems directly.	Establish an OT perimeter with authentication and authorization.	High
Access Control	Use of jump host and the third-party engineers cannot connect their notebooks on the OT network.	Good strategy to avoid external intrusion and malware.	Lack of authentication, authorization and audit to identify the actions of the users.	Establish a NAC solution for dynamic VLAN assignment, and integrate it to SIEM for full visibility on user actions.	Low
Asset Identification	Manual inventory for OT systems demands intensive human work and the information may not be accurate.	Offer some level of information about OT assets and systems.	It's not possible to identify changes on OT assets and systems in a timely fashion.	Establish an automated inventory solution.	Medium
Asset Identification	Good strategy. Your company is able to identify potentials vulnerabilities.	IT/OT segmentation based on protocols and its functions.	Lateral movement or lack of visibility inside the OT network.	Implement segmentation on the OT network based on OT protocols.	
Risk Management	No Cybersecurity KPIs generated.	N/A	Unable to identify risks, compare the results and plan ahead.	Use your cybersecurity systems already deployed to generate some cybersecurity information.	High
Risk Management	It's important to define a replicable methodology for risk assessment.	Minimal protection since this model is subjective and not replicable.	Don't engage and mitigate real or correct risks.	Establish a replicable and recurrent risk mitigation methodology.	

4



Propuesta de Fases de Proyecto

Score de Cibermadurez OT actual

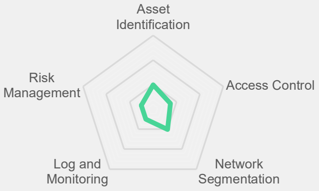
Fase 1 Segmentación y Visibilidad de red

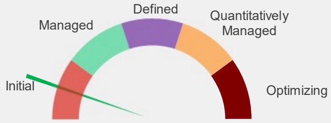
Fase 2 ZTNA y Visibilidad de Endpoint

Fase 3 Gestión de Incidentes

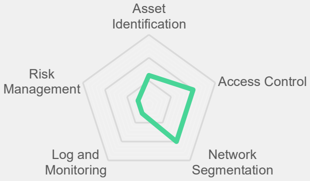
4. Un roadmap que los clientes usan internamente

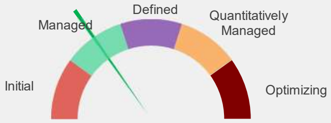
Today Status





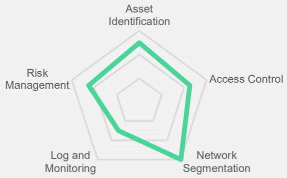
Phase 1
Zero Trust Network Access +
Segmentation IT/OT

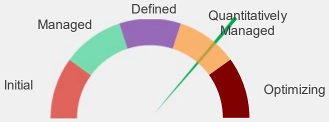




FortiGate
FortiSwitch
FortiSIEM
FortiAnalyzer
Fortimanager

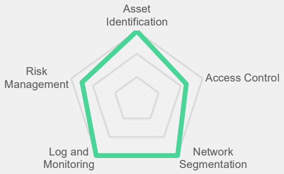
Phase 2
Incident
Management

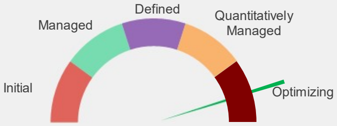




FortiEDR
FortiSIEM
FortiAuth
FortiToken
FortiClient

Phase 3
Persistent
Advanced
Threats
Protection



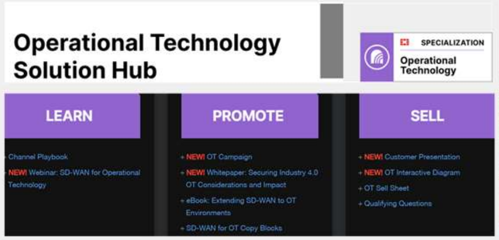


FortiDeceptor
FortiSOAR
FortiSandbox

Soporte y Capacitación de OT

Apoyo a los Socios/Canales

Partner Portal



Operational Technology Solution Hub

SPECIALIZATION
Operational Technology

LEARN	PROMOTE	SELL
Channel Playbook NEW! Webinar: SD-WAN for Operational Technology	+ NEW! OT Campaign + NEW! Whitepaper: Securing Industry 4.0 OT Considerations and Impact + eBook: Extending SD-WAN to OT Environments + SD-WAN for OT Copy Blocks	+ NEW! Customer Presentation + NEW! OT Interactive Diagram + OT Sell Sheet + Qualifying Questions

Digital security, everywhere you need it.

Protect the possibilities with Fortinet.

Manufacturing Plant Connected OT

Manufacturing Plant Floor

Site Público

Fundamentos

FORTINET
NSE Training Institute
Library
Securing OT

15 módulos (~10-15 min cada)

NSE 7 OT Security 6.4. Self-Paced

Técnico

OT Sales Training

Comercial

[Security Driven Networking] Cybersecurity for Safe, Reliable, Secure Industrial Control Systems (ICS)

Fast Track

Recursos Adicionales: Capacitación OT

OT Demo Room Dedicated at HQ

S#	Use Case
1	Secure Remote Access, Role-based Access Control,Single Sign-on, Multi-factorAuthentication
2	Network Segmentation andMicro-segmentation
3	Asset Management, Asset & Network Visibility
4	Advanced Threat Protection,Vulnerability Management
5	Centralized Logging, Monitoring and Reporting, Risk & ComplianceManagement
6	Centralized Management

Sumario

- Las redes OT están evolucionando debido a una variedad de presiones
  - OT tiene presiones y demandas similares y diferentes a las de TI
  - OT está reconociendo la necesidad de ciberseguridad en todo su entorno
- Fortinet es un proveedor de seguridad probado con soluciones para entornos de TI y OT
  - Amplia experiencia en tecnología operacional e infraestructura crítica desde 2004
  - Experiencia en convergencia de TI / OT, mercado emergente
- Fortinet tiene soluciones maduras, sólidas alianzas
  - Enfoque basado en un marco de referencia para tecnología operacional
  - Enfoque de consultoría con aliados y dentro de los procesos de Fortinet

Visibilidad

Control

Agilidad

FORTINET®

¡¡Nos mantenemos en contacto!!

Tecnología de Seguridad para

Proteger la Tecnología de Operación

Serafim Ivo de Faria
Business Development Manager
OTCI LATAM
idefaria@fortinet.com

¡Gracias!