Ciberseguridad

Foro ICAITren

17/11/2021

Indice

1/ Ciberseguridad
2/ Marco regulatorio
3/ Preguntas

Ciberseguridad

Ciberseguridad Ferroviaria

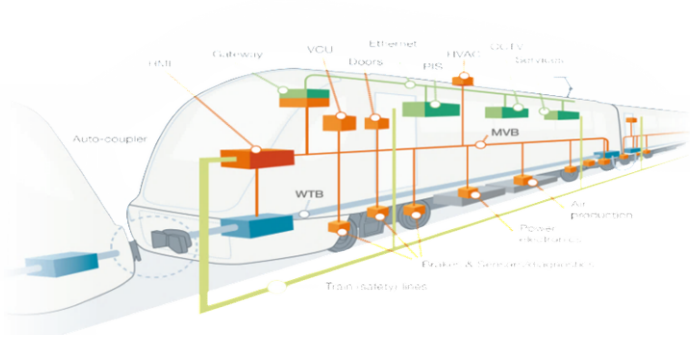
Introducción

¿Por qué estamos hablando de Ciberseguridad?

- Razones de mercado:
  - Cumplimiento legal
  - Ciberseguridad en los medios
  - Ciberseguridad en pliegos
  - Ciberseguridad durante el desarrollo de proyecto
  - Imagen corporativa/confianza de clientes
- Razones técnicas:
  - Tendencia a migrar a Ethernet
  - Cada vez más servicios digitales basados en IP
  - Cada vez más conectividad e intercambio de datos con tierra

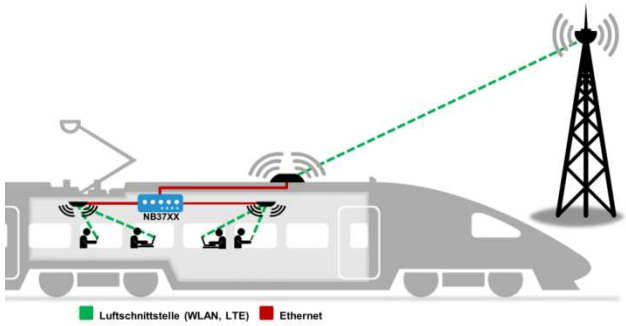
Ciberseguridad Ferroviaria

En los últimos años el nivel de las comunicaciones ha aumentado considerablemente



Múltiples sistemas embarcados

Tren Digital



Wifi Pasajeros

Ciberseguridad Ferroviaria

Introducción

¿Qué es ciberseguridad?

- La ciberseguridad es “gestión de riesgos asociados a la información”.
- Se centra en tres patas principales y dos adicionales:
  - Confidencialidad de los datos
  - Integridad de los datos
  - Disponibilidad de los datos
  - [Autenticidad]
  - [No repudio]
- Para garantizar esto y tras estudiar los riesgos, se aplicarán:
  - Controles organizativos
  - Controles procedimentales
  - Controles técnicos

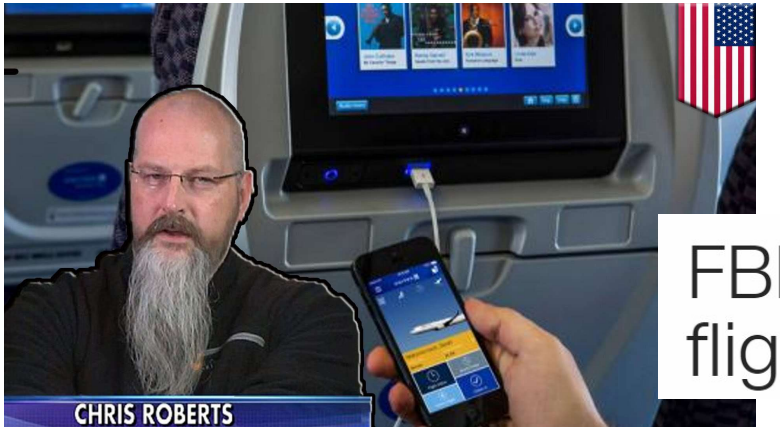
Ciberseguridad Ferroviaria

Ciberseguridad – IT vs OT

	IT	OT
RENDIMIENTO	Operación rápida	Operación en tiempo real
DISPONIBILIDAD	Interrupciones ocasionales toleradas	Interrupción intolerable
CONFIDENCIALIDAD	Privacidad es crítico	Menos crítico
CICLO DE VIDA DE LA TECNOLOGÍA	3 a 5 años	20+
OUTSOURCING	Común	Poco común
PARCHEO	Lo más rápido posible	Difícil
ANTI-VIRUS	Común	Difícil o imposible en OS de tiempo real
CONCIENCIACIÓN SOBRE SEGURIDAD INFORMÁTICA	Buena	Poca
SEGURIDAD FÍSICA	Poca, posible	Limitada
CAPACIDAD DE ADAPTACIÓN	Relativamente fácil	Difícil

Ciberseguridad Ferroviaria

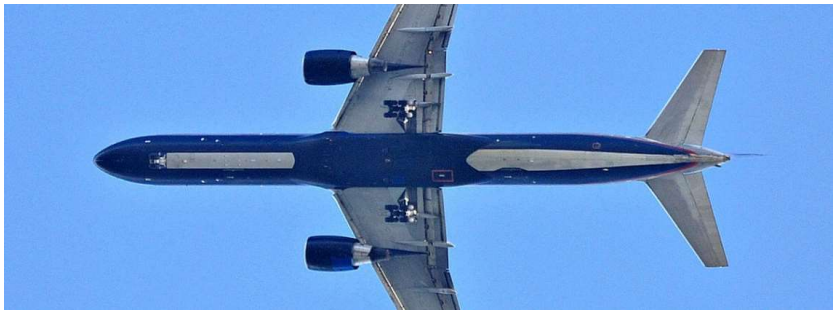
Un 'hacker' leonés revienta el sistema de entretenimiento de un vuelo Dubái-Madrid



FBI: Hacker claimed to have taken over flight's engine controls

Homeland Security team remotely hacked a Boeing 757

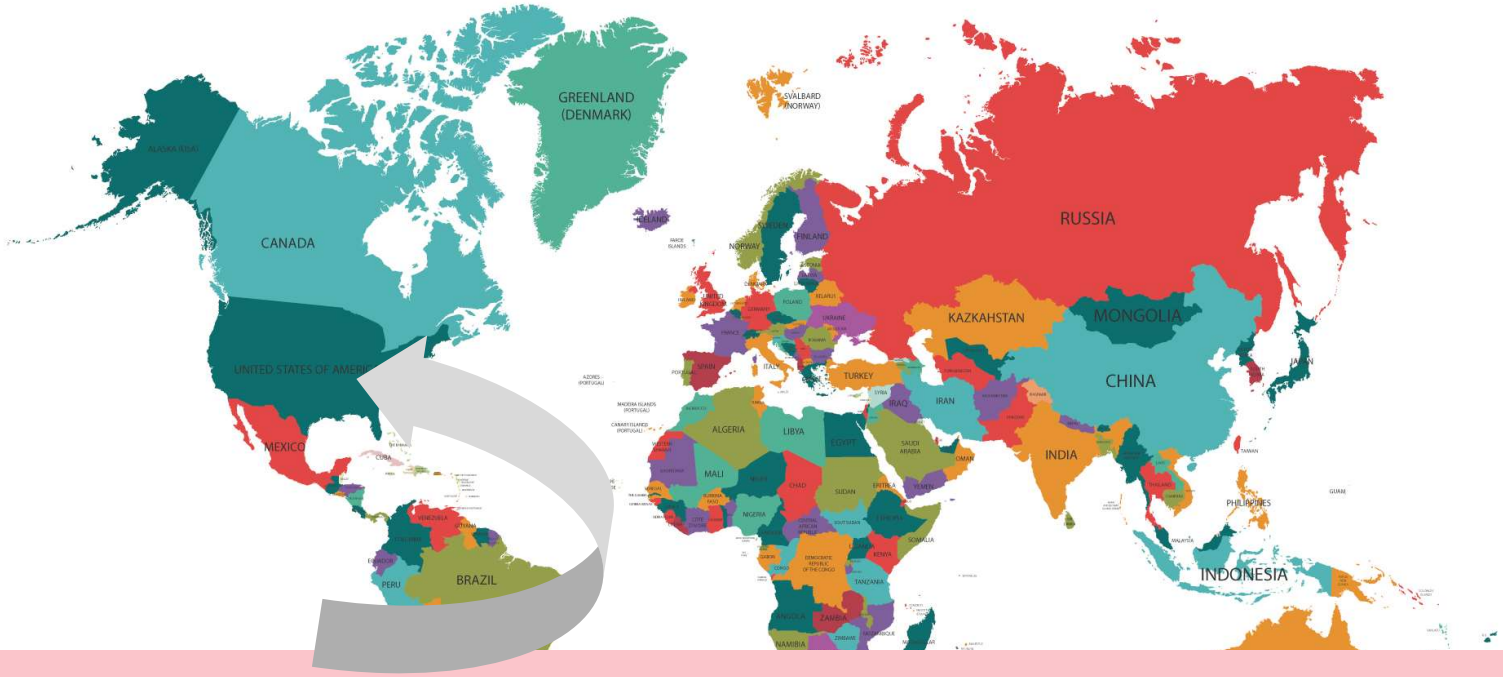
A Department of Homeland Security official admitted that a team of experts remotely hacked a Boeing 757 parked at an airport.



Ciberseguridad Ferroviaria

- Polonia, **2008**: Un adolescente causó estragos al descarrilar cuatro tranvías Lodz, Polonia, utilizando un control remoto de televisor adaptado. Hubo varias lesiones.

Ciberseguridad Ferroviaria

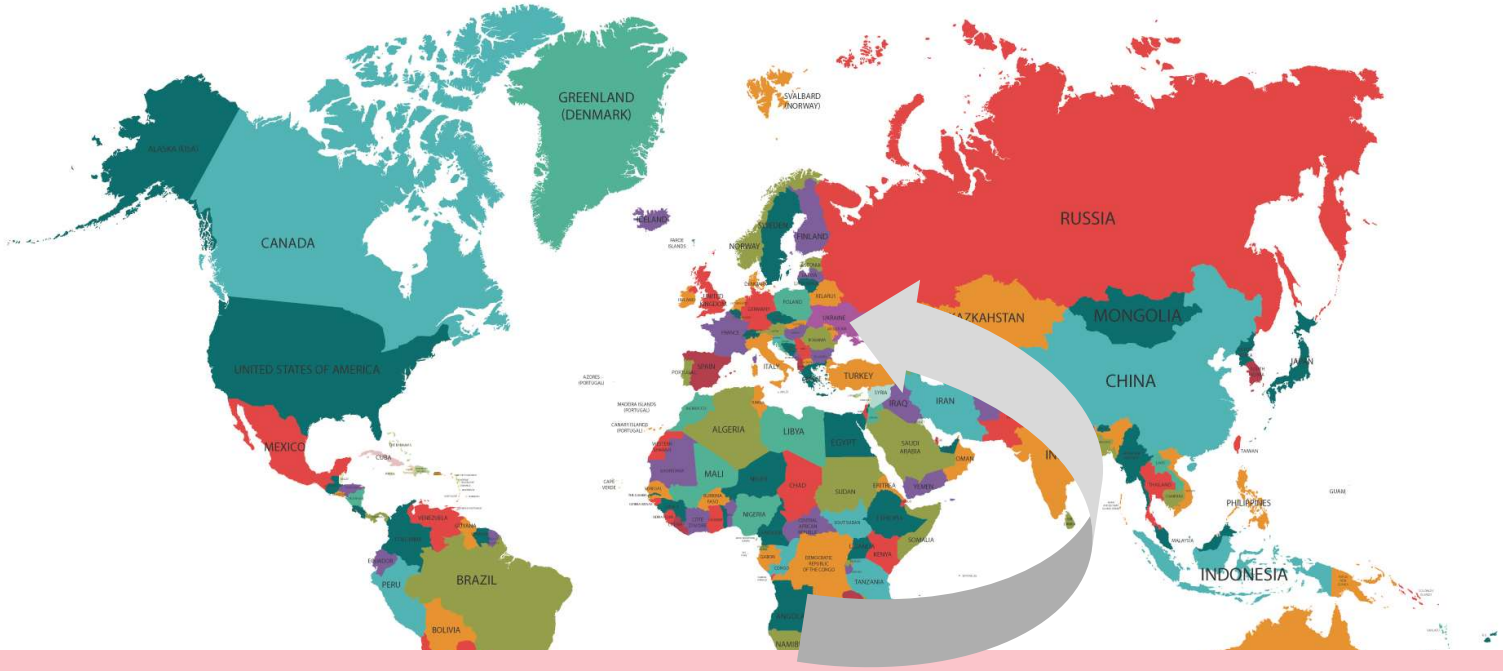


- EE. UU., **2011**: Piratas informáticos atacaron de forma remota ordenadores en el noroeste de los EE. UU., inutilizando las señales ferroviarias durante dos días

Ciberseguridad Ferroviaria

- Japón, **2015**: La red corporativa de Japan Railways Hokkaido fue violada mediante un ataque de phishing en un intento de robar información de seguridad ferroviaria

Ciberseguridad Ferroviaria



- Ucrania, **2015**: La red de un operador ferroviario ucraniano fue infiltrada con malware destructivo con la intención de interrumpir las operaciones ferroviarias

Ciberseguridad Ferroviaria

- Corea del Sur **2015** Piratas informáticos comprometieron la red de un controlador de tren automático de Corea del Sur y los datos extraídos que podrían contener información operativa relacionada. **2016**: Lanzada una campaña de Phishing contra dos operadores ferroviarios de Corea del Sur.

Ciberseguridad Ferroviaria

- EE.UU., **2016**: La Agencia de Transporte de San Francisco recibe un ataque que permite a los usuarios viajar gratis

Ciberseguridad Ferroviaria

- UK, **2016**: La empresa encargada de la seguridad en el transporte en UK, informa sobre 4 ciberataques importantes recibidos durante los últimos años.

Ciberseguridad Ferroviaria

- Worlwide, **2017:** Ataque de ransomware Wannacry: Ferrocarril ruso, Deustche Bahn.

Ciberseguridad Ferroviaria

- China, **2019:** Hacker web vende acceso de administrador a una empresa ferroviaria china

Ciberseguridad Ferroviaria

- España, **2020:** Ataque por ransomware a Adif: un grupo de ciberdelincuentes anuncia el robo de 800 GB y amenaza con difundir información sensible

Ciberseguridad Ferroviaria

- Un incidente de ciberseguridad puede tener impacto en:

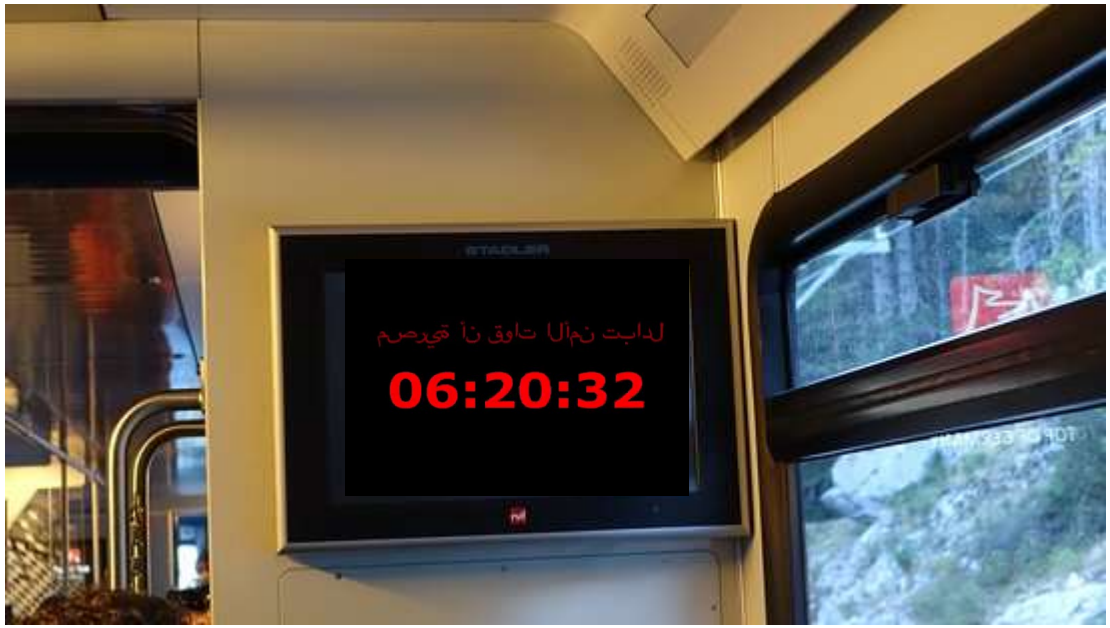
- La seguridad “safety” de los pasajeros.

- La reputación de la organización.

- Economía de la organización

Ciberseguridad Ferroviaria

- El pensamiento tradicional de **Safety no es aplicable a Security.**



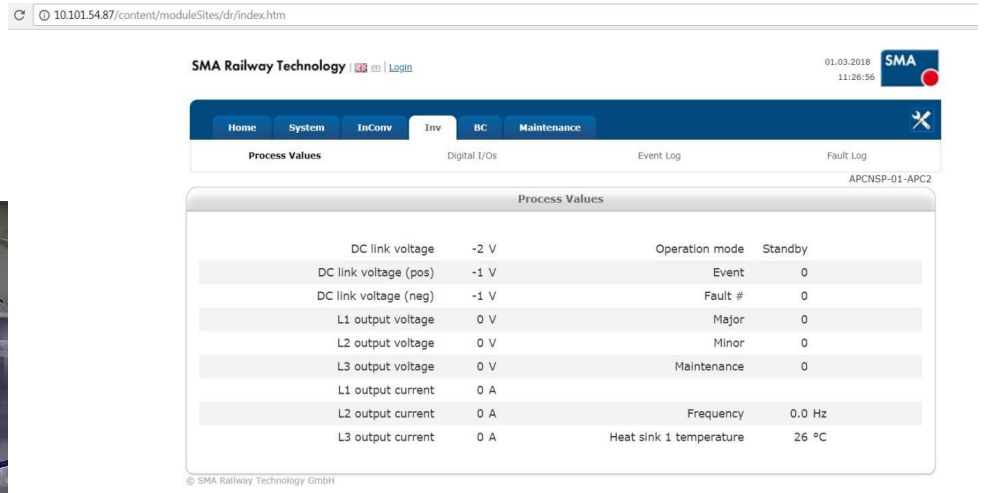
Ciberseguridad Ferroviaria

- Proyecto **HoneyTrain**
- En el año 2015 se detectan **2.745.267 ataques** durante 6 semanas.

1 semana = 457.544
1 día = 65.363
1 hora = 2.723
1 minuto = 45

Ciberseguridad Ferroviaria

- Hasta ahora la ciberseguridad únicamente se ha tenido en cuenta de **forma perimetral**.



Atacantes

Individuo / Activista

Trabajador descontento

Grupo Organizado / Competencia

Gobiernos

Ataques

ATAQUE	ORIGEN	IMPLICACIONES	SOLUCIÓN
Acceso No Autorizado a Sistemas	- Sin autenticación - Contraseñas por defecto - Contraseñas débiles	- Configuración maliciosa - Acceso a información (CCTV) - Distribución de contenido ilícito por megafonía/pantallas	- Requerir autenticación - Cambio de Contraseñas por defecto - Política de Contraseñas Seguras
DDoS/DoS (Denial-Of-Service)	- Agotamiento de recursos (flood) - Errores de código (crash)	- Parada del servicio - Activación de modos “bypass”	- Desarrollo seguro/buenas prácticas - Pruebas de rendimiento - Pruebas de fuzzing
Vulnerabilidades de Código	- Errores de código	- Desde parada del servicio a ejecución remota de código	- Desarrollo seguro/buenas prácticas - Análisis estático/dinámico de código - Auditorias de código - Parcheado de vulnerabilidades
MiTM (Man-In-The-Middle)	- ARP Poisoning - DNS Spoofing	- Captura de tráfico - Manipulación de tráfico	- ARP/DNS estáticas - Dispositivos de inspección de red - Cifrado de comunicaciones - Certificados
VLAN Hopping	- Switch Spoofing - Double tagging	- Acceso a VLANes no autorizadas	- Configuración adecuada de switches
Acceso Físico a Componentes	- Apertura de armarios - Acceso a cabina conductor	- Acceso a componentes - Acceso a tomas de red	- Protección física (llaves)
Malware	- Introducción de soporte externo (portatil, usb,…)	- Infección de sistemas	- Análisis previo de soportes - Custodia de soportes
Acceso no autorizado a la red	- Red WiFi de pasajeros - Red WiFi de mantenimiento	- Acceso a VLANes no autorizadas - Captura de tráfico - Manipulación de tráfico	- Aislamiento de redes WiFi - Protocolos WiFi seguros - Autenticación por certificado

Marco Regulatorio

Marco Regulatorio

Marco Regulatorio

- **Regulación Sector Ferroviario**
  - **Nada específico de Ciberseguridad en España**
  - **Otros países si (por ejemplo, UK con el "Railway Cybersecurity Guidance" del Department for Transport)**
- **Estándares Sector Ferroviario**
  - **Publicado:**
    - CLC/TS 50701: "Railway applications – Cybersecurity" (Adaptación de ISA-62443 al sector ferroviario)
  - **En desarrollo:**
    - Desarrollo de estándares para protección de señalización – Shift2Rail – X2Rail-1/3/5 [EUROPA]
- **Regulación General**
  - **Ciberseguridad**
    - Directiva NIS
  - **Protección de Datos de Carácter Personal**
    - RGPD/GDPR
- **Estándares Generales**
  - **Ciberseguridad**
    - ISO 27000
    - ISA 62443

Marco Regulatorio

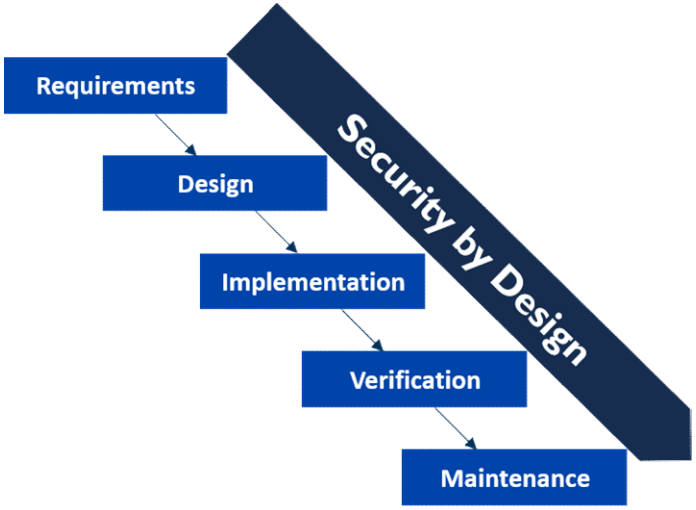
Directiva NIS - Directiva (UE) 2016/1148

- **Transposición en España: Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.**
  - **Identificar Centros de Respuesta a Incidentes**
    - Para [Sector Privado] -> **INCIBE-CERT** (Instituto Nacional de Ciberseguridad)
  - **Identificar Autoridades Competentes:**
    - Para [Operadores Críticos de Servicios Esenciales] -> **CNPIC** (Centro Nacional de Protección de Infraestructuras Críticas)
  - **Obligaciones:**
    - Notificar los incidentes que puedan tener efectos perturbadores significativos en dichos servicios y/o aquellos sucesos o incidencias que aún no hayan tenido un efecto adverso real (peligrosidad potencial).
    - Utilizar la plataforma del Centro de Respuesta para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes
    - Resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.
  - **Mínimos de ciberseguridad:**
    - La seguridad de los sistemas e instalaciones
    - La gestión de incidentes
    - La gestión de la continuidad de las actividades
    - La supervisión, auditorías y pruebas
    - El cumplimiento de las normas internacionales.

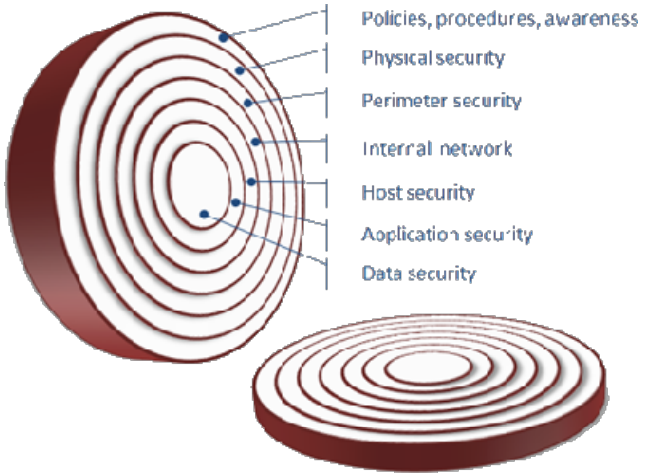
  - **Multas**
    - Desde multas de 100.000 euros para las infracciones leves hasta un millón de euros para las muy graves.

Marco Regulatorio

Security by Design



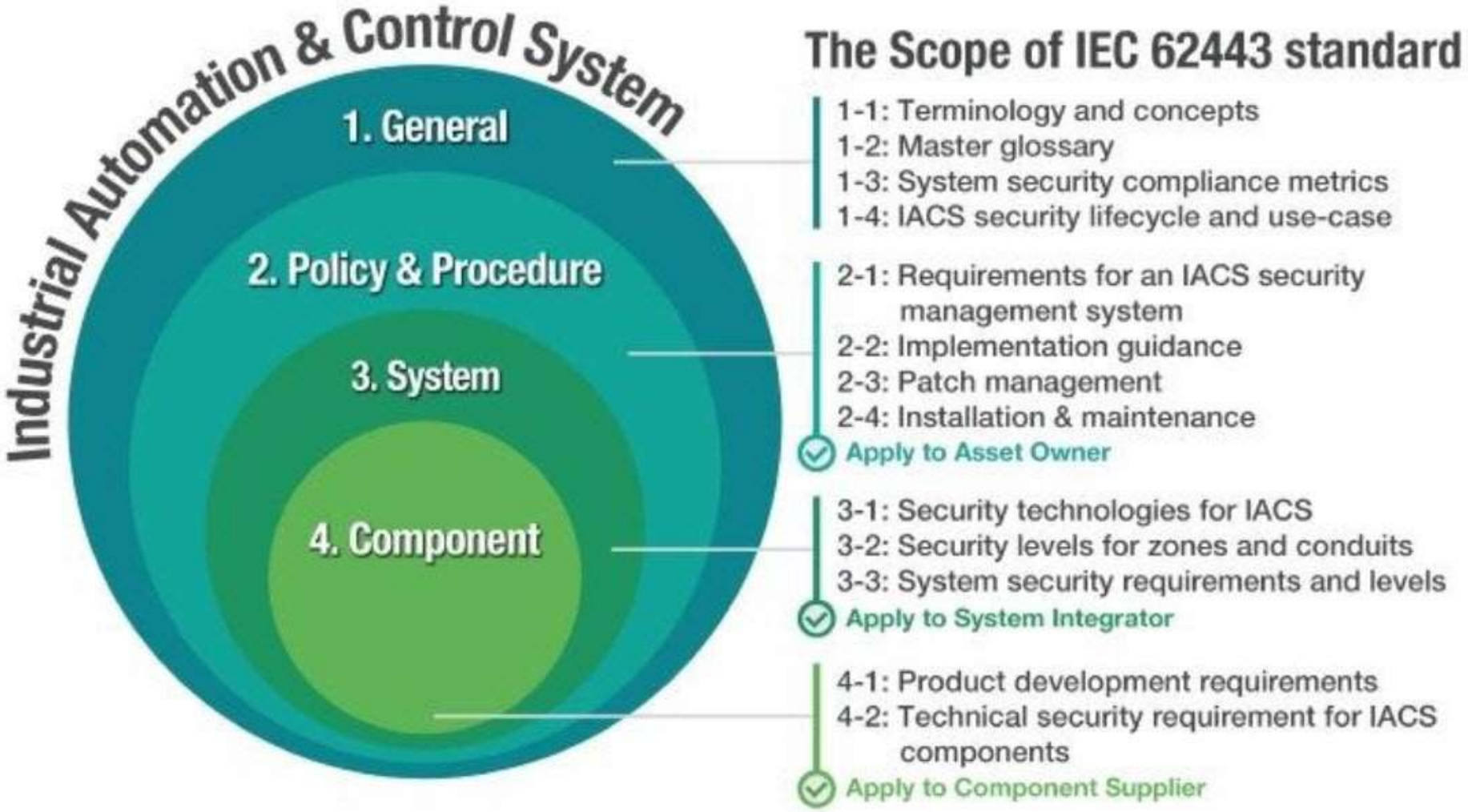
Defense In Depth



Security by Default

Marco Regulatorio

IEC 62443 Series – Multi-Industry Cybersecurity



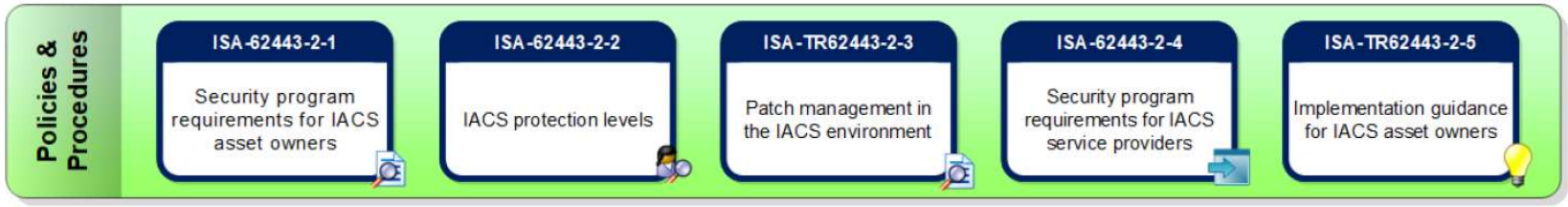
Marco Regulatorio

IEC 62443 Series – Multi-Industry Cybersecurity

- **General**
  - ISA-62443-1-1: Introduce los **conceptos y modelos** utilizados en toda la serie.
  - ISA-62443-1-2: Un **glosario** maestro de términos y abreviaturas utilizadas en toda la serie.
  - ISA-62443-1-3: Especifica los requisitos que deben abordarse en un conjunto completo de **métricas** para la serie 62443.
  - ISA-62443-1-4: Proporciona una descripción más detallada del **ciclo de vida** subyacente para la seguridad de IACS, así como **casos de uso** de servidores que ilustran varias aplicaciones.

Marco Regulatorio

IEC 62443 Series – Multi-Industry Cybersecurity



- **Policies & Procedures**

  - **ISA-62443-2-1:** Define los **requisitos para desarrollar un sistema** de administración de seguridad del sistema de control y automatización industrial (IACS) (SMS de IACS) y proporciona orientación sobre cómo desarrollar el sistema de administración. Utiliza la amplia definición y el alcance de lo que constituye un IACS descrito en ISA-62443-1-1.
  - **ISA-62443-2-2:** Proporcionar una manera consistente y repetible para **evaluar el nivel de protección** de la IACS en operación
  - **ISA-62443-2-3:** Describe un formato para el intercambio de información sobre el estado de los parches y su aplicabilidad, y brinda orientación sobre la planificación y la creación de un **programa de administración de parches** dentro de las organizaciones de proveedores de productos de IACS y propietarios de activos.
  - **ISA-62443-2-4:** Contiene **requisitos de seguridad para proveedores** de servicios de integración y mantenimiento para sistemas de control y automatización industrial (IACS).
  - **ISA-62443-2-5:** <Sin definir>

Marco Regulatorio

IEC 62443 Series – Multi-Industry Cybersecurity

- **System**
  - **ISA-62443-3-1:** Realiza encuestas y proporciona una evaluación de muchos **tipos actuales de tecnologías de ciberseguridad** basadas en la electrónica que pueden aplicarse para proteger un entorno IACS de intrusiones y ataques perjudiciales.
  - **ISA-62443-3-2:** Prescribe las actividades requeridas para realizar **evaluaciones de riesgos** de seguridad en un IACS nuevo o existente y las actividades de diseño requeridas para mitigar el riesgo a niveles tolerables.
  - **ISA-62443-3-3:** Prescribe los **requisitos de seguridad** para los sistemas de control relacionados con los siete requisitos fundamentales definidos en ISA-62443-1-1, y asigna niveles de seguridad del sistema (SL) al sistema en cuestión.

Marco Regulatorio

IEC 62443 Series – Multi-Industry Cybersecurity

- **Component**

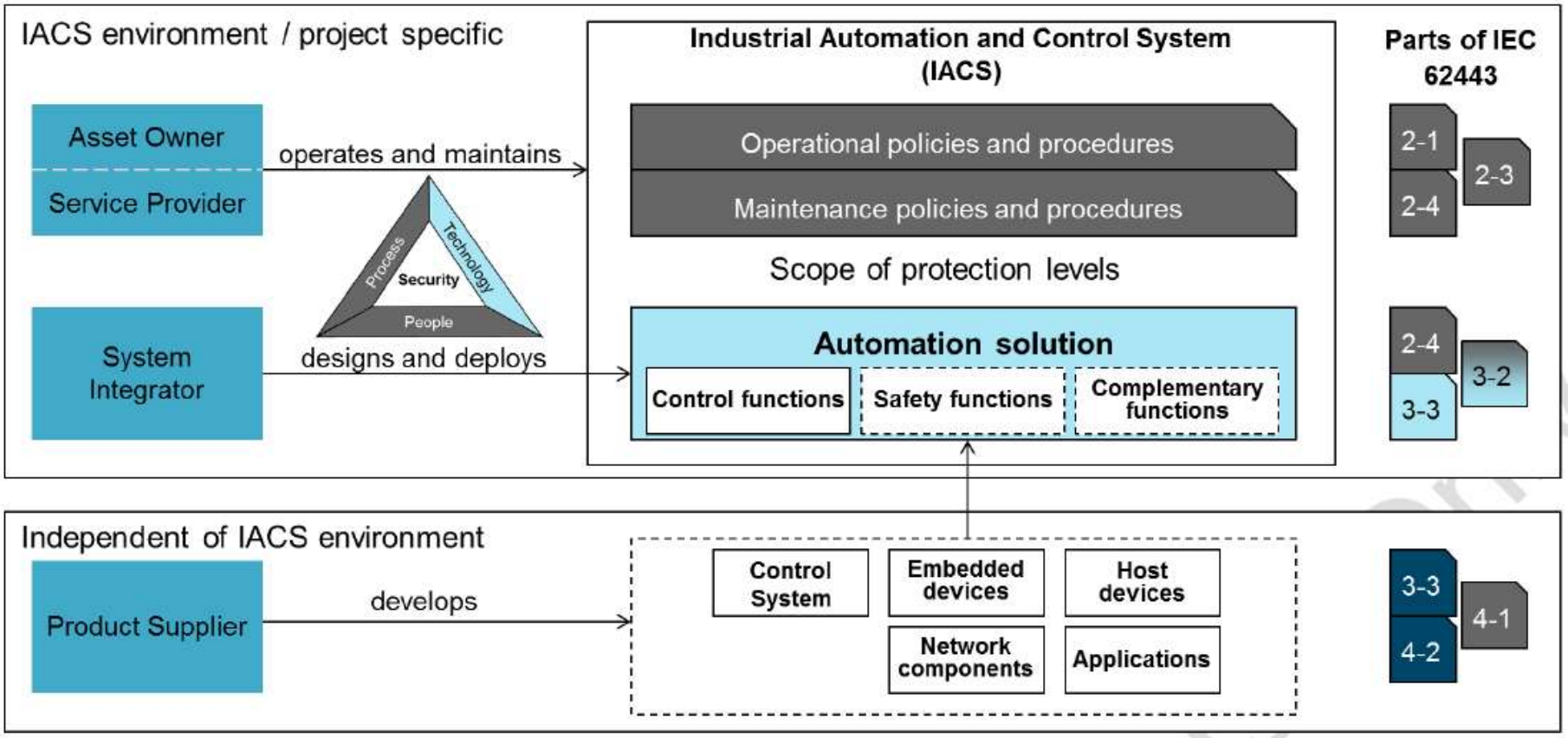
  - **ISA-62443-4-1:** Describe los **requisitos del ciclo de vida del desarrollo** de productos relacionados con la ciberseguridad para productos destinados al uso en el entorno de sistemas de control y automatización industrial y proporciona orientación sobre cómo cumplir los requisitos descritos para cada elemento.

  - **ISA-62443-4-2:** Prescribe los requisitos de **seguridad para los componentes** que se utilizan para construir sistemas de control. Estos requisitos se derivan de los requisitos del sistema para IACS definidos en el ISA-62443-3-3, y como tales, asignan niveles de seguridad (SL) de componentes que se basan en los niveles de seguridad del sistema.

Marco Regulatorio

IEC 62443 Series - Multi-Industry Cybersecurity

- **IEC-62443 - Seguridad para sistemas de control y automatización industrial**

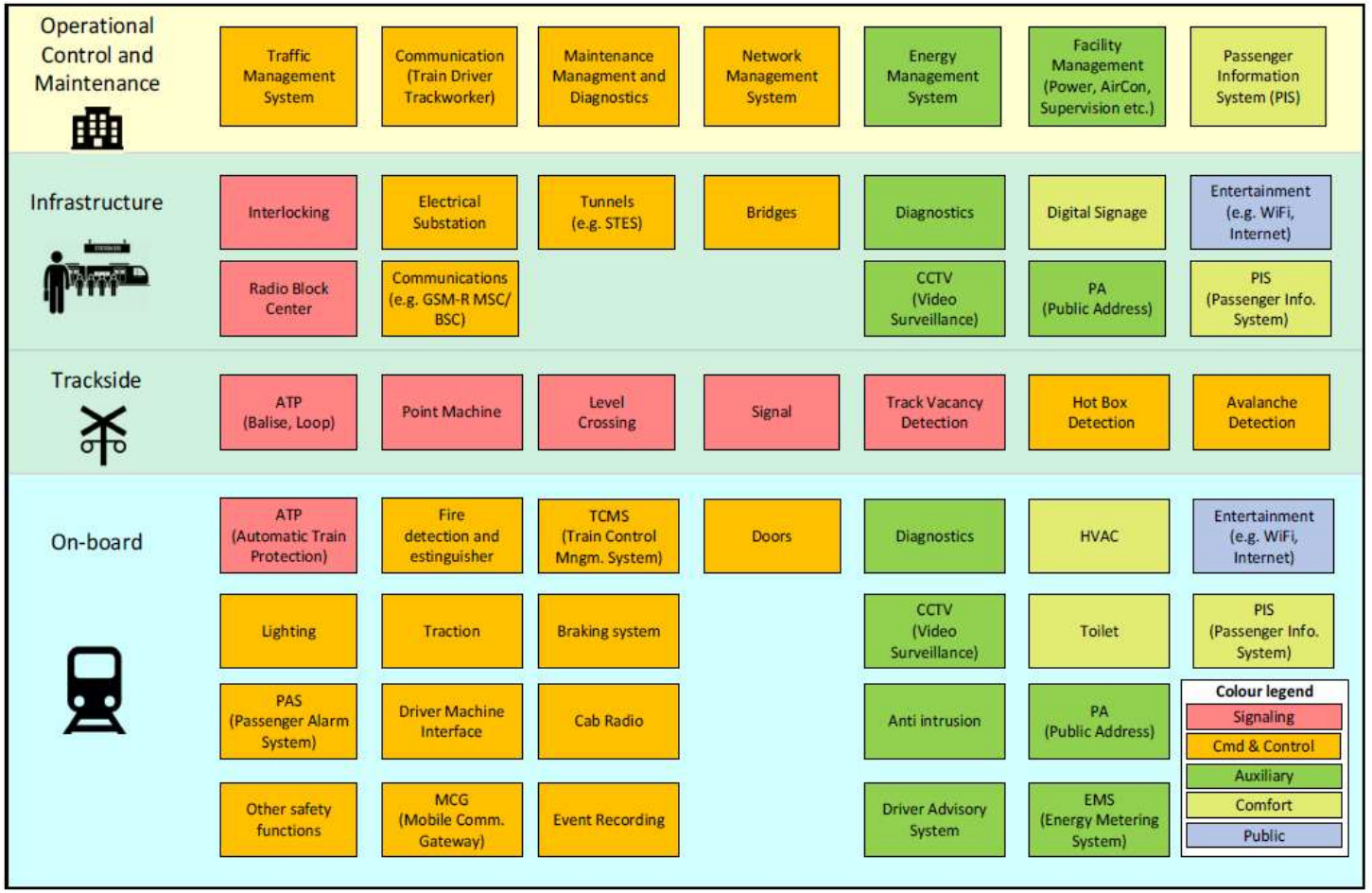


*Fuente IEC 62443

Marco Regulatorio

IEC 62443 Series - Multi-Industry Cybersecurity

- **ISA-62443 – Zonas y Conductos**
  - **Identificación de zonas (con distintos niveles de requerimientos de seguridad)**
  - **Identificación de comunicaciones entre zonas**



*Fuente CLC/TS 50701

Marco Regulatorio

IEC 62443 Series - Multi-Industry Cybersecurity

- **ISA-62443 – Security Levels**
  - **Niveles de Seguridad**
    - **SL-C – Security Level Capability – Nivel de Seguridad posible**
      - **Aplicable a zonas (y sistemas)**
      - **El nivel de seguridad que podría implementarse en dicha zona/sistema**
    - **SL-T – Security Level Target – Nivel de Seguridad objetivo**
      - **Podría ser aplicable a una zona**
      - **El nivel de seguridad que debe implementarse en esa zona o conducto**
    - **SL-A – Security Level Archieved – Nivel de Seguridad implementado**
      - **Aplicable a una zona**
      - **El nivel de seguridad con el que cuenta dicha zona o conducto**

Marco Regulatorio

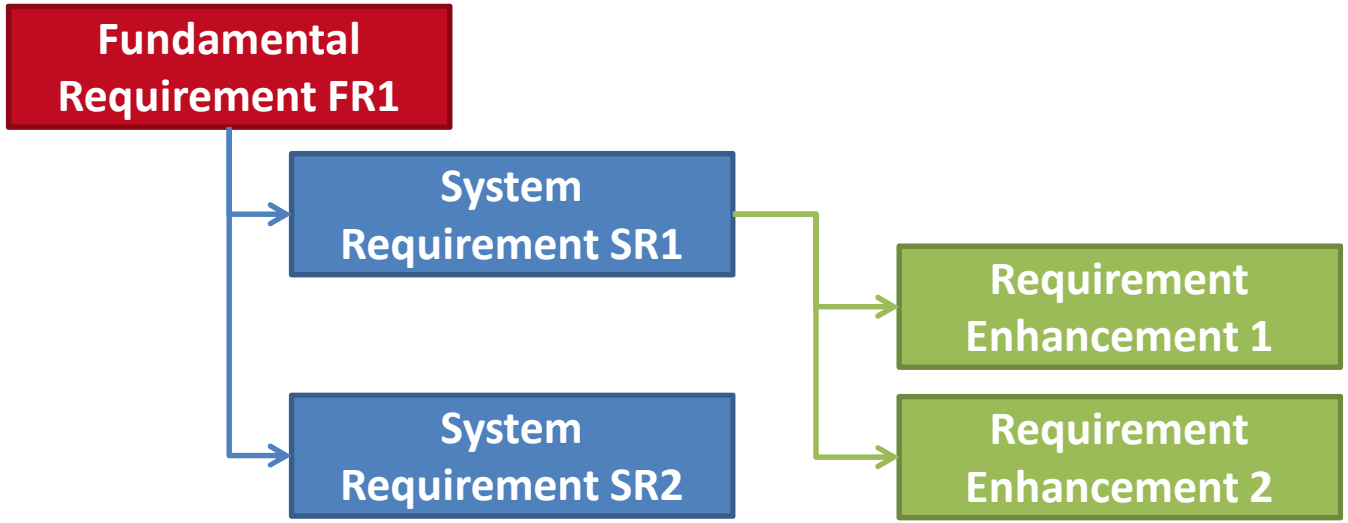
IEC 62443 Series - Multi-Industry Cybersecurity

- **ISA-62443 – Security Levels**
  - **La parte 3-3 propone identificar el nivel de una zona o un activo utilizando representación vectorial:**
    - **SL-T (XXXXXXXXXXX) {2 2 1 2 2 1 2}**
  - **Donde las 7 posiciones del vector son el nivel objetivo (en este caso) que el equipo es capaz de dar en relación a los requisitos esenciales definidos en la norma.**
    - **Los requisitos esenciales (FR) definidos en a parte 1-1 son:**
      - **FR 1: Indentification and authentication**
      - **FR 2: Use control**
      - **FR 3: System integrity**
      - **FR 4: Data confidentiality**
      - **FR 5: Restricted data flow**
      - **FR 6: Timely response to events**
      - **FR 7: Resource availability**

Marco Regulatorio

IEC 62443 Series - Multi-Industry Cybersecurity

- **ISA-62443 – Security Levels**
  - **Los 7 requisitos fundamentales (FR) tienen asociados a su vez un conjunto de requisitos de sistema (SR).**
  - **Los System requirements tienen a su vez Requirements enhancements (RE).**
  - **Para que en el vector de un sistema, puedas poner un nivel en un FR, tienes que cumplir unos determinados SRs y unos determinados RE que están definidos en la norma**



Marco Regulatorio

IEC 62443 Series - Multi-Industry Cybersecurity

- **ISA-62443 – Security Levels**
  - **El anexo B de la parte 3-3 aporta una tabla como la siguiente para cada FR**

SRs y Res – FR1	SL1	SL2	SL3	SL4
FR 1- Identification and authentication control (IAC)				
SR 1.1 – Human identification and authentication	✓	✓	✓	✓
RE 1 Unique identification and authentication		✓	✓	✓
RE 2 Multifactor authentication for untrusted networks			✓	✓
RE 3 Multifactor authentication for all networks			✓	✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE 1 Unique identification and authentication			✓	✓

Mario Oliva Pavón
Solution Development & Cybersecurity
Avda. de la Industria, 51. 28108 Alcobendas
Madrid, SPAIN
Tel. +34 91 789 27 50
e-mail: moliva@cafsignalling.com

Preguntas

TREN IRTENBIDE **GLOBALAK**
SOLUCIONES FERROVIARIAS **GLOBALES**
COMPREHENSIVE RAIL SOLUTIONS

ROLLING STOCK
SIGNALLING
SERVICES
EQUIPMENT & COMPONENTS
TRANSPORT SYSTEMS

www.caf.net