ANNEX C. Proposta temari Formació Nivell 3 Mòduls de Ciberseguretat al sector ferroviari (Ciberseguretat en el disseny de projectes aplicats al sector ferroviari, i Ciberseguretat a l'operació i al manteniment aplicat al sector ferroviari)

1. Ciberseguretat en el disseny de projectes aplicats al sector ferroviari

1.1. Context de Ciberseguretat Industrial (projectes).

- Context actual de ciberseguretat en infraestructures crítiques i transport.
- Requeriments normatius i marcs de referència (NIS2, PIC, CENELEC 50126/50128/50129/50701).
- Rol de la ciberseguretat en el cicle de vida del projecte ferroviari

1.2. Conceptes de tecnologíes d'operació (perspectiva projectes).

- Particularitats OT en entorns ferroviaris: disponibilitat, latència, determinisme.
- Sistemes d'automatització i control industrial aplicats al ferrocarril.
- Arquitectures típiques ferroviàries (SCADA, enclavaments, ATS/ATO/ATP, ERTMS/CBTC)

1.3. Xarxes indrustrials

- Protocols OT utilitzats en entorns ferroviaris.
- Comunicacions en sistemes de senyalització i control.
- Vulnerabilitats de protocols ICS/OT no autenticats.

1.4. Integració IT i OT

- Riscos i reptes de la convergència.
- Passarel·les, DMZ OT, segmentació i aïllament.
- Models Zero Trust aplicats a OT ferroviari.

1.5. Model d'actius ferroviaris segons CENELEC 50701

- Classificació d'actius i nivells d'automatització.
- Diferències entre zones i conductes.
- Aplicació del model a senyalització, telemandos, OCC i tren.

1.6. Models de Zones i Conductes

- Identificació de segments crítics.
- Requeriments de seguretat per zones i connectors OT.

1.7. Vulnerabilitats i amenaces en un ambient industrial ferroviari

- Amenaces sobre enclavaments, balises, sistemes d'energia i telemetria.
- Casuística real en el sector ferroviari (incidents internacionals).
- Amenaces dirigides a operadors de transport.

1.8. Threat Intelligence en el sector ferroviari

- Grups APT dirigits al sector ferroviari.
- Tècniques MITRE ATT&CK for ICS aplicades a sistemes ferroviaris.
- Tendències d'atac emergents (ransomware OT, laterals des d'IT, sabotatge digital).

1.9. Metodologia de diagnosi d'arquitectura de xarxes i sistemes i terceres parts

- Validació de disseny des d'un punt de vista de seguretat.
- Checklist de seguretat en projectes ferroviaris.
- Avaluació de ciberseguretat de terceres parts, integradors i fabricants.

1.10. Seguretat en la cadena de subministrament (Supply Chain)

- Riscos en firmware, components, PLCs i dispositius.
- SBoM (Software Bill of Materials) en projectes ferroviaris.
- Validació i certificació de components OT ferroviaris.

1.11. Ciberseguretat en el cicle de vida d'un projecte d'automatització industrial

- Procés de disseny, implantació, validació i acceptació.
- Proves FAT/SAT amb criteris de ciberseguretat.

1.11.1. Ciberseguretat a la fase de disseny

- Integració de requisits de seguretat des de l'origen.
- Identificació de superfícies d'atac en els plànols i arquitectures.
- Criteris de selecció d'equipament segur.

1.11.2. Problemàtica Security–Safety en el disseny

- Interacció entre SIL i ciberseguretat.
- Com compatibilitzar requisits de seguretat funcional i ciberseguretat.
- Riscos de common cause failure.

1.11.3. Definició i defensa de requisits de ciberseguretat

- Com documentar requisits segons CENELEC 50701.
- Com negociar-los amb fabricants i integradors.

1.11.4. Ciberseguretat a la fase de provisionament i execució

- Seguretat en instal·lació, parametrització i integració.
- Validació de dispositius OT i xarxes industrials.

2. Ciberseguridad a l'operació i al manteniment aplicat al sector ferroviari.

2.1. Context de Ciberseguretat Industrial (operació)

- Diferències entre projectes i operació.
- Garantia de continuïtat operacional.
- Gestió de canvis i manteniment segur.

2.2. Conceptes de tecnologies d'operació

- Arquitectures OT en operació quotidiana.
- Estructura i funcions del material mòbil, instal·lacions fixes i OCC.

2.3. Sistemes d'automatització i control industrial

- Particularitats ferroviàries en sistemes de control.
- Protocols i dispositius habituals.

2.4. Xarxes industrials i integració IT/OT
- Comunicacions tren–terra.
- Xarxes de senyalització i control descentralitzat.

2.5. Model d'actius ferroviaris segons CENELEC 50701
- Identificació d'actius crítics en operació.

2.6. Model de Zones i Conductes
- Aplicació pràctica a una operació ferroviària.

2.7. Vulnerabilitats i amenaces en operació
- Error humà, configuracions errònies i accessos insegurs.
- Amenaces internes i internes-intencionades.

2.8. Model d'amenaces i vulnerabilitats al sector ferroviari (error humà)
- Casos reals de fallades de configuració i errors d'operació.
- Bones pràctiques per reduir l'impacte del factor humà.

2.9. Diagnosi d'arquitectura de xarxes, sistemes i terceres parts
- Avaluació continuada d'exposició i riscos.

2.10. Cas d'ús pràctic — Arquitectura ERTMS
- Identificació de riscos per cada nivell d'automatització.
- Mesures bàsiques de protecció per cada nivell i subsistema.

2.11. Gestió de la ciberseguretat en un entorn d'automatització industrial
- Política, processos i rols implicats.
- Integració amb sistemes corporatius.

2.11.1. Anàlisi de riscos de ciberseguretat en un entorn ferroviari
- Metodologies recomanades (CENELEC, MAGERIT adaptat, IEC 62443-3-2).
- Quantificació i criteris d'acceptació.

2.11.2. Ciberseguretat a la fase d'operació
- Supervisió, actualitzacions, gestió de vulnerabilitats.
- Monitorització i SOC OT ferroviari.

2.11.3. Ciberseguretat a la fase de manteniment
- Manteniment predictiu i problemes de seguretat associats.
- Control d'accés de mantenidors.
- Gestió de portàtils de manteniment i eines OT.

3. IA aplicada al sector ferroviari i als entorns OT

3.1. Introducció a la IA en el sector ferroviari

- Tipus d'IA utilitzada: predicció, detecció d'anomalies, planificació, visió artificial.
- Aplicació en sistemes OCC, ERTMS, vigilància, manteniment, energia.

3.2. Riscos de seguretat i vulnerabilitats de la IA en OT ferroviari

- *Model poisoning*, *data poisoning*, manipulació de telemetria.
- Engany a models de detecció i visió artificial.
- Dependència operativa d'IA en sistemes de seguretat.

3.3. IA adversària en entorns ferroviaris

- Deepfakes per enginyeria social o manipulació operativa.
- Atacs adversaris en sensors i models vision-based.

3.4. IA en el cicle de vida de projectes ferroviaris

- Ús de IA per documentació, codi o configuracions → validació humana obligada.
- Impacte en FAT/SAT i en la certificació ferroviària.
- Consideracions de Safety quan la IA afecta funcions crítiques.

3.5. Ús segur de IA generativa per personal tècnic

- Bones pràctiques per evitar exfiltració de dades.
- Què no es pot introduir mai en una IA pública.
- IA en diagnosi i troubleshooting.

3.6. IA i marcs normatius

- Relació amb CENELEC 50701 (encara que indirecta).
- Relació amb ENS:
    - M.6, M.10 → configuració segura
    - M.15 → monitorització d'ús
    - M.17 → gestió d'incidents derivats d'IA

Yolanda Roldán Millán

Tècnica Assessoria Jurídica Laboral TMB