



OBJECTE

En l'àmbit de **FMB** i d'acord amb l'aplicació de les **recomanacions recopilades a la Normativa: UNE-EN IEC 62443, ISO 27000, ISO 27001, CENELEC EN 50126 RAMS i EN 50701 i l'Esquema Nacional de Seguretat (CCN)**, sobre els criteris del tractament de la ciberseguretat de l'àmbit OT, aquest document recopila els conceptes recollits dins del llistat SuC (System under Consideration) que s'han d'emplenar per a la gestió interna correcta dels sistemes ferroviaris operats o mantinguts per FMB. De la mateixa manera, aquest document adjunta un model complet de llistat SuC i els detalls per emplenar-los correctament.

DEFINICIÓ DEL SuC

El sistema en consideració (SuC) forma part del sistema ferroviari, format per subsistemes i components que proporcionen la funcionalitat requerida. Les amenaces de ciberseguretat poden comprometre aquesta funcionalitat i afectar la seguretat, les finances o la disponibilitat del sistema. Per identificar aquestes amenaces, cal descriure el SuC, les seves funcions i totes les interfícies.

Per a la descripció del SuC s'apliquen les regles següents:

- La definició del SuC ha d'incloure l'abast i els límits del sistema que es desenvoluparà i s'avaluarà.
- El SuC forma part d'un sistema operatiu per controlar els sistemes tècnics relacionats amb el ferrocarril.
- La descripció funcional i arquitectònica del SuC ha de seguir l'enfocament jeràrquic que es dona a la norma EN 50126-1:2017, 5.2 per identificar-lo exactament, incloses les vores i les interfícies externes.

DESCRIPCIÓ FUNCIONAL GENERAL

La ubicació del SuC dins de l'arquitectura ferroviària indica a quin tipus de sistema pertany (com ara material rodant, senyalització o infraestructura) i quines funcions principals exerceix. Per identificar les amenaces de ciberseguretat del SuC, incloses les vulnerabilitats conegudes, cal definir-ne les funcions, els límits i la funcionalitat que proporciona. Per tant, la identificació de les funcions principals s'ha de detallar tenint en compte:

- L'objectiu o propòsit del SuC, que inclou la definició de les funcions, els límits i les interfícies del sistema.
- Els escenaris operatius que descriuen com es farà servir el SuC i quins actors hi interactuen o hi interfereixen.
- El context d'implantació i ús.
- La vida útil esperada del SuC, tenint en compte les possibles actualitzacions necessàries en maquinari i programari.
- Els plans i conceptes de manteniment.
- Les restriccions ambientals que afecten el SuC.



CONCEPTES RECOLLITS AL LLISTAT SuC

- **ID*:** identificador únic associat a l'actiu. * Aquest camp només el pot emplenar el personal de TMB.
- **CARACTERÍSTIQUES DEL MAQUINARI (HW):** característiques que fan referència a la part física de l'actiu on s'aclareixen els detalls sobre la seva procedència i altres dades que fan falta per a la seva identificació única dins del conjunt d'actius.

Els camps que s'especifiquen en aquest apartat són els següents:

- **Identificador:** conjunt de lletres o números que serveixen per identificar un actiu per part de l'empresa.
- **Descripció:** explicació del producte. Exemple: ordinador portàtil.
- **Marca:** marca actual a què pertany l'actiu.
- **Model:** model a què pertany l'actiu.
- **Núm. de sèrie:** codi alfanumèric que identifica l'actiu, pot contenir només nombres o també lletres.
- **Fabricant** (camp de SAP): empresa que produeix l'actiu.
- **Proveïdor** (camp de SAP): empresa que ven l'actiu. Pot ser la mateixa que el fabricant o una altra de diferent.
- **Tipus:**
 - *Físic:* actiu tangible. Exemple: dispositius com un mòbil o un sensor.
 - *Virtual:* actiu intangible. Exemple: base de dades.
- **Adreça MAC*:** identificador únic que cada fabricant assigna a la targeta de xarxa dels seus dispositius. Exemple: 00:1e:c2:9e:28:6b * Si escau.
- **CARACTERÍSTIQUES PROGRAMARI (SW):** característiques de la part no física de l'actiu, és a dir, el conjunt de programes i dades que permeten que faci accions determinades. Pot ser el mateix en diferents actius.

Els camps que s'especifiquen en aquest apartat són els següents:

- **Sistema operatiu*:** sistema operatiu o programari de l'actiu. Exemple: Windows. * Si escau.
- **Versió del sistema operatiu:** versió actual del sistema operatiu. Exemple: XP.
- **Microprogramari:** microprogramari instal·lat al sistema. Cal especificar-ne el nom.
- **Actualització del microprogramari?:** si s'ha fet algun tipus d'actualització al microprogramari de l'actiu, marqueu "SÍ" i especifiqueu-ne la nova versió. Si no s'ha actualitzat, cal indicar "NO".
- **Necessita pedaç?:** si cal, especifiqueu "SÍ" i el tipus, en cas contrari, cal indicar "NO".



- **DADES DE COMPRA / MANTENIBILITAT:** Dades per identificar criteris financers, ambientals, d'impacte social, de gestió de riscos, qualitat de servei, seguretat i exercici al llarg de la vida de l'actiu.

Els camps que s'especifiquen en aquest apartat són els següents:

- **Data fabricació (camp de SAP):** cal indicar el dia, el mes i l'any de la fabricació de l'actiu en format DD/MM/AA.
 - **Data adquisició (camp de SAP):** cal indicar el dia, el mes i l'any de la compra de l'actiu en format DD/MM/AA.
 - **Data PES (camp SAP):** cal indicar el dia, el mes i l'any de la posada en marxa de l'actiu en format DD/MM/AA.
 - **Data inici de garantia:** cal indicar el dia, el mes i l'any de l'inici de la garantia de l'actiu en format DD/MM/AA.
 - **Data fi de garantia:** cal indicar el dia, el mes i l'any de la fi de la garantia de l'actiu en format DD/MM/AA.
 - **Valor d'adquisició (camp de SAP):** valor de compra (en euros) de l'actiu.
 - **Fiabilitat de referència:** previsió de la capacitat per executar correctament una funció sostinguda en el temps de l'actiu. Des del punt de vista de conèixer els possibles modes de fallada del sistema, la probabilitat d'ocurrència associada i l'efecte en la funcionalitat. Valor de l'equip o de la mitjana de la família de l'actiu.
 - **Anys de cicle de vida:** previsió de temps en què l'actiu farà el seu funcionament de manera normal.
- **EMPLAÇAMENT:** localització dels diferents actius en relació amb l'espai físic o virtual i en referència a un sistema.

Els camps que s'especifiquen en aquest apartat són els següents:

- **Ubicació:** localització específica, física o virtual, on es troba l'actiu.
 - **Servei essencial a què pertany:** servei de referència al qual correspon l'actiu.
- **INTERFÍCIES:** el SuC es pot veure compromès mitjançant l'accés a través de les seves interfícies, tant humanes com tècniques. Aquestes interfícies poden permetre que dispositius no autoritzats es connectin al sistema o que s'hi accedeixi a través de xarxes de comunicació. Per protegir el SuC, és important comptar amb una llista completa de totes les seves interfícies que inclogui la definició dels elements següents:
 - **Funció interfície:** funció per a la qual es fa servir cada interfície.
 - **Protocol de transport:** protocol utilitzat (com ara TCP o UDP), si està disponible.



- **Tipus de connexió física:** tipus de connexió com ara cable de coure, fibra òptica o sense fil.
 - **Dades funcionals:** dades que es gestionen mitjançant la interfície.
 - **Impacte:** impacte en cas de pèrdua de confidencialitat, integritat o disponibilitat.
 - **Funció dels sistemes adjacents:** funció que tenen els sistemes veïns.
 - **Interfícies organitzacionals:** interfícies que interactuen amb el SuC.
- **OBSERVACIONS:** text lliure per incloure, si voleu, qualsevol aclariment sobre el que s'ha comentat anteriorment.

COMMON PLATFORM ENUMERATION (CPE)

Es tracta d'un estàndard que permet identificar de manera única i estandarditzada programari, maquinari i sistemes operatius. Aquest sistema de nomenclatura facilita la comunicació sobre productes de tecnologia de la informació, especialment en el context de seguretat informàtica i de gestió de vulnerabilitats.

El format general d'un CPE és el següent:

cpe:cpe_version:[part]:[vendor]:[product]:[version]:[update]:[edition]:[language]:[sw_edition]:[target_sw]:[target_hw]:[other]

Components del CPE:

1. **cpe:** indica que és un identificador de CPE.
2. **cpe_version:** és la versió del format CPE. Actualment, la versió més utilitzada és 2.3.
3. **part:** tipus de producte, que pot ser:
 - *a (application)* per a aplicacions.
 - *o (operating system)* per a sistemes operatius.
 - *h (hardware)* per a maquinari.
4. **vendor:** nom del proveïdor o fabricant del producte.
5. **product:** nom del producte.
6. **version:** versió del producte (pot ser un rang o un asterisc * si no se n'especifica cap).
7. **update:** actualització o peça específic (pot ser un rang o un asterisc * si no se n'especifica cap).
8. **edition:** edició del producte (per exemple, "Professional", "Enterprise").
9. **language:** idioma del producte (per exemple, "en" per a anglès).
10. **sw_edition:** edició específica del programari, si escau (generalment es fa servir per a programari empresarial).
11. **target_sw:** programari de destinació, que pot ser afectat pel producte.
12. **target_hw:** maquinari de destinació, que pot ser afectat pel producte.
13. **other:** qualsevol altre atribut addicional que no s'hagi cobert als camps anteriors.