Arquitectura de xarxes embarcades i comunicacions tren-terra

A causa de l'evolució dels sistemes i serveis propis del tren, cada vegada és més necessari que aquests intercanviïn informació amb sistemes centrals i migrin cap a un escenari de 'tren connectat'. No obstant això, a causa que els sistemes propis del tren són crítics i cal aplicar-hi polítiques de ciberseguretat (tant d'obligat compliment legal com les marcades des de TMB com a polítiques internes), és necessari que els sistemes embarcats compleixin uns criteris d'arquitectura i de comunicacions generals que en garanteixin el bon funcionament i la seguretat.

A continuació, es llisten algunes premisses i requisits bàsics d'arquitectura que s'han de complir a les xarxes embarcades i comunicacions tren-terra del tren:

Identificador	Concepte	Aplicació	Descripció
ARQ_RE_CTT.1	General	Obligatori	Qualsevol equip embarcat o central que requereixi una integració i/o comunicacions tren-terra haurà de complir amb l'arquitectura, requisits, premisses, etc., indicats en tots els apartats del present document.
ARQ_RE_CTT.2	Comunicació tren-terra	Obligatori	Qualsevol equip embarcat o central que requereixi comunicacions tren-terra haurà de fer aquesta comunicació a través d'un encaminament privat de TMB (p. ex.: APN privat TMB, xarxa 5G privada, "wireless" privat, etc., segons serveis disponibles a la infraestructura de terra de TMB) i contra un tallafoc de TMB.
ARQ_RE_CTT.3	Comunicacions tren-terra	Recomanat	Les comunicacions dels sistemes embarcats amb sistemes centrals (via wifi i WAN) es faran preferentment a través de la passarel·la de comunicació ("communication gateway").
ARQ_RE_CTT.4	Comunicacions tren-terra	Recomanat	Per garantir la seguretat i disponibilitat, es recomana que les comunicacions tren-terra estiguin redundades, preferentment en extrems oposats del tren.
ARQ_RE_CTT.5	Xarxes Ethernet embarcades	Obligatori	El disseny i l'especificació de l'arquitectura de les xarxes i dels elements del tren, la seva connexió en local i la comunicació amb terra hauran de ser consensuats i aprovats per TMB. Aquesta aprovació haurà d'obtenir-se tant del departament de Metro com de l'àrea de tecnologia de TMB. No es donarà per tancada aquesta etapa fins que ambdues àrees de TMB hi donin l'aprovació. Per a això, el licitador haurà de lliurar la documentació necessària perquè s'avaluï i les iteracions successives segons els comentaris de TMB.

ARQ_RE_CTT.6	Xarxes Ethernet embarcades	Obligatori	La xarxa del tren s'ha de segmentar en subxarxes, amb les seves zones i conductes corresponents. Les subxarxes es definiran sobre la base de la tipologia dels sistemes i com són de crítics aquests. Aquest disseny haurà de realitzar-se amb una visió general de totes les xarxes embarcades i segons les normes aplicables legals i de TMB vigents a cada moment.
ARQ_RE_CTT.7	Xarxes Ethernet embarcades	Obligatori	La xarxa física estarà composta per commutadors gestionats distribuïts en tots els cotxes. Cada subxarxa ha de tenir una arquitectura en anell que en garanteixi la redundància i ha de disposar dels mecanismes necessaris per evitar bucles. Ha d'existir un element de xarxa de nivell 3 que gestioni la comunicació entre subxarxes. Aquest equip ha d'estar redundat als extrems oposats del tren i disposar dels mecanismes necessaris per gestionar aquesta redundància.
ARQ_RE_CTT.8	Xarxes Ethernet embarcades	Obligatori	La xarxa ha d'estar prou dimensionada perquè tots els elements d'un mateix cotxe es connectin als commutadors del mateix cotxe. El cablatge entre cotxes estarà limitat a la connexió entre commutadors.
ARQ_RE_CTT.9	Xarxes Ethernet embarcades	Recomanat	Es recomana que els commutadors del tren siguin de nivell 3 per permetre configurar diferents subxarxes al mateix commutador, de manera que s'optimitzi el nombre de commutadors per cotxe.
ARQ_RE_CTT.10	Xarxes Ethernet embarcades	Obligatori	Totes les zones definides a la xarxa embarcada han de comunicar-se entre si a través d'un tallafoc que permeti gestionar la seguretat entre aquestes. Aquest equip ha d'estar redundat als extrems oposats del tren i disposar dels mecanismes necessaris per gestionar aquesta redundància. Aquesta solució ha de ser coherent amb l'arquitectura de xarxa definida.
ARQ_RE_CTT.11	Xarxes Ethernet embarcades	Recomanat	El proveïdor haurà de fer una proposta per a una subxarxa de gestió sobre la base de la norma, que haurà de ser consensuada i validada amb TMB.
ARQ_RE_CTT.12	Integració	Obligatori	Totes les comunicacions amb sistemes externs han d'estar protegides mitjançant TLS (xifratge de dades en trànsit). S'han d'utilitzar protocols segurs, evitant versions obsoletes (TLS 1.0, 1.1 i anteriors estan prohibits).

			Addicionalment, caldrà implementar xifratge en repòs per a allò que contingui dades confidencials (PII, credencials, secrets, etc.).
ARQ_RE_CTT.13	Integració	Obligatori	Si es requereix autenticació d'usuaris, se n'ha d'implementar una de basada en SAML 2.0 i OpenID Connect (OIDC) i s'ha d'integrar amb el proveïdor d'identitat corporatiu. Per a “dispositius” / “elements no interactius” / ”sense usuaris”, es podrà emprar un mecanisme d'API-Key, o un “client_credentials grant” d'OIDC, per identificar-se i comunicar-se amb els sistemes corporatius, sempre a través de l'API de TMB.
ARQ_RE_CTT.14	Integració	Obligatori	Si es requereixen autoritzacions, s'ha d'utilitzar un esquema de control d'accés basat en rols (RBAC), atributs (ABAC) o preferiblement polítiques (PBAC), sota el principi d'assignació de mínim privilegi.
ARQ_RE_CTT.15	Integració	Recomanat	Les comunicacions entre els sistemes embarcats i l'exterior hauran de ser iniciades sempre pel sistema embarcat. Es recomana que tota comunicació, enviament de dades o accés a serveis de l'exterior del tren es faci a través de serveis web, publicats a través de l'API i Broker corporatius, que acabin en un sistema central en TMB o un al núvol. Això pot implicar, en molts casos, publicar serveis que inverteixin el flux de les comunicacions. Per exemple, no es podran “enviar” fitxers al tren, sinó que aquest els consumirà des d'un servei extern de publicació d'informació, etc.
ARQ_RE_CTT.16	Integració	Obligatori	Tota comunicació que justificadament no pugui iniciar-se des del tren, i hagi d'iniciar-se des de l'exterior, ha de respectar la segmentació de xarxes i els salts a través de les diferents zones desmilitaritzades (DMZ), OT i IT disponibles, mai no pot ser directa, i mai no s'ha d'aplicar a gran quantitat d'usuaris.
ARQ_RE_CTT.17	Integració	Recomanat	Implementar sistemes de “logging” centralitzats per recopilar i gestionar “logs” de totes les aplicacions i serveis. Mantenir registres d'auditoria de totes les interaccions als sistemes, per facilitar el seguiment i la resolució d'incidències. Es recomana l'ús d'agents com Filebeat, NXLog, Vector.dev o similars per a l'enviament de dades a través del Broker de TMB. S'ha d'evitar, costi el que costi, la transferència manual de fitxers de “log”.
ARQ_RE_CTT.18	Integració	Obligatori	Tota integració amb un sistema que no sigui “on-prem” i es realitzi contra un entorn al núvol i no sigui en

			modalitat “SaaS” ha d'estar sota el marc de govern centralitzat de TMB, com AWS Organizations o Azure Management Groups, per permetre la gestió centralitzada de polítiques de seguretat, control de costos i compliment normatiu.
ARQ_RE_CTT.19	Integració	Recomanat	Es facilitarà, en la mesura del possible, la integració de tots els entorns al núvol sota la protecció de les eines especialitzades que tingui TMB. Principalment, CASB (Cloud Access Security Broker) o CNAP (Cloud-Native Application Protection Platform) per a l'avaluació contínua de la postura de seguretat, la detecció de possibles desviacions de configuració, el monitoratge i el control d'accés, etc. Aquestes, al seu torn, estaran integrades amb el SIEM de TMB.
ARQ_RE_CTT.20	Integració	Obligatori	Per a les aplicacions al núvol, en modalitat SaaS, caldrà aplicar-hi els mateixos principis d'autenticació i autorització que la resta dels entorns. Hauran d'integrar-se amb el proveïdor d'identitat corporatiu mitjançant protocols estàndard com SAML 2.0 o OIDC. Les autoritzacions granulars es poden continuar aplicant a la plataforma SaaS i es realitzaran sobre la base de “rols” definits internament en l'AD de TMB. Aquests, al seu torn, arribaran en forma de “claim” o “assertion” per via estàndard en OIDC o SAML respectivament.