Arquitectura de redes embarcadas y comunicaciones tren-tierra

Debido a la evolución de los sistemas y servicios propios del tren, cada vez es más necesario que estos intercambien información con sistemas centrales migrando hacia un escenario de 'tren conectado'. No obstante, debido a la criticidad de los sistemas propios del tren y a la necesidad de aplicar políticas de ciberseguridad (tanto de obligado cumplimiento legal como las marcadas desde TMB como políticas internas) es necesario que los sistemas embarcados cumplan con unos criterios de arquitectura y de comunicaciones generales que garanticen su buen funcionamiento y seguridad.

A continuación, se listas algunas premisas y requisitos básicos de arquitectura que se han de cumplir en las redes embarcadas y comunicaciones tren-tierra del tren:

Identificador	Concepto	Aplicación	Descripción
ARQ_RE_CTT.1	General	Obligatorio	Cualquier equipo embarcado o central que requiera una integración y/o comunicaciones tren-tierra deberá cumplir con la arquitectura, requerimientos, premisas, etc. indicadas en todos los apartados del presente documento.
ARQ_RE_CTT.2	Comunicación tren-tierra	Obligatorio	Cualquier equipo embarcado o central que requieren comunicaciones tren-tierra deberá realizar dicha comunicación a través de un direccionamiento privado de TMB (p.ej.: APN privado TMB, red 5G privada, Wireless privado, etc. según servicios disponibles en infraestructura de tierra de TMB) y contra un firewall de TMB.
ARQ_RE_CTT.3	Comunicaciones tren-tierra	Recomendado	Las comunicaciones de los sistemas embarcados con sistemas centrales (vía WiFi y WAN) se realizarán preferentemente a través del Communication Gateway.
ARQ_RE_CTT.4	Comunicaciones tren-tierra	Recomendado	Para garantizar la seguridad y disponibilidad se recomienda que las comunicaciones tren-tierra estén redundadas, preferentemente en extremos opuestos del tren.
ARQ_RE_CTT.5	Redes ethernet embarcadas	Obligatorio	El diseño y especificación de la arquitectura de las redes y elementos del tren, su conexión en local y comunicación con tierra deberá ser consensuado y aprobado por TMB. Esta aprobación deberá obtenerse tanto por el departamento de Metro como por el área de tecnología de TMB. No se dará por cerrada está etapa hasta que ambas áreas de TMB den su aprobación. Para lo anterior, el licitante deberá entregar la documentación necesaria para su evaluación e iteraciones sucesivas según los comentarios de TMB.

ARQ_RE_CTT.6	Redes ethernet embarcadas	Obligatorio	La red del tren debe segmentarse en subredes con sus zonas y conductos correspondientes. La definición de subredes se realizará en base a la tipología de los sistemas y su criticidad. Este diseño deberá realizarse con una visión general de todas las redes embarcadas y según las normas aplicables legales y de TMB vigentes en cada momento.
ARQ_RE_CTT.7	Redes ethernet embarcadas	Obligatorio	La red física estará compuesta por switches gestionados distribuidos en todos los coches. Cada subred debe tener una arquitectura en anillo que garantice su redundancia y debe disponer de los mecanismos necesarios para evitar bucles. Debe existir un elemento de red de nivel 3 que gestione la comunicación entre subredes. Este equipo debe estar redundado en los extremos opuestos del tren y disponer de los mecanismos necesarios para gestionar dicha redundancia.
ARQ_RE_CTT.8	Redes ethernet embarcadas	Obligatorio	La red debe estar suficientemente dimensionada para que todos los elementos de un mismo coche se conecten a los switches del mismo coche. El cableado entre coches estará limitado a la conexión entre switches.
ARQ_RE_CTT.9	Redes ethernet embarcadas	Recomendado	Se recomienda que los switches del tren sean de nivel 3 permitiendo configurar distintas subredes en el mismo switch de manera que se optimice el número de switches por coche.
ARQ_RE_CTT.10	Redes ethernet embarcadas	Obligatorio	Todas las zonas definidas en la red embarcada deben comunicarse entre ellas a través de un Firewall que permita gestionar la seguridad entre ellas. Este equipo debe estar redundado en los extremos opuestos del tren y disponer de los mecanismos necesarios para gestionar dicha redundancia. Esta solución debe ser coherente con la arquitectura de red definida.
ARQ_RE_CTT.11	Redes ethernet embarcadas	Recomendado	El proveedor deberá hacer una propuesta para una subred de gestión en base a la norma, que deberá ser consensuado y validado con TMB.
ARQ_RE_CTT.12	Integración	Obligatorio	Todas las comunicaciones con sistemas externos deben estar protegidas mediante TLS (cifrado de datos en tránsito). Se deben utilizar protocolos seguros, evitando versiones obsoletas (TLS 1.0, 1.1 y anteriores están prohibidos).

			Adicionalmente será necesario implementar cifrado en reposo para aquello que contenga datos sensibles (PII, credenciales, secrets, etc).
ARQ_RE_CTT.13	Integración	Obligatorio	De requerir autenticación de usuarios, se debe implementar una basada en SAML 2.0 y OpenID Connect (OIDC) e integrarse con el proveedor de identidad corporativo. Para “dispositivos”/“elementos no interactivos”/”sin usuarios”, se podrá usar un mecanismo de API-Key, o un “client_credentials grant” de OIDC, para identificarse y comunicarse con los sistemas corporativos, siempre a través del API de TMB.
ARQ_RE_CTT.14	Integración	Obligatorio	De requerir autorizaciones, se debe utilizar un esquema de control de acceso basado en roles (RBAC), atributos (ABAC) o preferiblemente políticas (PBAC), bajo el principio de asignación de mínimo privilegio.
ARQ_RE_CTT.15	Integración	Recomendado	Las comunicaciones entre los sistemas embarcados y el exterior deberán ser iniciadas siempre por el sistema embarcado. Se recomienda que toda comunicación, envío de datos o acceso a servicios del exterior del tren se realice a través de servicios web, publicados a través del API y Broker corporativos, acaben en un sistema central en TMB o uno en el Cloud. Esto puede implicar en muchos casos publicar servicios que inviertan el flujo de las comunicaciones. Por ejemplo, no se podrán “enviar” ficheros al tren, sino que este los consumirá desde un servicio externo de publicación de información, etc.
ARQ_RE_CTT.16	Integración	Obligatorio	Toda comunicación que justificadamente no pueda iniciarse desde el tren, y deba iniciarse desde el exterior, debe respetar la segmentación de redes y los saltos a través de las diferentes zonas desmilitarizadas (DMZ), OT e IT disponibles, nunca puede ser directa, y nunca debe aplicar a gran cantidad de usuarios.
ARQ_RE_CTT.17	Integración	Recomendado	Implementar sistemas de logging centralizados para recopilar y gestionar logs de todas las aplicaciones y servicios. Mantener registros de auditoría de todas las interacciones en los sistemas. Para facilitar el seguimiento y la resolución de incidencias. Se recomienda el uso de agentes como Filebeat, NXLog, Vector.dev o similares para el envío de datos a través del Broker de TMB. Se debe evitar a toda costa la transferencia manual de ficheros de log.
ARQ_RE_CTT.18	Integración	Obligatorio	Toda integración con un sistema que no sea “on-prem” y se realice contra un entorno cloud y no sea en

			modalidad “SaaS”, debe estar bajo el marco de gobierno centralizado de TMB, como AWS Organizations o Azure Management Groups, permitiendo la gestión centralizada de políticas de seguridad, control de costos y cumplimiento normativo.
ARQ_RE_CTT.19	Integración	Recomendado	Se facilitará en la medida de lo posible la integración de todos los entornos cloud bajo la protección de las herramientas especializadas que tenga TMB. Principalmente, CASB (Cloud Access Security Broker) o CNAP (Cloud-Native Application Protection Platform) para la evaluación continua de la postura de seguridad, la detección de posibles desviaciones de configuración, el monitoreo y control de acceso, etc. Estas, a su vez, estarán integradas con el SIEM de TMB.
ARQ_RE_CTT.20	Integración	Obligatorio	Para las aplicaciones Cloud, en modalidad SaaS, se deberá aplicar los mismos principios de autenticación y autorización que el resto de los entornos. Deberán integrarse con el proveedor de identidad corporativo mediante protocolos estándar como SAML 2.0 u OIDC. Las autorizaciones granulares se pueden seguir aplicando en la plataforma SaaS y se realizaran en base a “roles” definidos internamente en el AD de TMB. Éstos a su vez, llegaran en forma de “claim” o “assertion” por vía estándar en OIDC o SAML respectivamente.