



Transports Metropolitans
de Barcelona

Plec de l'eina de monitorització del Telecomandament de Trànsit

Versió 1.1

Novembre 2023

Contingut

Introducció:	3
Necessitats:	4
Situació actual del Telecomandament de Trànsit:.....	5
Requeriments de l'eina:	7
1. Requeriments funcionals:	7
A. Monitorització telecomandament de trànsit:.....	7
B. Monitorització comunicacions	8
2. Requeriments interfície amb usuari:.....	9
3. Requeriments de l'eina: Interfícies amb telecomandament de trànsit i altres sistemes	10
Altres tasques.....	12
Requeriments ciberseguretat:	13
Arquitectura servei:.....	15

Introducció:

Es requereix una millora en les eines de monitorització del telecomandament de trànsit de xarxes convencionals.

La millora té l'objectiu de disposar d'informació ampliada del sistema de telecomandament a tots els àmbits: maquinari, sistema operatiu, serveis i aplicacions del telecomandament, monitorització de llocs d'operació, monitorització d'alarmes del telecomandament, monitorització del maquinari de comunicacions, monitorització de les comunicacions.

Aquesta informació haurà de millorar els temps de resposta en cas d'incidència, així com realitzar actuacions preventives que a dia d'avui amb la informació disponible no es poden realitzar.

A més, la disponibilitat d'informació del sistema també hauria de permetre la connexió de les dades disponibles, ja siguin estats i alarmes dels actius que controla, informes o indicadors, amb altres sistemes externs a la pròpia eina.

Es requereix que l'eina disposi de la possibilitat de connectar-la amb altres sistemes externs.

Necessitats:

1. Subministrament del maquinari necessari per suportar l'eina en l'entorn actual tant del telecomandament de trànsit com de serveis auxiliars al mateix (moviola enclavaments Siemens).
2. Subministrament de l'aplicació adequada per connectar-se a fonts de dades, processar les dades i generar els corresponents informes i indicadors
3. Desenvolupament o configuració d'una interfície de connexió amb altres sistemes, adaptant la interfície a les necessitats que pugui demanar Metro Barcelona. Aquesta interfície ha de ser multicanal i ha de permetre tant enviar dades com sol·licitar-ne a demanda.
4. Configuració de l'eina / aplicació principal:
 - a. Configuració de les fonts de dades
 - b. Configuració de la recepció de les fonts de dades
 - c. Configuració d'informes: alarmes i indicadors
5. Formació per la configuració dels informes / indicadors de forma autònoma, incloent com a mínim una formació presencial i adaptant-se a les necessitats del personal de manteniment (torns rotatius, etc)
6. Documentació de tot el sistema, incloent esquemes d'instal·lació, esquemes de funcionament / arquitectura de l'eina, documentació del funcionament del sistema i documentació de manteniment de l'eina si es requereix
7. Tots els elements del sistema han de ser compatibles amb el telecomandament de trànsit actualment instal·lat a Ferrocarril Metropolità de Barcelona, del proveïdor Siemens Automation SL (Rail9000). La compatibilitat ha d'estar certificada per part del proveïdor per evitar qualsevol afectació al sistema en producció, degut a que pot provocar incidències al Servei Comercial.

Situació actual del Telecomandament de Trànsit:

Maquinari:

Actualment el telecomandament de trànsit està distribuït en dos centres de control. Un a Sagrada Família i un altre a La Sagrera. El centre de control de La Sagrera és el principal i el centre de control de Sagrada Família és el de suport per als llocs d'operació mentre que totes dues ubicacions tenen com a missió donar servei a nivell de servidors al sistema, sense que un sigui principal i l'altre secundari.

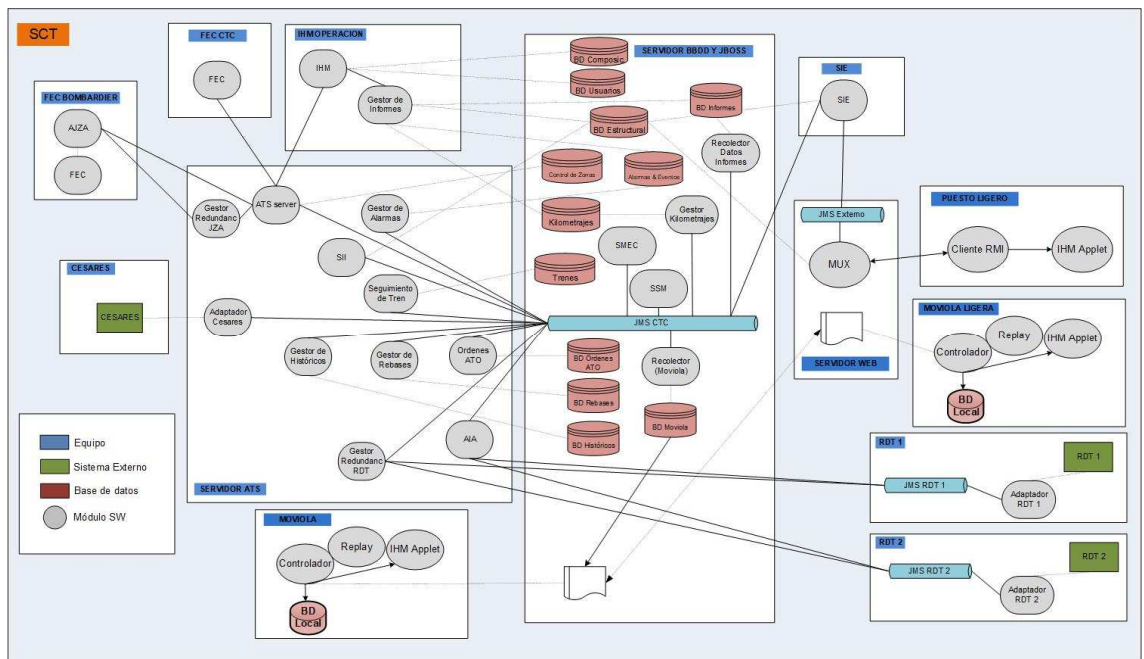
A La Sagrera existeix el STM1 on estan ubicats tots els equips tant servidor com llocs d'operació. Les CPU dels llocs d'operació estan situades en una sala diferent de la sala d'operació. Es disposen actualment de 18 llocs d'operació a monitoritzar. Per altra banda, a STM1 també estan instal·lats els servidors del sistema CTC: ctc_ls, bbdd_ls, sie_ls i FECs, en total 8 servidors.

A Sagrada Família, a la sala STM2 estan ubicats 7 llocs d'operació i la resta de servidors del sistema: ctc_sf, bbdd_sf, sie_sf i FECs_sf. En total són 8 servidors.

El sistema Telecomandament també integra electrònica de xarxa, que en el cas de STM1 són 4 switch Cisco i en el cas de STM2 són 2 switch més. També caldrà considerar l'electrònica de xarxa addicional (FW o altres) que puguin formar part del sistema.

Programari:

El sistema està compost de diversos elements de programari. L'arquitectura dels serveis que estan funcionant al telecomandament de trànsit és el següent:



Cadascun d'aquests processos està gestionat pel telecomandament, però no es disposa d'una eina que permeti la monitorització de l'estat d'aquests processos fora del mateix telecomandament.

Requeriments de l'eina:

1. Requeriments funcionals:

A. Monitorització telecomandament de trànsit:

L'eina de recollida de dades ha de ser compatible amb les següents fonts de dades:

- Monitorització maquinari servidors (HPE / DELL)
- Monitorització maquinari llocs operació del telecomandament de trànsit
- Monitorització maquinari ThinClient
- Monitorització sistema operatiu servidors:
 - o Compatible amb telecomandament de trànsit XC
 - o Compatible amb sistema operatiu Linux (altres futurs sistemes)
 - o Compatible amb sistema Windows Server (altres sistemes)
- Monitorització serveis telecomandament de trànsit (bases de dades, redundància, serveis telecomandament...)
- Monitorització serveis auxiliars telecomandament de trànsit
- Monitorització estat aplicació llocs d'operació telecomandament trànsit xc
- Monitorització estat aplicació thin client
- Alarmes i events del sistema telecomandament de trànsit
- Disponibilitat de dades d'operació del sistema: seguiment tren, estat ocupacions, estat senyals, agulles, ordres enviades, etc. segons disponibilitat

Com a mínim s'haurien de disposar de les següents informacions:

Detall de les monitoritzacions:

- Monitorització de hardware, com a mínim hauria de permetre monitoritzar:
 - o CPU
 - o Memòria
 - o Disc dur
 - o Alarmes maquinari (ventilador, font alimentació, etc.)

- Monitorització sistema operatiu:
 - o Alarmes i events del sistema operatiu
 - o Visualització versions i pedaços instal.lats
 - o Monitorització recursos consumits
 - o Disponibilitat visualització registres del propi sistema operatiu
 - o Altres

- Monitorització serveis bàsics del telecomandament:

- Estat serveis “core” del telecomandament
 - Estat redundàncies
- Monitorització alarmes basades en patrons ja predefinitos pel proveïdor del telecomandament, dels registres del telecomandament
- Monitorització aplicació dels llocs d’operació:
 - Monitorització estat del lloc d’operació
 - Visualització versions i pedaços instal·lats
 - Monitorització recursos consumits
 - Monitorització alarmes basades en patrons ja predefinitos pel proveïdor del telecomandament, dels registres del lloc d’operació
- Monitorització dades del telecomandament de trànsit:
 - Connexió alarmes telecomandament de trànsit
 - Connexió events telecomandament de trànsit
 - Connexió ordres telecomandament de trànsit

B. Monitorització comunicacions

L’eina de recollida de dades ha de ser compatible amb les següents fonts de dades:

- Monitorització equipament xarxa telecomandament de trànsit (Sagrera, Sagrada Família)
- Monitorització equipament de xarxa del transport de comunicacions amb elements de camp (RPSA, RPSB, sempre i quan sigui viable tècnicament la seva accessibilitat amb la configuració actual)

Com a mínim s’haurien de disposar de les següents informacions:

Detall de les monitoritzacions:

- Monitorització equipament xarxa telecomandament de trànsit:
 - Alarmes i events del maquinari
 - Alarmes i events del sistema operatiu de l’equipament de xarxa
 - Alarmes i events del sistema de comunicacions (enrutament o switching)
 - Disponibilitat de visualització de versió de maquinari programari carregada
- Monitorització equipament de xarxa del transport de comunicacions amb elements de camp:
 - Alarmes i events del maquinari
 - Alarmes i events del sistema operatiu de l’equipament de xarxa
 - Alarmes i events del sistema de comunicacions (enrutament o switching)
 - Disponibilitat de visualització de versió de maquinari programari carregada

2. Requeriments interfície amb usuari:

L'eina disposarà d'un front-end amb l'usuari per a visualitzar de forma gràfica les dades recollides.

La visualització de les dades ha de ser configurable pel propi usuari, disposant de l'eina per crear informes d'alarmes, events i determinats indicadors clau del sistema.

La visualització de les dades hauria de permetre noves alarmes, events o indicadors a partir de les dades rebudes. Aquestes noves alarmes s'haurien de poder configurar a nivell d'usuari, ja sigui amb condicions lògiques o matemàtiques (condicions lògiques, operadors lògics, operadors matemàtics, comptadors, etc.).

3. Requeriments de l'eina: Interfícies amb telecomandament de trànsit i altres sistemes

1. L'eina haurà de ser compatible amb tots els equips del telecomandament amb el que es vol integrar.
2. L'eina haurà de ser compatible amb els serveis de sistema operatiu i serveis de telecomandament amb què es vol integrar.

En cas que no fos compatible es proporcionarà l'alternativa adequada per a fer d'interfície amb qualsevol equipament o servei, sense que produeixi interferència en el correcte funcionament ni de l'equipament ni dels serveis que estan en funcionament.

3. L'eina haurà de permetre l'exportació de dades de la pròpia eina (ja siguin recollides i/o calculades).

Es requereix:

1. API exportació de dades:

API genèrica de consulta:

- a. Tipus: es disposarà d'API (API-REST) per a consultar dades per sistemes externs.
- b. Connexió:
 - i. La connexió es realitzarà des dels sistemes externs per a consultar dades
 - ii. Ha de permetre la gestió de les connexions remotes (login / connexió / desconnexió)
 - iii. Permetrà connexions segures
- c. Endpoint: Es definiran endpoints amb filtres actius. Un endpoint per cada tipologia d'actiu o dispositiu que gestiona el telecomandament: circuit de vies, agulles, senyals, lògica enclavament, etc. en funció de les dades disponibles. Es definiran filtres com a mínim per línia, enclavament, estació. D'aquesta forma amb instruccions de tipus get info i filtre es podrà accedir d'una forma fàcil al conjunt de dades que es requereixi.
Es disposarà de totes les dades des de l'última consulta. D'aquesta forma es podran recollir totes les dades tot i que hi hagi problemes de sincronització, per tant al recuperar comunicacions o sincronisme, s'obtidran totes les dades que s'hagin pogut emmagatzemar anteriorment.

Es crearan com a mínim dos API-REST de connexió de consulta: una per al sistema SmartMotors, i una altra quedarà disponible de forma genèrica.

Es sistema haurà de permetre disposar de més API-REST a partir de la genèrica, quan es considerin noves futures necessitats.

L'API haurà d'estar documentada de forma adequada per a que es pugui utilitzar. L'API disposarà d'algun mètode de proves per tal de confirmar el seu funcionament sense afectar al sistema en producció.

Es demana, com a mínim, de la disponibilitat de les següents dades a l'API-REST:

- Estats dels elements de camp: tots els elements que poden arribar des de camp. Ja siguin circuits de via, senyals, agulles, i altres elements del de l'enclavament.
- Dades estat Servei: stops
- Alarmes calculades pel telecomandament de trànsit:
 - Alarmes falsa ocupació
 - Alarmes depassament
 - Qualsevol altra alarma calculada pel sistema
- Ordres enviades pel telecomandament de trànsit, ja siguin ordres simples o automàtiques / ordres múltiples
- Estat i alarmes del propi telecomandament

2. Exportació de dades programades:

L'eina haurà de permetre configurar l'exportació de dades de forma programada.

Es podrà programar la data i hora de l'exportació o bé fer programacions per intervals horaris (ja sigui en segons, minuts, hores, dies, setmanes, etc.).

L'exportació de dades programades haurà de ser compatible amb algun tipus de fitxers que pugui admetre sistemes de tractament de dades tipus PowerBI o similars. Per exemple exportació de dades en fitxers o bases de dades estàndard.

La programació d'exportació haurà de permetre enviar dades ja siguin en brut (recol·leccions de dades) o bé dades ja calculades pel sistema de monitorització.

Altres tasques

Subministrament i instal·lació del maquinari a les instal·lacions de Metro de Barcelona (STM1). S'instal·laran els equips en els bastidors que indiqui Metro de Barcelona.

Subministrament i instal·lació del material de comunicacions necessari per la interconnexió de les fonts de dades amb el sistema de recollecció. Es subministrarà material de comunicacions (cablejat) així com l'equipament de xarxa, si fós necessari.

Subministrament i instal·lació de l'aplicació recol·lectora de dades de les fonts de dades al maquinari subministrat.

Requeriments ciberseguretat:

Els sistemes operacionals hauran de complir amb l'aplicació de les recomanacions recopilades a les Normatives: UNE-EN IEC 62443, EN 50701 i l'Esquema Nacional de Seguretat (ENS – CCN), segons nota tècnica NTIICC_014 REQUISITOS SEGURIDAD PARA SISTEMAS OPERACIONALES FMB.

L'arquitectura a definir haurà de basar-se en el model Purdue, que recull IEC62443 / TS50701, identificant totes les zones de seguretat i conductes, així com els mecanismes de seguretat a aplicar entre zones.

A priori, el nivell de seguretat sol·licitat pels sistemes operacionals de senyalització és SL3.

El proveïdor del servei haurà de realitzar un anàlisi de riscos detallat dels seus sistemes per determinar els nivells de seguretat objectiu (SL-T), els nivells de seguretat assolits (SL-A) i els nivells de seguretat de capacitat (SL-C) per a cada actiu i zona identificat, abans de traspasar els riscos residuals a TMB, segons nota tècnica NTIICC_011_MAPA DE RIESGOS OT+IICC_v2.

El sistema haurà de complir la política de ciberseguretat de Metro de Barcelona en l'àmbit dels sistemes operacionals (OT).

L'eina de monitorització s'instal·larà i comunicarà amb sistemes crítics de Metro de Barcelona, per tant l'eina haurà de disposar com a mínim el mateix nivell de seguretat exigida a l'eina a la qual s'ha de connectar en tots els seus àmbits.



NTIICC_014
REQUISITOS SEGURIDAD PARA SISTEMAS OPERACIONALES FMB



NTIICC_011_MAPA DE RIESGOS OT+IICC_v2



NTIICC_012_DESCRIPCION DE LOS CONCEPTOS DE SEGURIDAD

Els elements mínims a tenir present són:

- Gestió d'usuaris / Control accés
- Arquitectura del sistema: segmentació de xarxes i nivells seguint com a guia la norma IEC 62443
- Bastionat del sistema
- Disponibilitat d'implementar d'eines de detecció d'intrusió i codi maligne o connexió a una eina que faci aquestes funcions

- Registre / Auditoria de funcionament del sistema
- Disponibilitat del sistema: pla de contingència i continuïtat, recuperació del sistema

En el cas del bastionat del sistema, veure nota tècnica de bastionat per tenir present les característiques necessàries, segons ENS (Esquema Nacional de Seguretat):



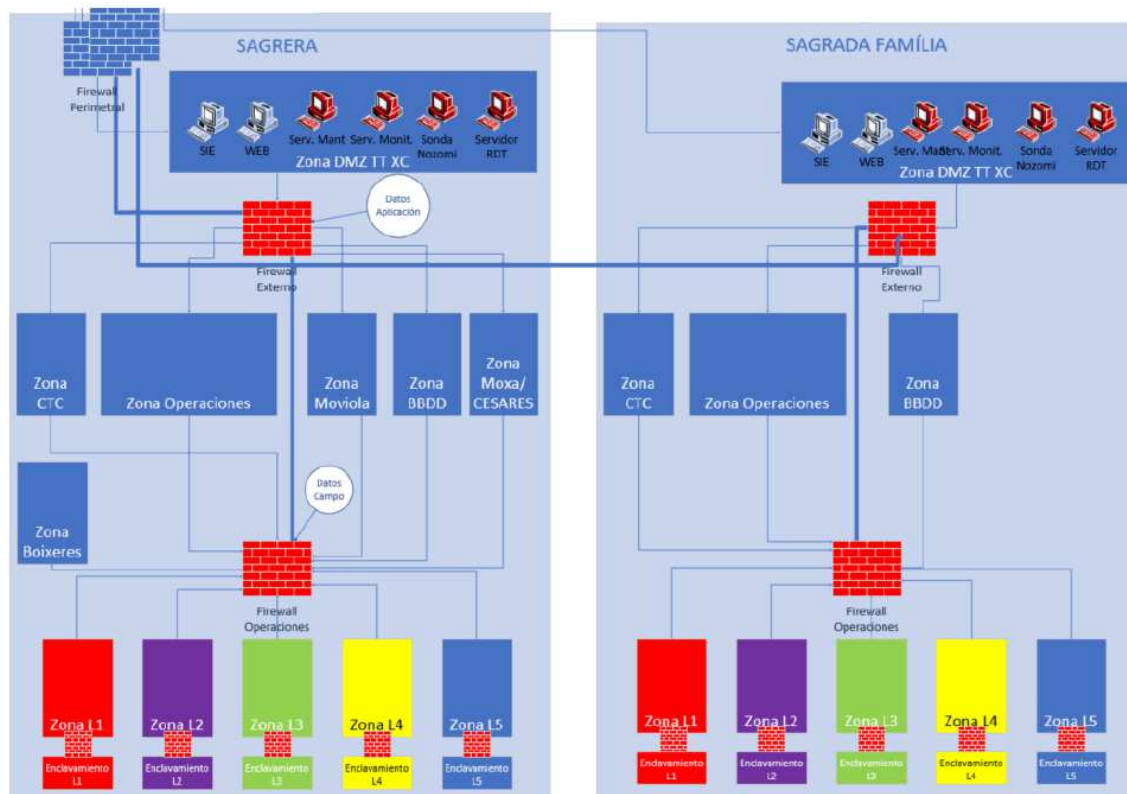
MEDIDAS MÍNIMAS
DE BASTIONADO PA

Arquitectura servei:

Es considera que telecomandament forma part del sistema senyalització.

En aquest escenari, es consideren que els nivells de seguretat segons norma 62443 són comuns per senyalització i telecomandament de trànsit.

Es defineix la següent arquitectura de nivells lògics:



El servei de monitorització hauria d'estar disponible a la zona DMZ TT XC, per a que pugui ser accessible des de l'exterior complint els requeriments de la norma 62443.

Aquesta arquitectura mostra uns elements de seguretat (Firewall) que a dia d'avui no estan instal·lats, que permeten l'aïllament entre les zones d'operació i comunicacions i de camp. Aquests equips queden fora de l'àmbit d'aquest projecte.