



ATL

Ens d'Abastament
d'Aigua Ter-Llobregat

1.10 DISSENY TÈCNIC DEL SCADA

26.02.2025

1.10 Disseny tècnic del SCADA

Índex de continguts

1.	Introducció	3
2.	Característiques generals	4
3.	Alta disponibilitat	5
3.1.	Redundància de components SCADA	7
3.2.	Redundància de Base de Dades	7
3.3.	Procediments de Recuperació davant Desastres (<i>Disaster Recovery</i>)	7
4.	Controladors i components d'adquisició	8
5.	Accés centralitzat a visualitzadors	8
6.	Intercanvi d'informació amb tercers	9

Llista de figures

Figura 3-1: Arquitectura SCADA.	6
Figura 5-1: Accés a visualitzadors.....	8

1.10 Disseny tècnic del SCADA

1. INTRODUCCIÓ

El present document descriu les necessitats d'arquitectura del nou SCADA, el qual substituirà l'SCADA d'ATL actualment en operació. Aquest document té com a objectiu la definició dels requisits d'arquitectura per a implantar un sistema SCADA robust i d'alta disponibilitat, permetent l'operativitat davant de fallades, així com durant les tasques de manteniment de hardware sobre el que es s'executin els components software.

1.10 Disseny tècnic del SCADA

2. CARACTERÍSTIQUES GENERALS

A continuació s'indiquen aquelles característiques que s'han d'assolir en el disseny de l'arquitectura del sistema SCADA:

- a. El sistema de telecontrol consta de quatre centres productius:
 - Tres estacions de tractament d'aigua potable (ETAP del Ter, ETAP del Llobregat i ETAP del Cardener)
 - Xarxa d'abastament amb un conjunt de aproximadament 300 estacions remotes repartides arreu del territori català (Fontsanta).
- b. El sistema complet serà capaç de gestionar al voltant de 500.000 senyals analògics i digitals, tant de lectura com d'escriptura.
- c. La infraestructura d'ATL consta d'un CPD a cadascun dels centres productius (ETAP del Ter, ETAP del Llobregat, ETAP del Cardener i estacions remotes).
- d. Tot el sistema estarà virtualitzat i redundat en màquines físiques situades als CPDs d'ATL. Tot i així, no es descarta la possibilitat que tot o part del sistema es pugui integrar en algun servei del núvol, ja sigui l'entorn principal o el redundat.
- e. Quan sigui possible i si les xarxes d'interconnexió entre centres ho permeten, cada centre productiu disposarà d'un sistema redundat situat en un altre centre productiu. D'aquesta forma en cas de pèrdua del sistema principal d'un centre productiu, aquest podrà ser gestionat des d'un altre centre productiu.
- f. Cadascun dels centres serà gestionat per un sistema SCADA autònom, assegurant l'operativitat local de cadascun del centre i evitant la dependència amb un sistema central. Tot i així, tots els centres seran visibles entre ells, permetent l'operativitat remota de tots els centres des de qualsevol altre centre.
- g. Els usuaris, a més de poder connectar-se directament als visualitzadors web de cada centre productiu, també han de poder connectar-se als visualitzadors de tots els centres productius de forma centralitzada.
- h. Cada centre disposarà d'un sistema de preproducció que permeti desenvolupar àgilment qualsevol modificació i corregir errades del sistema desplegat a producció (ja siguin sinòtics, estructures d'objectes, codis alternatius, etc.), per tal de validar-los prèviament al desplegament al sistema productiu.

1.10 Disseny tècnic del SCADA

- i. El sistema disposarà d'un registre d'auditoria en el que s'enregistrin tots els accessos i accions realitzades per els usuaris. Aquest registre constarà almenys dels següents camps:
 - a. Data i hora de l'event.
 - b. Usuari que ha provocat l'event.
 - c. Acció realitzada.
 - d. Valor introduït. Aquest només serà necessari en cas de canvi de propietats de paràmetres o escriptures d'ordres.
- j. El sistema disposarà d'un sistema o procediments de control de versions i gestió dels canvis que permeti mantenir la traçabilitat de les millores introduïdes al llarg del temps i amb la possibilitat de posar en producció versions anteriors en cas de detectar un estat inconsistent o degradació del sistema a partir de determinat moment.

3. ALTA DISPONIBILITAT

El sistema SCADA es essencial per a la monitorització, control i gestió de processos en temps real. L'alta disponibilitat i la redundància són components crítics per assegurar l'operativitat continua del sistema SCADA, inclús davant de fallades de hardware o software. En un entorn com el d'ATL, qualsevol interrupció del sistema SCADA pot resultar en pèrdua d'informació i la impossibilitat de gestionar i controlar els actius dels centres productius.

L'arquitectura d'alta disponibilitat del sistema SCADA ha de permetre l'operativitat sense interrupcions davant de situacions com les que s'indiquen a continuació:

- Fallades de comunicacions entre components.
- Aturada de components del sistema degut a tasques subjectes a treballs de manteniment.
- No disponibilitat de servidors durant tasques de manteniment del hardware o sistema base (sistema operatiu, antivirus, etc.)

Per tant, tots els component crítics involucrats en l'adquisició i emmagatzematge de la informació estaran redundats, assegurant la disponibilitat i l'accés a la informació davant de les situacions esmentades anteriorment.

Idealment, els components redundats es desplegaran en un centre productiu alternatiu. D'aquesta manera, en cas de fallada de la infraestructura principal d'un centre productiu, aquest podria ser operat i gestionat des de la resta de centres productius.

1.10 Disseny tècnic del SCADA

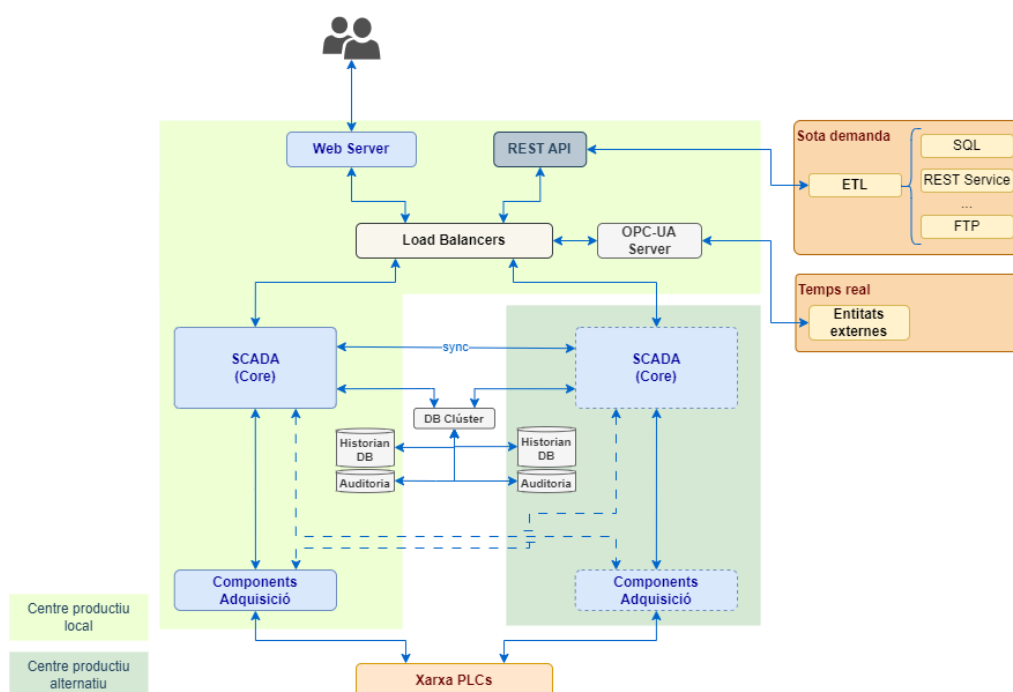


Figura 3-1: Arquitectura SCADA.

Una arquitectura redundante implicará la implementación de componentes adicionales al sistema SCADA para asegurar que, en caso de falla de un componente crítico, el sistema siga capaz de continuar funcionando sin interrupciones y de forma transparente a los usuarios. Es decir, la estrategia de redundancia se implementará de manera que actúe de forma automática minimizando al máximo o evitando la ejecución de procedimientos manuales.

El diseño de la arquitectura de alta disponibilidad ha de prever las siguientes acciones:

- **Avaluació de riscos i anàlisi d'impacte:** Avaluar els riscos potencials per al sistema SCADA y realitzar un anàlisi d'impacte en caso de fallades. Aquest anàlisi ajudarà a prioritzar les àrees crítiques que han de tenir major nivell de redundància i disponibilitat.
- **Proves regulars de commutació per error:** Realitzar simulacions periòdiques i de forma controlada de fallades per a verificar l'eficiència del sistema de *failover* i garantir que el sistema es capaç de recuperar-se ràpidament sense interrompre les operacions.
- **Manteniment i actualització de components:** Implementar un pla de manteniment preventiu per a tots els components del sistema SCADA. Això inclou actualitzacions de software, reemplaçament de hardware i millores de seguretat.

1.10 Disseny tècnic del SCADA

- **Documentació actualitzada:** Mantenir una documentació detallada sobre la configuració del sistema, l'arquitectura redundant, procediments de commutació per error i els plans de recuperació. Això és vital para una respuesta rápida y eficiente en situaciones críticas.

3.1. Redundància de components SCADA

Els servidors SCADA son els responsables de processar la informació rebuda dels equips de camp i centres productius i proporcionar les interfícies d'usuari per a la gestió i control del sistema.

L'alta disponibilitat s'implementarà amb els component crítics redundats, una instància actuant com a component principal i una instància secundària que prendrà el control en cas de fallida de la instància principal. En cas de fallada de la instància principal o del hardware sobre el que s'executa, la instància secundària prendrà el control sense causar interrupcions. Aquesta configuració es coneix com a commutació per error o *failover*.

3.2. Redundància de Base de Dades

La base de dades o sistema historian és un component crític d'un sistema SCADA, ja que emmagatzema i gestiona tota la informació històrica de supervisió i control. La redundància de la base de dades pot implementar-se mitjançant:

- **Bases de dades en clúster:** Configuració de bases de dades d'alta disponibilitat, on la informació es replica entre servidors. En cas de fallida del servidor principal, el servidor secundari pot assumir el rol d'aquest de forma transparent per als usuaris i components del sistema SCADA.
- **Replicació d'informació:** Implementació d'una replicació contínua de la base de dades entre servidors, assegurant que sempre existeixi una còpia actualitzada de la informació en una ubicació alternativa.

3.3. Procediments de Recuperació davant Desastres (*Disaster Recovery*)

La planificació per a la recuperació davant desastres es un component vital de l'estratègia d'alta disponibilitat. Aquesta pràctica inclou:

- **Còpies de seguretat regulars:** Realitzar còpies de seguretat regulars de configuracions i bases de dades. Aquestes còpies es deuen emmagatzemar en ubicacions físiques externes a la infraestructura principal del sistema SCADA per a evitar la pèrdua d'informació en cas de desastre. Alternativament, les còpies de seguretat poden ser emmagatzemades al núvol.

1.10 Disseny tècnic del SCADA

- **Plans de recuperació:** Establir procediments detallats per a la recuperació del sistema en cas de desastre. Aquests plans o procediments han de provar-se regularment per assegurar que el temps d'inactivitat es minimitza al màxim.

4. CONTROLADORS I COMPONENTS D'ADQUISICIÓ

Els controladors són els components encarregats d'establir i gestionar les comunicacions de temps real amb els PLCs Allen-Bradley i altres tipus d'equips remots. Aquests components actuen com a interfície entre l'SCADA i els dispositius de camp.

El controladors de comunicacions permetran l'adquisició de dades tant dels equips Rockwell de la xarxa dels PLC actuals d'ATL com d'altres dispositius basats amb protocols estàndard en l'àmbit del telecontrol, com poden ser DNP3, IEC60870, MQTT, OPC DA/UA, etc.

A més, el sistema d'adquisició inclourà funcionalitats de *Store & Forward*. D'aquesta forma, en cas de pèrdua de comunicació entre components d'adquisició i el SCADA, la informació podrà ser recuperada un cop restablerta la connexió.

5. ACCÉS CENTRALITZAT A VISUALITZADORS

Un accés web centralitzat permetrà gestionar i controlar els actius de tots els centres productius des d'un accés únic. Aquesta solució facilita la gestió d'actius i visualització de sinòtics de tota la xarxa d'ATL des d'un únic punt d'entrada.

Per altra banda, l'accés directe a cada servidor web permetrà un accés a un centre productiu en concret. Aquest tipus d'accés serà necessari en cas d'indisponibilitat de l'accés centralitzat o en casos en els que es produeix un pèrdua de connectivitat entre un centre productiu i l'accés centralitzat.

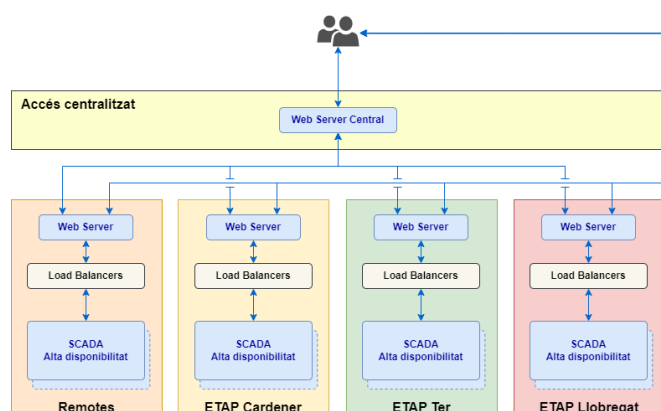


Figura 5-1: Accés a visualitzadors.

1.10 Disseny tècnic del SCADA

6. INTERCANVI D'INFORMACIÓ AMB TERCERS

El sistema SCADA permetrà l'intercanvi d'informació tant amb entitats externes com amb eines corporatives d'ATL.

En l'àmbit del intercanvi d'informació amb tercers es poden distingir les següents tipologies:

- **Publicació d'informació sota demanda:** Destinat a la consulta d'informació des de components o eines externes al SCADA a petició. Idealment aquest tipus de consulta hauria d'implementar-se mitjançant APIs REST. En cap cas es permetrà l'accés directe a la informació emmagatzemada al SCADA.
- **Publicació d'informació en temps real:** Destinat a la publicació d'informació a entitats externes que així ho requereixin. Actualment, aquest tipus de publicació es realitza mitjançant connexions OPC UA degudament protegides amb restricció d'accés exclusivament a la informació necessària.
- **Integració de dades amb processos *batch*:** Integració de dades històriques des de serveis corporatius d'ATL que s'executa amb una freqüència regular. En l'actualitat aquest tipus d'integració es realitza mitjançant eines d'ETL.
- **Integració de dades en temps real:** Destinat a la integració d'informació de temps real des d'entitats externes, actualment aquest tipus de publicació es realitza mitjançant connexions OPC UA degudament protegides.

En tots el casos, tant la integració com la consulta d'informació es realitzarà mitjançant l'ús de canals segurs com HTTPS o altres protocols basats en certificats TLS 1.2 o superiors. A més, es restringirà l'accés a la informació mitjançant credencials d'usuari o altre tipus de sistema que assegurí l'accés segur a la informació.