



ATL

Ens d'Abastament
d'Aigua Ter-Llobregat

1.11 DISSENY FUNCIONAL DE L'SCADA

11.02.2025

1.11 Disseny funcional de l'SCADA

Índex de continguts

1.	Introducció	3
2.	Identificació dels requisits funcionals de l'SCADA	4
3.	Identificació de requisits d'adaptació de dispositius de camp	10

Llista de taules

Taula 2-1: Requisits de l'SCADA	9
Taula 3-1: Requisits dels PLC i HMI	11

1.11 Disseny funcional de l'SCADA

1. INTRODUCCIÓ

El present document descriu l'especificació funcional del nou SCADA, el qual substituirà l'SCADA d'ATL actualment en operació. Aquest document té com a objectiu la definició del disseny funcional atenent a criteris d'usabilitat, seguretat, flexibilitat, coherència, facilitat de manteniment i robustesa, que garanteixin una gestió eficient i fiable de la xarxa d'abastament.

L'evolució de les necessitats operatives, juntament amb l'obsolescència tecnològica del sistema actual, han impulsat la definició d'una nova aproximació a la gestió, operació i manteniment de la xarxa d'abastament amb tecnologies modernes de telecontrol. Aquest nou sistema no només millorarà la supervisió i el control dels actius distribuïts, sinó que també permetrà la integració amb tecnologies emergents, el compliment de normatives i estàndards vigents i l'optimització del rendiment operacional.

En aquest document s'estableixen els requisits funcionals clau que definiran l'abast i les capacitats del sistema i posa en relació els diferents documents en què s'estableixen els aspectes particulars relatius a la implementació de la funcionalitat prevista per als diferents components, tals com la gestió d'alarmes, la gestió de la seguretat de la informació, l'arquitectura tècnica, la interoperabilitat amb altres sistemes o l'experiència d'usuari. El contingut del document servirà com a base per al desenvolupament, implementació i validació de la nova solució SCADA, promovent la seva alineació amb els objectius estratègics de l'organització.

1.11 Disseny funcional de l'SCADA

2. IDENTIFICACIÓ DELS REQUISITS FUNCIONALS DE L'SCADA

En aquest capítol es detallen els requisits funcionals del nou sistema SCADA, organitzats en categories segons el seu àmbit d'aplicació. Aquesta estructura permet una visió clara i ordenada de les capacitats esperades del sistema i facilita la seva anàlisi i validació.

A continuació es llisten altres fonts de requisits d'elements específics que han estat incorporats a la taula de requisits d'SCADA que s'inclou a continuació bé per la seva especificitat o bé perquè constitueixen elements perifèrics no inclosos directament a l'SCADA:

- Els requisits de hardware dels dispositius de camp es troben als documents 1.1 – Grau d'automatització en funció del nivell de servei i 1.2 – Directrius tecnològiques i metodologies de migració.
- Els requisits relatius als objectes de l'SCADA es desenvolupen al document 1.3 – Llibreria d'objectes i a les fitxes corresponents.
- Els requisits relatius a les interfícies d'intercanvi de dades mitjançant API REST i OPC UA es troben al document 1.4 – Racionalització de dades.
- Els requisits relatius a les comunicacions i els protocols de comunicació amb els autòmats es troben al document 1.5 – Disseny tècnic de les comunicacions.
- Els requisits específics del sistema d'alarmes es troben al document 1.6 – Tractament d'alarmes.
- Els requisits relatius a la seguretat de la informació es troben al document 1.7 – Directrius de seguretat.
- Els requisits específics de la implementació d'interfícies HMI es troben al document 1.9 – Definició d'interfícies d'usuari.
- Els requisits relatius al marc de treball i l'assegurament de la qualitat es troben al document 1.12 – Qualitat i marc de treball.

Malgrat la distribució dels requisits entre els documents esmentats prèviament, se n'han extret aquells específicament relacionats amb l'SCADA o aquells que tenen una rellevància singular per a l'operació i manteniment de les instal·lacions d'ATL. La taula presentada a continuació els incorpora agrupats per categoria. No obstant això, qualsevol implementació es farà en concordança amb els documents esmentats en el llistat anterior.

ID	Requisit	Categoria
AL001	El sistema de gestió d'alarmes permet, de manera directa, assignar prioritats, tipus i classe a cada alarma, amb un mínim de cinc nivells de prioritat.	Alarmes
AL002	El sistema d'alarmes permet reconèixer, tant en condicions de reconeixement manual com automàtic, múltiples alarmes de manera simultània.	Alarmes

1.11 Disseny funcional de l'SCADA

AL003	El visor d'alarmes actuals i històriques permet filtrar per totes les columnes disponibles mitjançant text lliure i selectors, incloent-hi-hi alarma, descripció, prioritat i classe.	Alarmes
AL004	És possible extreure un informe, de manera directa i automàtica, de les alarmes per a les quals s'ha habilitat la notificació sonora.	Alarmes
AL005	En pulsar sobre una alarma en el llistat d'alarmes actuals, es mostra la pantalla corresponent, ressaltant l'equip afectat.	Alarmes
AL006	És possible generar, de manera directa i automàtica, un informe detallat amb informació sobre les alarmes inhabilitades, l'usuari que les va inhabilitar, la data i el motiu.	Alarmes
AL007	L'SCADA disposa de pantalles de gestió d'històrics d'alarma i de gestió d'alarmes actuals.	Alarmes
AL008	El sistema d'àudio genera senyals acústics adequats per a alarmes.	Alarmes
AL009	L'associació d'una alarma a un senyal acústic és configurable.	Alarmes
AL010	L'SCADA permet configurar l'autoreconeixement per a cada alarma de forma independent.	Alarmes
AR001	L'SCADA permet la creació d'objectes imbricats (<i>nested</i>) tant a l'entorn gràfic com en el model de dades.	Arquitectura
AR002	La modificació d'una plantilla d'objecte es propaga automàticament a totes les instàncies que en depenen o que se'n deriven.	Arquitectura
AR003	L'SCADA és instal·lable en entorns virtualitzats.	Arquitectura
AR004	Els frontals de comunicació externs són redundants, en el cas d'existir, amb almenys una instància addicional.	Arquitectura
AR005	L'SCADA té un sistema de redundància complet, incloent-hi-hi el servidor de llicències.	Arquitectura
AR006	Els clients SCADA poden desplegar-se en HMI locals (panells de camp), de manera que els canvis realitzats al servidor SCADA estiguin sempre disponibles als HMI locals sense necessitat d'accions addicionals. En cas de pèrdua de les comunicacions amb el servidor SCADA, els clients locals (o clients alternatius activats automàticament) continuen funcionant de manera autònoma. Quan es restableixen les comunicacions, els clients SCADA recuperen automàticament el seu funcionament normal (connexió amb el servidor SCADA) i sincronitzen amb el servidor SCADA totes les dades emmagatzemades durant el període de desconnexió.	Arquitectura
AU001	L'SCADA compta amb un sistema d'auditoria de canvis.	Auditoria
AU002	El sistema d'auditoria implementat monitoritza accions i esdeveniments de l'entorn d'execució i disseny, amb possibilitat de recerca per múltiples camps, com ara data i hora, usuari, tipus de comandament o esdeveniment, objecte afectat, entre d'altres.	Auditoria
AU003	El sistema d'auditoria és capaç d'integrar altres sistemes d'auditoria, com els de l'HMI o PLC.	Auditoria
AU004	Tots els canvis relatius als còmputos de variables calculades queden registrats en els informes d'auditoria.	Auditoria
CO001	L'intercanvi de dades amb les estacions està optimitzat per prioritzar les dades requerides per l'operador, de manera que la comunicació de les dades involucrades en les operacions executades per l'usuari es prioritzen per minimitzar els temps d'espera.	Comunicacions
CO002	L'SCADA permet connexió directa i segura amb els PLC d'ATL sense necessitat de recórrer a frontals de comunicació (com els actuals KepServerEx).	Comunicacions
CO003	Es poden inhibir els intercanvis de dades amb els PLC per a cada variable de manera independent.	Comunicacions

1.11 Disseny funcional de l'SCADA

CO004	L'SCADA ofereix una interfície de diagnòstic de la comunicació amb les estacions mitjançant l'enviament de paquets ICMP (ping).	Comunicacions
DA001	L'SCADA inclou, de sèrie o a través d'integracions incloses en el subministrament, funcionalitats d'analítica avançada per a la realització de càlculs estadístics, correlacions, prediccions i còmputos similars.	Dades y anàlisi
DA002	Cada variable de l'SCADA té un valor de qualitat configurable.	Dades y anàlisi
DA003	L'origen de la dada de qualitat és configurable.	Dades y anàlisi
DA004	Es pot indicar el responsable del procés o pantalla en forma de metadada.	Dades y anàlisi
DA005	L'SCADA compta amb un sistema de recuperació d'històrics a partir de dades emmagatzemades en estacions remotes durant episodis de fallada de les comunicacions.	Dades y anàlisi
ES001	Totes les pantalles de l'SCADA s'adeqüen a l'estàndard ANSI/ISA-101.01-2015 o versions posteriors.	Estàndards
ES002	Tot el sistema de gestió d'alarmes està dissenyat conforme a l'estàndard ANSI/ISA-18.2-2016 o versions posteriors.	Estàndards
GR001	El sistema de gestió de gràfiques permet la inclusió de qualsevol variable historitzada mitjançant el mecanisme d'arrossegar i soltar o un altre mètode senzill.	Gràfiques
GR002	El sistema de gestió de gràfiques manté en memòria la darrera configuració realitzada i permet emmagatzemar diferents configuracions per carregar-les posteriorment. Això inclou, per exemple, elements com els colors assignats a les diferents corbes, els límits dels eixos, el nombre d'eixos, els cursors, etc.	Gràfiques
GR003	L'SCADA permet l'emmagatzematge de diferents configuracions del sistema de gestió de gràfiques i la seva recuperació sota demanda.	Gràfiques
GR004	Les gràfiques delimiten clarament els valors de monitoratge de senyals analògics segons l'estàndard ANSI/ISA-101.01-2015 o versions posteriors.	Gràfiques
HI001	Es pot seleccionar si els canvis en els còmputos associats a variables calculades afecten o no les dades històriques.	Històrics
HI002	El sistema permet reconstruir automàticament l'estat passat del procés mitjançant una barra de desplaçament temporal sense afectar de cap manera el procés actual, mostrant l'estat dels objectes i les dades associades en el moment històric seleccionat, essent possible retornar a l'instant present en qualsevol moment.	Històrics
IF001	És possible realitzar l'exportació de fitxers d'auditoria de manera senzilla i directa, de forma tant manual com automàtica, en formats comuns, PDF i CSV com a mínim.	Informes
IF002	És possible realitzar l'exportació d'alarmes actuals i històriques de manera senzilla i directa, de forma tant manual com automàtica, en formats comuns, PDF i CSV com a mínim.	Informes
IF003	És possible exportar les gràfiques de manera senzilla i directa, de forma tant manual com automàtica, en diferents formats, XLSX com a mínim.	Informes
IF004	Tots els informes poden ser configurats per almenys un rol amb permisos adequats a través d'una interfície amigable.	Informes
IF005	Es permet l'exportació senzilla i directa, tant manual com automàtica, de dades actuals i històriques, incloent-hi dades calculades i metadades.	Informes
IF006	És possible generar, de manera senzilla i directa, tant de forma automàtica com manual, informes de la situació actual del procés, així com de condicions històriques.	Informes
IF007	L'SCADA permet la creació, per part de l'usuari, d'informes i <i>dashboards</i> personalitzats, els quals mostren la informació referenciada en temps real sense necessitat d'exportar-los a fitxers externs (PDF o similars).	Informes

1.11 Disseny funcional de l'SCADA

IF008	L'SCADA permet a l'usuari compartir els seus informes i <i>dashboards</i> personalitzats amb altres usuaris de l'SCADA.	Informes
IN001	L'SCADA inclou un component que permet la visualització de vídeos obtinguts de càmeres de monitoratge remotes.	Integració
IN002	Cada pantalla permet accedir a un pop-up amb vincles a documentació o aplicacions externes, amb un mínim de 10 vincles.	Integració
IN003	L'SCADA permet la introducció i extracció de dades a través d'interfícies normalitzades (API REST i OPC UA) de manera controlada.	Integració
IN004	L'SCADA permet configurar quines dades són accessibles a través de l'API REST i OPC UA, així com assignar permisos adequats (lectura i/o escriptura) als usuaris sobre aquestes dades.	Integració
IN005	Les escriptures de dades que es realitzin a través de l'API REST o OPC UA han de ser registrades en un històric accessible i auditable per un usuari amb el rol corresponent. Si aquesta escriptura implica un enviament de d'ordres o dades cap a un equip remot (com pot ser un PLC), l'usuari de l'SCADA ha de poder veure aquesta informació a la pantalla de nivell corresponent.	Integració
IN006	L'SCADA s'integra amb els GMAO GIM i/o EasyVista i és possible generar ordres de treball des del propi SCADA.	Integració
IN007	L'SCADA incorpora un connector GIS per a la representació d'informació georeferenciada.	Integració
IN008	Els identificadors de base de dades SCADA són independents dels del GMAO, però aquests últims s'emmagatzemen com a metadades modificables per usuaris amb permisos adequats.	Integració
IN009	És possible incrustar pàgines web a les pantalles.	Integració
NA001	Es pot configurar un botó del ratolí per agilitzar la navegació a la pantalla anterior amb una única pulsació.	Navegació
NA002	La pantalla de nivell 2 mostra les estacions de forma esquemàtica, mentre que la pantalla de nivell 1 les presenta georeferenciades sobre un mapa.	Navegació
NA003	La pantalla de nivell 1 mostra un <i>tooltip</i> sobre cada estació amb, almenys, el nom d'estació.	Navegació
NA004	La navegació està optimitzada per minimitzar el nombre de pulsacions de ratolí necessàries.	Navegació
NA005	L'SCADA permet la recerca d'elements per <i>tag</i> i nom, obrint la pantalla corresponent al nivell configurat en seleccionar l'element trobat.	Navegació
NA006	La pantalla de nivell 1 proporciona una visió general de la instal·lació i els principals indicadors sense funcions de control.	Navegació
NA007	La pantalla de nivell 2 permet realitzar operacions rutinàries.	Navegació
NA008	La pantalla de nivell 3 permet realitzar accions no rutinàries.	Navegació
NA009	La pantalla de nivell 4 permet realitzar diagnòstics, manteniment i modificacions avançades.	Navegació
NO001	L'SCADA inclou un registre o sistema de missatgeria interna que facilita la comunicació entre els usuaris de l'SCADA, especialment entre torns. Concretament, existeix un sistema de missatgeria a diferents nivells: un nivell general, un nivell d'estació i, finalment, un nivell d'objecte, de manera que es pot accedir als missatges generals des de la pantalla de nivell 1, als missatges d'estació des de la pantalla de nivell 3 i als missatges d'objecte en pulsar sobre aquest.	Notificacions
NO002	És possible enviar notificacions per correu electrònic i Microsoft Teams. Aquestes notificacions poden estar relacionades amb alarmes del sistema, notificacions manuals o altres esdeveniments registrables.	Notificacions

1.11 Disseny funcional de l'SCADA

NO003	Es permet l'emissió de notificacions tipus <i>broadcasting</i> en <i>banners</i> d'alerta amb diferents nivells de granularitat: tots els centres de control, un centre de control concret o una estació concreta.	Notificacions
NO004	El sistema de notificacions permet enviaments massius amb nivells de granularitat de destinataris diferents (estacions, rols, usuaris, notificacions generals, etc.).	Notificacions
OP001	L'enviament d'ordres permet establir condicions o restriccions a la seva aplicació.	Operació segura
OP002	Es poden inhibir alarmes d'equips en manteniment.	Operació segura
OP003	És possible escriure manualment el valor de les variables les comunicacions amb el PLC de les quals es trobin inhibides (mode de simulació en SCADA).	Operació segura
RE001	L'SCADA garanteix un temps de resposta òptim sense demores significatives en la presentació de dades, generació d'informes o canvi de pantalles, amb un temps inferiors a 1 segon a les pantalles associades a dades actuals i 3 segons en pantalles associades a dades històriques.	Rendiment
RE002	Es pot limitar el nombre de peticions per usuari i grup en les interfícies API REST i OPC UA.	Rendiment
RE003	L'SCADA està dissenyat per a les configuracions existents, incloent-hi els <i>videowalls</i> .	Rendiment
RE004	Es pot limitar el nombre de connexions i ample de banda pel que fa a l'ús de les interfícies API REST i OPC UA.	Rendiment
SE001	El sistema permet la creació de rols d'usuari amb permisos granulars (com a mínim, els següents rols: administrador, supervisor de manteniment, supervisor d'operació, operador i visualitzador). A tall il·lustratiu, per a cada rol és possible determinar si l'usuari pot modificar consignes, assignar notificacions d'àudio a alarmes, executar ordres, generar informes, accedir a determinades pantalles, canviar paràmetres de configuració avançats, etc.	Seguretat
SE002	La sessió de l'SCADA es tanca automàticament després d'un període d'inactivitat.	Seguretat
SE003	Es permet l'habilitació de doble autenticació per a determinats usuaris.	Seguretat
SE004	Les dades associades als objectes es poden modificar segons els permisos assignats.	Seguretat
SE005	Els intercanvis de dades a través de les interfícies API REST i OPC UA són segurs, amb autenticació i xifrat de la informació.	Seguretat
SE006	Les connexions ODBC es poden restringir sota demanda.	Seguretat
SE007	Es pot restringir l'accés a dades i la quantitat consultable a través de les interfícies API REST i OPC UA.	Seguretat
SE008	El nivell de granularitat més fi de l'accés a les interfícies API REST i OPC UA és l'usuari.	Seguretat
SE009	La base de dades es pot independitzar de les altres bases de dades internes de l'SCADA per permetre l'intercanvi de dades amb usuaris externs mitjançant les interfícies API REST i OPC UA.	Seguretat
SE010	Els usuaris amb permisos adequats poden modificar operacions de variables calculades.	Seguretat
SE011	L'SCADA s'integra amb Active Directory i altres solucions de gestió d'accés i identitat.	Seguretat
SV001	L'SCADA compta amb un servei de suport directe del fabricant inclòs en el subministrament.	Serveis
US001	L'SCADA permet l'automatització d'accions recurrents mitjançant un sistema similar a macros.	Usabilitat
US002	El contingut de les pantalles és adaptable a cada usuari de manera programàtica.	Usabilitat

1.11 Disseny funcional de l'SCADA

US003	Es poden obrir múltiples finestres pop-up simultàniament i moure-les lliurement.	Usabilitat
US004	Els informes es poden generar des de la pantalla de l'estació sense accedir a una pantalla específica de gestió d'informes.	Usabilitat
MQ001	Un usuari, amb els permisos adients i sense necessitat de coneixement tècnic del sistema, ha de poder realitzar el canvi corresponents a les modificacions esmentades al document 1.12 a través d'una eina web interactiva, o el propi SCADA, que li proveeixi el suport durant el procés i que registri tots els canvis realitzats pel propi usuari.	Marc de Qualitat
MQ002	Els atributs d'elements de les bases de dades d'SCADA que es mostren per pantalla han de tenir designat un control d'edició. Un usuari amb un permís d'edició ha de poder fer la modificació corresponent i que el sistema deixi constància del canvi i l'usuari que ha realitzat la modificació. Un exemple clar és el canvi d'una descripció d'un element. Aquest canvi han de ser propagats al PLC o HMI, si la informació també fos visualitzada o utilitzada per algun d'aquests elements.	Marc de Qualitat

Taula 2-1: Requisits de l'SCADA

1.11 Disseny funcional de l'SCADA

3. IDENTIFICACIÓ DE REQUISITS D'ADAPTACIÓ DE DISPOSITIUS DE CAMP

Com a conseqüència de l'adaptació de l'SCADA, s'ha identificat un conjunt de requisits que afecten als dispositius de camp i que no han estat encara incorporats a les plantilles de disseny. Per tal de centralitzar en un únic document tots els requisits funcionals que afecten el sistema de control i directa o indirectament l'SCADA, s'ha incorporat la taula següent amb identificació del tipus de dispositius afectats. No obstant això, qualsevol implementació es farà en concordança amb els documents llistats a continuació:

- Requisits específics de la implementació de la configuració i programació dels PLC, detallats al document 1.8 – Configuració d'autòmats i definició de programació.
- Requisits específics de la implementació d'interfícies HMI, detallats al document 1.9 – Definició d'interfícies d'usuari.

ID	Requisit	Dispositiu
PL001	Propagació l'activació de determinades alarmes cap a un sistema de notificació sonora configurable per l'operador amb els permisos adequats (requereix modificació de hardware).	PLC
PL002	Integració de la base de dades d'auditoria del PLC amb la base de dades de l'SCADA, incloent-hi la informació enregistrada al software AssetCentre.	PLC
PL003	Exportació de la base de dades d'auditoria del PLC a un format comú (com a mínim, CSV).	PLC
PL004	Modificació de les rutines d'escalat dels autòmats per tal de permetre'n l'adaptació des de l'HMI o SCADA.	PLC
PL005	L'identificador d'ATL d'un equip ha de poder ser modificable per un usuari amb el privilegis corresponents a través de l'SCADA del Centre de Control i propagat al PLC.	PLC
PL006	Ha de ser compatible amb la taula d'intercanvi de l'anterior sistema o incloure un mecanisme que permeti commutar l'intercanvi d'informació amb el sistema antic o el sistema nou. ¹	PLC
PL007	La gestió de la comunicació Tetra que contenen els programes de PLC de l'antic codi de programa ha de mantenir-se	PLC
HM001	Incorporació d'una pantalla de modificació de l'escalat dels senyals analògics a l'HMI.	HMI
HM002	A la planta de Cardener, visualització de qualsevol part de la planta des de qualsevol HMI de la instal·lació.	HMI
HM003	Integració de la base de dades d'auditoria de l'HMI amb la base de dades de l'SCADA, incloent-hi la informació enregistrada al software AssetCentre.	HMI
HM004	Exportació de la base de dades d'auditoria de l'HMI a un format comú (com a mínim, CSV).	HMI

¹ Es possible que la solució d'aquest punt vingui donada pel propi frontal de comunicacions que implementi la solució d'arquitectura final en comptes del PLC, essent aquest frontal l'encarregat de fer la traducció al sistema antic.

1.11 Disseny funcional de l'SCADA

HM005	Adaptació dinàmica de les escales de les gràfiques a l'HMI o adaptació sota demanda de l'operador.	HMI
HM006	Enregistrament d'1 hora de duració de les dades històriques de s'han de representar a l'HMI i configuració de les pantalles gràfiques corresponents.	HMI
HM007	Modificar el sistema de doble confirmació de les accions a l'HMI per tal de millorar-ne la usabilitat (confirmació conjunta de diverses accions).	HMI
HM008	L'identificador d'ATL d'un equip ha de poder ser modificable per un usuari amb el privilegis corresponents a través de l'SCADA del Centre de Control i propagat a l'HMI.	HMI

Taula 3-1: Requisits dels PLC i HMI