UNIVERSITÀ DEGLI STUDI DI GENOVA

CENTRO DI SERVIZI PER IL PONENTE LIGURE

Giardini Botanici Hanbury - Imperia - Savona

ALLEGATO TECNICO

Indagine di mercato per la realizzazione (fornitura, posa in opera, configurazione, collaudo) di un nuovo sistema SCADA e BMS (Building Management System) a servizio dell'infrastruttura di ricerca denominata Smart Polygeneration Microgrid in uso presso il Campus Universitario di Savona

Premessa 5
Descrizione della Microrete poligenerativa - Smart Polygeneration Microgrid (SPM) 5
La Smart Polygeneration Microgrid – SPM 5
Topologia di rete della SPM 6
Lo Smart Energy Building (SEB) 8
Descrizione dei sistemi SCADA e BMS esistenti 10
Generalità 10
Protocolli di comunicazione 10
SCADA 10
Sistema BMS 11
Descrizione degli interventi di adeguamento e obiettivi del nuovo Sistema 14
Sviluppo integrato 14
Connessioni 15
Networking 15
Connettività 16
Cyber security 16
Modularità ed espandibilità 16
Aggiornamenti sistema e compatibilità 17
Lifecycle 18
Licensing e assistenza 18
Caratteristiche generali 19
Sistema operativo 19
Gestione utenti 20
Interfaccia utente 22
Pagine grafiche 22
Pagine panoramiche 23
Operatività sistemi 23

Guida interattiva 23
Diagnostica 23
Gestione variabili 24
Definizione 24
Visualizzazione 25
Allarmi 25
Lista eventi 26
Modellizzazione impianto 26
Archiviazione 26
Servizio di notifica (Message Control) 27
Process recorder 28
geographic information system (GIS) 28
Soft PLC 29
Programmazione della produzione e degli impianti 29
Diagnostica sistemi 30
Caratteristiche energetiche 31
Colorazione topologica 31
Controllo topologia 31
Command processing 31
Command sequencers 31
Token di rete 32
Operating security 32
Funzioni di alto livello per la rete elettrica 32
Localizzazione guasti nella rete elettrica 32
Localizzazione di guasti basata su impedenza 33
Calcolo Load flow,state estimator e (N-1) calculation 33
Caratteristiche reportistica 34

Base 34
Avanzata 34
Caratteristiche principali 35
Temi template 36
Analisi predittiva 37
Condivisione dati vs terzi (Process Gateway) 38

Premessa

Il presente documento sintetizza gli interventi da eseguirsi sugli Impianti Tecnologici tali da garantire una corretta gestione e continuità della Microrete poligenerativa (SPM – Smart Polygeneration Microgrid) installata presso il Campus di Savona dell'Università di Genova, Via Magliotto 2, Savona.

Viene nel seguito introdotta l'infrastruttura Smart Polygeneration Microgrid, i suoi componenti e il sistema SCADA, BMS, EMS attualmente in uso e verranno elencate in via sommaria le caratteristiche del sistema richiesto in fase di gara.

Scopo della presente fornitura è la realizzazione di un sistema hardware-software unico per la gestione di tutta l'infrastruttura di generazione di energia, termica ed elettrica, presso il Campus Universitario di Savona. Viene richiesto quindi, un unico strumento software, per la gestione dei consumi/generazioni elettriche e termiche, per il controllo e il monitoraggio degli edifici oggetto di intervento (BMS) e per l'analisi e per il processo decisionale e automatizzato della gestione dell'energia.

Maggiori dettagli verranno esplicati nel capitolato tecnico allegato al bando di gara successivo alla manifestazione di interesse.

Descrizione della Microrete poligenerativa- Smart Polygeneration Microgrid (SPM)

La fornitura del nuovo sistema dovrà garantire la piena compatibilità con tutti gli elementi descritti e identificati nel seguito. Dal macro sistema fino all'ultimo dei componenti in campo.

Il sistema di supervisione e controllo oggetto della specifica sarà dedicato alla supervisione delle seguenti infrastrutture elettriche e termiche presenti al Campus, attualmente monitorate da diversi sistemi:

- la Smart Polygeneration Microgrid (SPM)
- lo Smart Energy Building (SEB) o palazzina Oliva
- la centrale termica, il primo piano della palazzina Delfino e le aree comuni della palazzina "Nuove residenze"

Le infrastrutture elettriche della SPM sono monitorate da uno SCADA (Supervisory Control and Data Acquisition) tipo SIEMENS Sicam WinCC, mentre le grandezze termiche dei dispositivi della SPM (es. potenza termica prodotta dalle turbine), l'intero SEB, la centrale termica, il primo piano della palazzina Delfino e le aree comuni della palazzina "Nuove residenze" sono monitorati e gestiti da un sistema di supervisione edificio – Building Management System (BMS) tipo SIEMENS Desigo Insight.

I sistemi vengono brevemente descritti nel seguito.

La Smart Polygeneration Microgrid – SPM

La SPM è costituita da un sistema di distribuzione trifase in bassa tensione (tensione nominale: 400 V concatenata) con generazione elettrica (e termica), equipaggiato con sistemi di comunicazione, controllo e gestione dedicati. La Figura 1 mostra la localizzazione all'interno del Campus dei dispositivi principali facenti parte della SPM, oltre che la posizione degli edifici del campus ed in particolare dell'edificio SEB.

I principali dispositivi connessi alla microrete sono:

- 2 cogeneratori (CHP) Capstone: una microturbina C65 Dual-Mode ed una C65 Grid Connected (entrambe caratterizzate da una potenza elettrica nominale di 65 kWe ed una termica nominale di 112 kWth)
- 2 caldaie alimentate a gas naturale;
- due chiller: essi permettono di impiegare la potenza termica delle microturbine per il raffrescamento estivo della biblioteca e della palazzina Delfino
- accumulo elettrico (batterie al sodio – nickel SoNick, energia nominale 141 kWh)
- due impianti fotovoltaici (potenza di picco 80 kWp e 15 kWp);
- due stazioni di ricarica per veicoli elettrici.

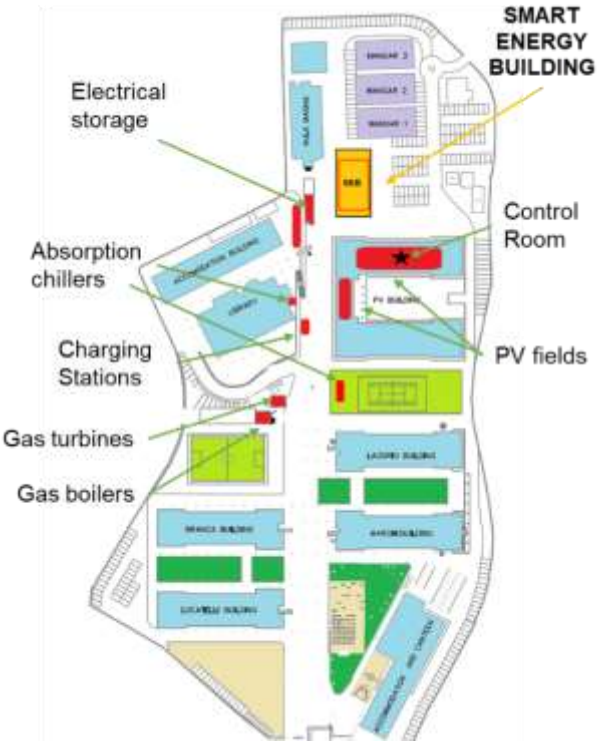

Figura 1. Planimetria del Campus con ubicazione degli edifici, dei dispositivi principali della SPM ed il SEB, delle Unità di generazione ed altri dispositivi

Topologia di rete della SPM

Per quanto riguarda la topologia di rete, nelle Figure 2 e 3 sono riportati due schemi unifilari di massima del sistema elettrico del Campus e della SPM rispettivamente.

Il campus è allacciato alla rete di Media Tensione dell'Ente Distributore a 15 kV 3F 50Hz mediante un unico punto di fornitura. La trasformazione al livello di tensione di utilizzo (400V 3F+N 50 Hz) avviene mediante una serie di trasformatori MT-BT.

La rete principale del Campus in bassa tensione, preesistente alla SPM, è connessa alla sezione principale di media tensione mediante due trasformatori MT-BT. Un terzo trasformatore MT-BT dedicato, installato nella cabina principale del Campus, connette la microrete alla sezione principale di media tensione.

La microrete è caratterizzata da un sistema di distribuzione ad anello che connette un quadro elettrico principale denominato QEG a cinque quadri secondari denominati rispettivamente Q01, Q02, Q03, Q04, Q05, oltre che ad un certo numero di quadri secondari.

I vari dispositivi della microrete sono collegati ai suddetti quadri ed in particolare:

- un chiller ed il campo fotovoltaico di potenza minore sono connessi al Q01
- il campo fotovoltaico principale e l'accumulo elettrico sono connessi al Q02
- il quadro Q03 è dedicato alla connessione di un laboratorio e di una delle stazioni di ricarica per veicoli elettrici
- il Q04 è dedicato ai CHP e all'altra stazione di ricarica
- il Q05 connette il SEB alla SPM.

Uno schema unifilare dettagliato della SPM è riportato nell'Allegato 1 "Unifilare_SPM.pdf".

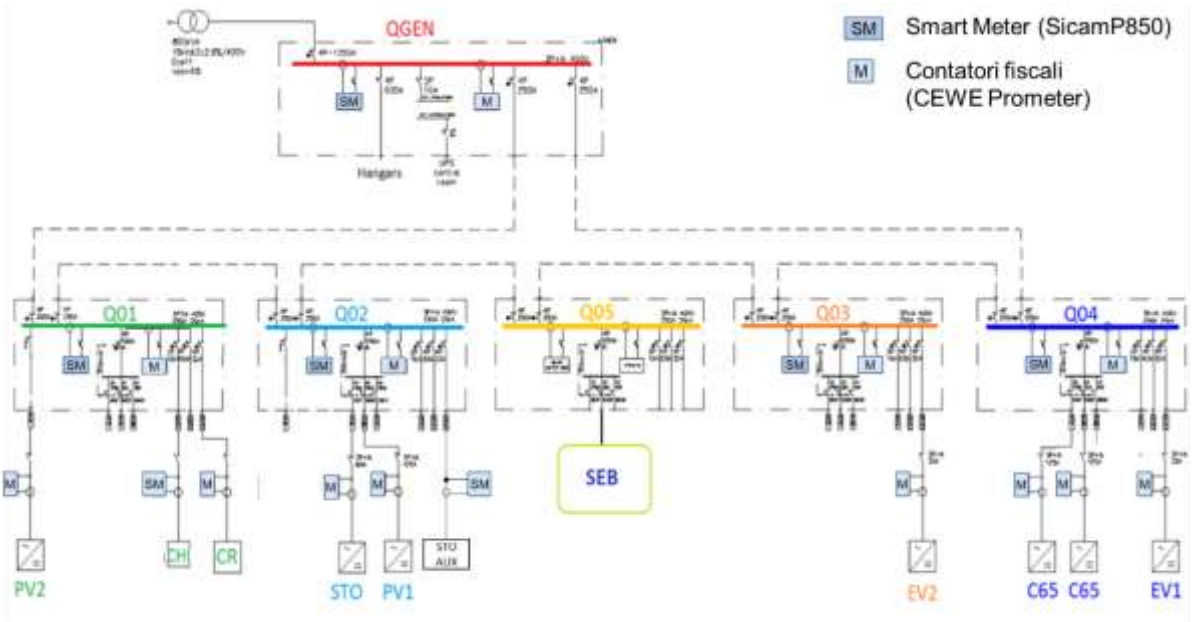

Figura 2. Schema elettrico unifilare semplificato della SPM (PV1 e PV2: fotovoltaici da 80 kWp e 15 kWp, CH: chiller, STO: accumulo elettrico, EV1 ed EV2: stazioni di ricarica veicoli elettrici, C65: microturbine, CR: control room)

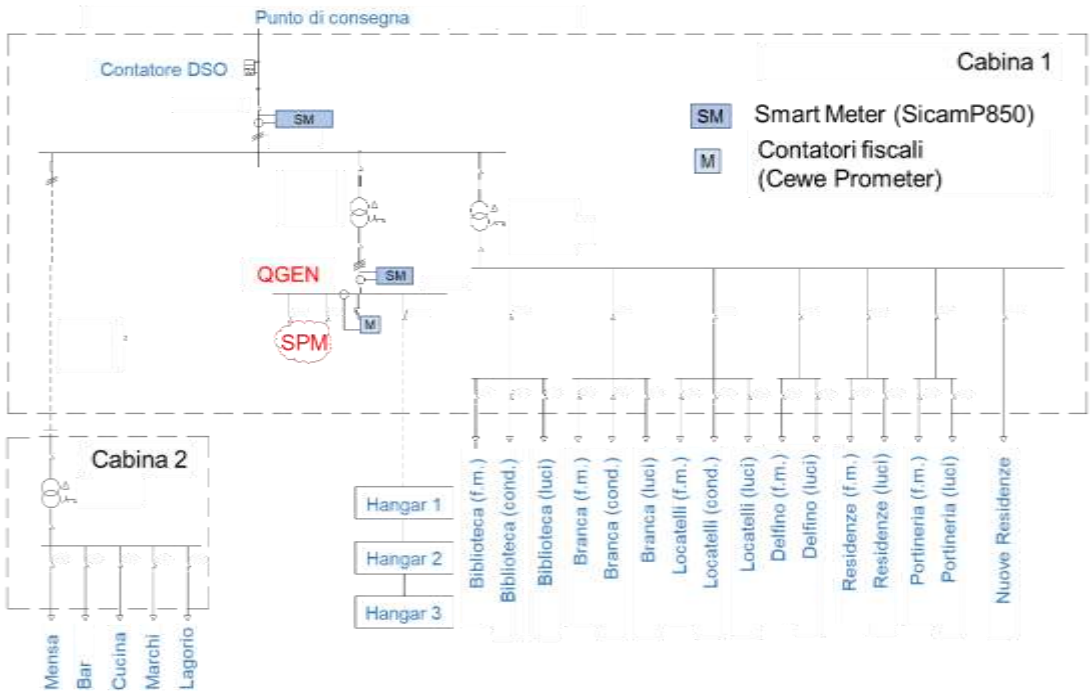

Figura 3. Schema elettrico unifilare di massima del Campus

Lo Smart Energy Building (SEB)

Il SEB (Figura 4) è stato progettato per essere un edificio innovativo e dalle alte prestazioni, volto a raggiungere gli obiettivi di emissioni di anidride carbonica nulla, alta efficienza energetica e nell'uso della risorsa idrica, elevata automazione.

La peculiarità del SEB è costituita dalla sua interazione con la SPM, rispetto alla quale si configura come un "prosumer", in grado di auto-produrre l'energia termica ed elettrica necessaria per la sua domanda, erogare verso la SPM l'energia in eccesso o, in caso di necessità, assorbire energia da essa. I consumi e le produzioni sono costantemente monitorati per valutare i benefici ambientali ed economici. Alcuni dei carichi sono controllabili.

Il SEB è caratterizzato dai seguenti dispositivi e soluzioni costruttive:

- Materiali ad alto isolamento termico
- Pompa di calore geotermica (circa 45 kWth, 8 sonde che arrivano ad una profondità di più di 100 m) per il riscaldamento ed il raffrescamento
- Pannelli solari termici
- Sistema di controllo della ventilazione e unità di trattamento aria
- Pompa di calore per l'acqua calda sanitaria
- Impianto fotovoltaico (PV3, 21 kWp)
- Illuminazione a basso consumo
- Recupero acqua piovana
- Facciate ventilate

Il SEB ha infine la funzione di "Living Lab" permettendo ricerche nel campo delle tecnologie sostenibili.

Figura 4. SEB

Descrizione dei sistemi SCADA e BMS esistenti

Generalità

Il sistema attualmente installato è basato su due sistemi SCADA ed interfaccia utente:

- uno SCADA, SICAM-WinCC (Siemens), per la supervisione della "parte elettrica" della microrete
- un BMS, Desigo Insight (Siemens), per la supervisione di:
  - "parte termica" della microrete (es. potenze termiche, portate, temperature, ecc… di microturbine, caldaie)
  - palazzina "Smart Energy Building" (palazzina Oliva)
  - secondo piano della Palazzina Delfino e dei locali comuni delle "nuove Residenze".

La tabella seguente fornisce un ordine di grandezza delle "TAGs" acquisite dallo SCADA e del totale delle variabili ed allarmi acquisiti dalle centraline di Desigo:

Sottosistema	TAGs
SCADA WinCC	2500
BMS Desigo Insight	15000

Protocolli di comunicazione

I protocolli attualmente utilizzati nel sistema sono:

- per la parte elettrica:
  - IEC 61850 per la comunicazione fra SCADA e remote terminal unit o "smart meter"
  - Modbus RTU a livello di campo (quasi tutti i dispositivi possono essere interfacciati sia in Modbus RTU che in Modbus TCP)
  - OPC-DA (Open Platform Communications) per l'interfacciamento di sistemi di gestione e terze parti con lo SCADA elettrico (WinCC)
- per la parte termica:
  - BACnet per la comunicazione fra il BMS e le relative centraline (v. sezione BMS)

SCADA

Il sistema SCADA è connesso, mediante una rete locale in anello in fibra ottica, a 5 remote terminal unit (RTU) del tipo TM 1703 ACP. Le RTU, a loro volta, sono interfacciate con i dispositivi in campo (sistemi di controllo interni dei dispositivi, multimetri, contatori, organi di protezione e manovra, ecc…) mediante comunicazione via Modbus RTU e I/O analogici o digitali.

La comunicazione fra SCADA ed RTU avviene in protocollo IEC 61850.

Circa 10 strumenti di misura multifunzione tipo smart meter Sicam P850 sono inoltre interfacciati con lo SCADA, direttamente in IEC 61850.

Una pagina tipica dello SCADA è riportata nella seguente Figura 5.

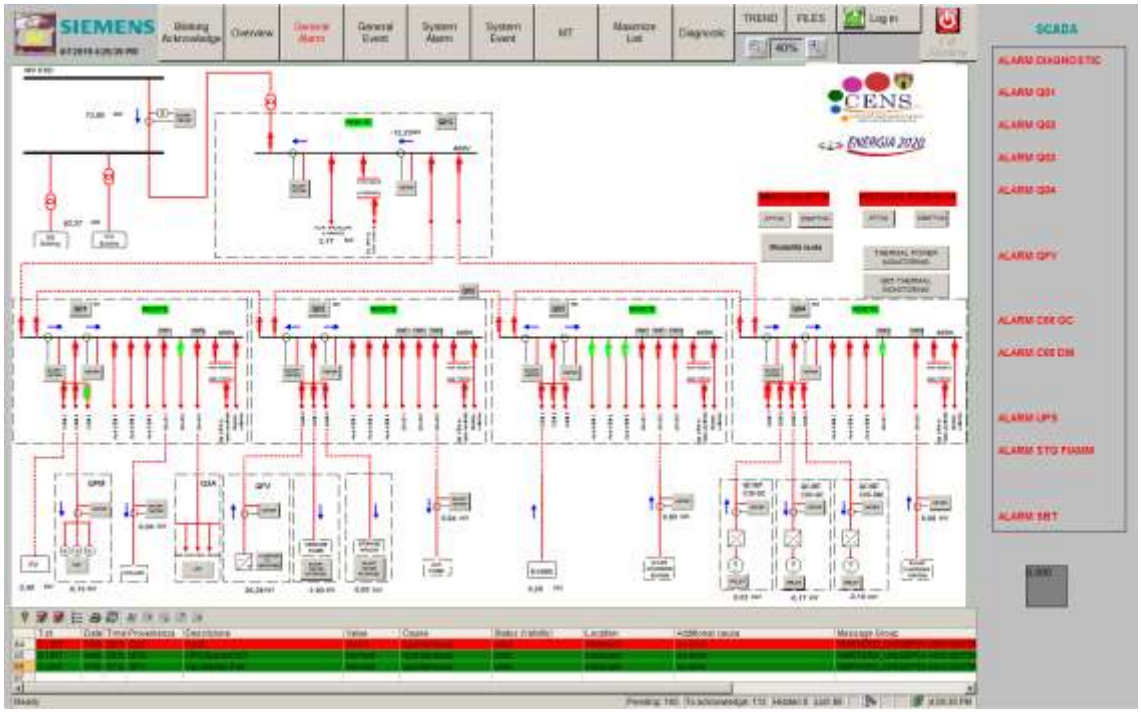

Figura 5: Scada - Sinottico Principale (in basso: allarmi/eventi)

Sistema BMS

La comunicazione fra Desigo Insight e le centraline installate avviene in BACnet. Inoltre, una centralina è attualmente interfacciata in Modbus con una RTU del sistema SCADA per inviare allo stesso i dati riguardanti le potenze termiche prodotte dalle turbine e dalle caldaie. Le centraline presenti sono ubicate come graficamente rappresentato nella figura seguente ed elencate nella successiva tabella.

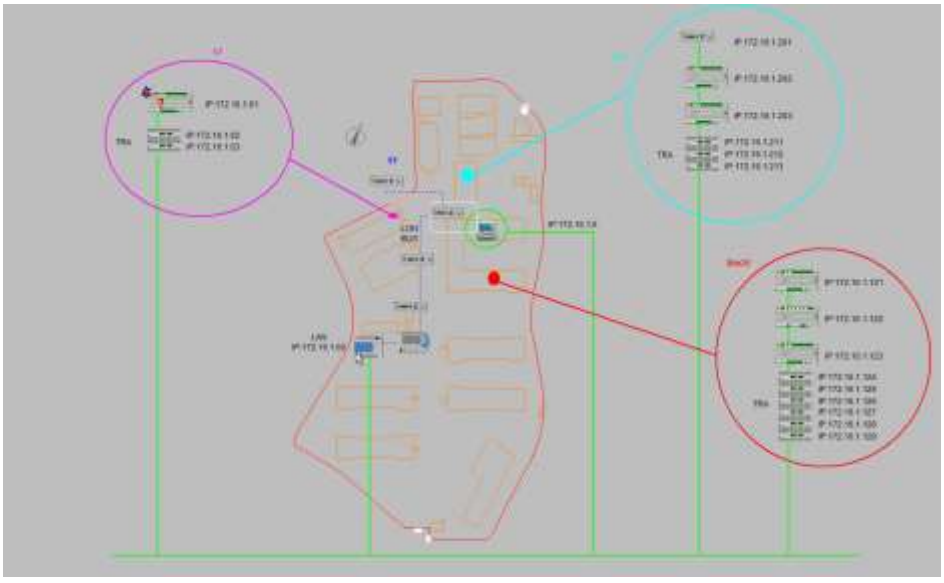

Figura 6: BMS- Ubicazione delle centraline

Tabella 1: BMS- Elenco delle centraline

Nome	Costruttore	Indirizzo	Device ID	Tipo
Site20'AS01	Siemens Building Technologies	172.16.1.121	2117633	PXC12-E.D / HW=V11.01
Site20'AS02	Siemens Building Technologies	172.16.1.122	2117634	PXC22-E.D / HW=V11.01
Site20'AS03	Siemens Building Technologies	172.16.1.123	2117635	PXC001-E.D / HW=V4.01
AS_10 B Sud	Siemens Building Technologies	172.16.1.124	10	TRA
AS_11 A Sud	Siemens Building Technologies	172.16.1.125	11	TRA
AS_12 B Ce	Siemens Building Technologies	172.16.1.126	12	TRA
AS_13 A Ce	Siemens Building Technologies	172.16.1.127	13	TRA
AS_14 B Nord	Siemens Building Technologies	172.16.1.128	14	TRA
AS_15 A Nord	Siemens Building Technologies	172.16.1.129	15	TRA
S10'AS01	Siemens Building Technologies	172.16.1.201	2107393	PXC200-E.D / HW=V3.00
S10'AS02	Siemens Building Technologies	172.16.1.202	2107394	PXC001-E.D / HW=V4.01
S10'AS03	Siemens Building Technologies	172.16.1.203	2107395	PXC001-E.D + PXA40-RS1 / HW=V4.01
POL908_FFB47B	Siemens Building Technologies	172.16.1.205	4174971	POL908
AS11_PT	Siemens Building Technologies	172.16.1.211	211	TRA
AS12_P1	Siemens Building Technologies	172.16.1.212	212	TRA
AS13_P1	Siemens Building Technologies	172.16.1.213	213	TRA
DWS01	Siemens Building Technologies	172.16.1.6	1048577	INSIGHT (BMS)
BNR01	Siemens Building Technologies, Landis & Staefa	172.16.1.60	1050625	PX GATEWAYS, PXG80-N
S7'AS01	Siemens Building Technologies	172.16.1.61	2104321	PXC001-E.D / HW=V2.01
AS_1	Siemens Industry, Inc.	172.16.1.62	62	TRA

AS_2	Siemens Industry, Inc.	172.16.1.63	63	TRA
S1'AS01	Siemens Building Technologies	1:0x0101	2098177	PXC00-U + PXA30-RS2 / HW=V1.02
S1'AS02	Siemens Building Technologies	1:0x0102	2098178	PXC02 Q04
S1'AS03	Siemens Building Technologies	1:0x0104	2098179	PXC50.D / HW=V3.00
S1'AS04	Siemens Building Technologies	1:0x0105	2098180	PXC50.D / HW=V1.00
S1'AS06	Siemens Building Technologies	1:0x0107	2098182	PXC50.D / HW=V1.00

TRA: total room automation (unità remote, attuatori e sensori per la supervisione ed il controllo delle singole stanze, sottese ad una centralina)

Nella Figura seguente è riportato un esempio di pagina grafica del BMS Desigo.

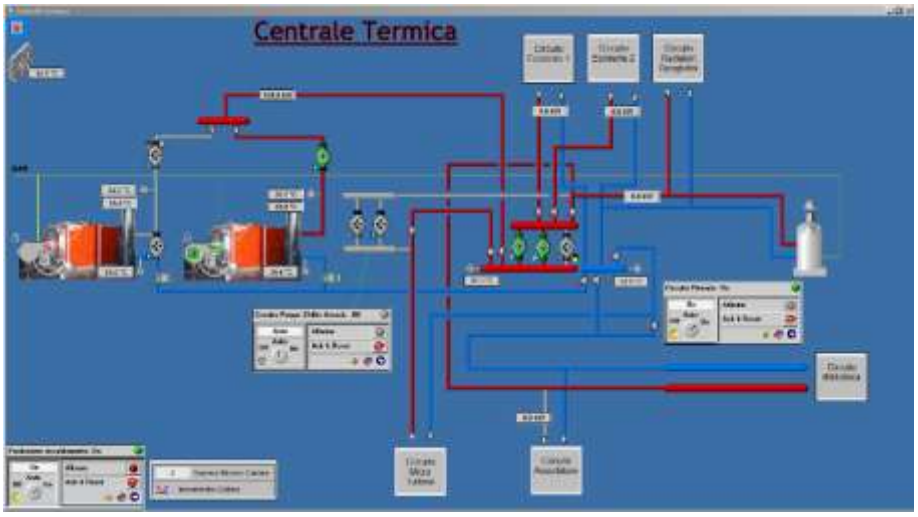

Fig. 7: Pagina pagina relativa alla Centrale Termica

Descrizione degli interventi di adeguamento e obiettivi del nuovo Sistema

Il nuovo sistema di supervisione e controllo SCADA, BMS ed EMS dovrà garantire la piena funzionalità con tutti gli elementi esistenti al Campus Universitario di Savona e descritti nei paragrafi precedenti. Si dovrà inoltre prevedere la possibilità di inserirne di nuovi, in futuro, senza l'intervento da parte di tecnici esterni ma con l'ausilio del personale UNIGE ricercatore e tecnico formato a tale scopo a seguito della presente fornitura.

Il nuovo sistema di supervisione e controllo dovrà quindi essere una **piattaforma software** scalabile e sicura, che possa soddisfare non solo esigenze generiche di HMI/SCADA, bensì anche necessità più avanzate come servizi di analisi e report, Building Management System, Energy Management System. Deve quindi possedere un elevato grado di connettività verso i dispositivi in campo, funzionalità ingegnerizzate appositamente per esigenze del mondo energetico, supportare la creazione di architetture di rete complesse, integrare linguaggi di programmazione PLC (ad es: IEC 61131-3) e permettere la condivisione dei dati verso sistemi di terze parti con tecnologie standard (es. OPC UA) e non. Di seguito i moduli e le funzionalità complete che devono pertanto essere garantiti.

Sviluppo integrato

È necessaria una piattaforma software integrata per la creazione delle funzionalità di SCADA elettrico/BMS/Business Intelligence. Le funzionalità principali devono essere native e non sviluppate con codice esterno custom. L'acquisizione delle competenze necessarie allo sviluppo non devono richiedere conoscenze di programmazione approfondita di alto livello, bensì si dovrà poter diventare autonomi nella gestione di analisi e modifiche basilari attraverso corsi fruibili in pochi giorni.

I sistemi adottati dovranno essere compatibili con Unicode; permettendo l'utilizzo di qualsiasi set di caratteri. Dovrà essere possibile creare progetti o parti di progetto attraverso wizard sviluppati ad-hoc cosi come espandere i sistemi con funzionalità non previste attraverso l'integrazione di WPF (Windows Presentation Foundation) / elementi .NET Control di terze parti, o in alternativa programmi sviluppati in-house. Per tale scopo i linguaggi di programmazione supportati dovranno essere Visual Basic for Application (VBA), VB.NET, C# o REST. Il codice aggiuntivo sviluppato deve poter essere eseguito come macro o funzionare come servizio sia a livello di engineering che runtime.

Funzionalità native di importazione e esportazione (es. XML) devono essere utilizzabili all'interno degli ambienti di sviluppo così da garantire modifiche esterne degli elementi del progetto (es. pagine grafiche, funzioni, variabili,…)

I progetti sviluppati devono poter essere trasferiti semplicemente (con pochi click) via TCP/IP direttamente dall'ambiente di sviluppo, potendo discriminare i dispositivi di destinazione e preferibilmente ottimizzando la procedura di trasferimento includendo solo i file modificati e infine applicando le modifiche attraverso una procedura che per i cambiamenti più comuni eviti il riavvio dei Runtime. Inoltre, sempre la stazione di ingegneria deve poter permettere sia lo sviluppo che funzionalità di Runtime così da agevolare il debug delle applicazioni.

È molto importante poter eseguire backup regolari, versionabili automaticamente e con descrizione, durante le varie fasi di sviluppo. Questi poi devono poter essere utilizzati facilmente anche per operazioni di rollback e tramite l'ausilio di un apposito tool per comparare differenti versioni e per analizzare le differenze tra di

essi. È auspicabile avere un registro dei cambiamenti al progetto contestualizzato ai moduli e all'utente che ha effettuato la modifica.

Connessioni

Networking

Per permettere l'integrazione di sistemi eterogenei, da differenti aree e plessi, la piattaforma software deve garantire funzionalità native, che con una ragionevole quantità di tempo permettano la creazione di architetture topologiche complesse server/client/sistemi di terze parti anche su più sedi anche senza l'utilizzo di VPN attraverso i protocolli TCP/IP, UDP e HTTP, garantendo comunque la sicurezza e l'integrità del dato. Lo scambio dati tra tutti i componenti dell'architettura deve attuarsi in modo trasparente e spontaneo, idealmente sia attraverso l'indirizzo IP sia attraverso l'Hostname e questi protocolli di comunicazione è auspicabile che possano essere crittografati così da garantire una maggior sicurezza informatica.

Le parti critiche degli impianti devono poter essere ridondate in modo tale da garantire il corretto funzionamento degli impianti/edifici per cui sono state realizzate. Dovranno essere quindi implementati dei meccanismi nativi che in automatico eseguano lo switch al sistema di backup garantendo un flusso senza interruzioni di comunicazione con i dispositivi in campo, la registrazione di allarmi, eventi e dati storici. Altresì è importante poter continuare ad operare e controllare tutto quanto necessario sia dalle stazioni server che dai client. In aggiunta è importante poter effettuare il cambio di ruolo dei server (primario/secondario) anche in funzione di parametri "vitali" inerenti all'hardware (es. memoria disponibile, utilizzo CPU,…). Come negli altri casi sono preferibili soluzioni nativamente integrate che non abbiano come prerequisito approfondite conoscenze di programmazione. Di seguito vengono specificate meglio le varie tipologie di ridondanza che possono essere realizzate.

Deve essere supportata sia la ridondanza hardware che software. Con la ridondanza hardware in modalità nativa e automatica deve essere garantita la coerenza della comunicazione con i dispositivi di controllo (ad es. doppi PLC/RTU ridondati). Con la ridondanza software occorre comunque garantire una soluzione senza perdita di continuità nel momento in cui viene attuata la commutazione al server stand-by. Nel momento in cui cambierà il server anche tutti i client connessi alla rete in automatico dovranno rilevare l'anomalia e collegarsi al nuovo server. Il sistema deve permettere di poter configurare anche il comportamento da tenere al ripristino del guasto permettendo di scegliere che il server "riparato" torni ad essere il primario oppure che riprenda ad operare con il ruolo di server stand-by.

Nel caso della ridondanza circolare il computer A è il server per il progetto A e il server stand-by per il progetto B. Il computer B è il server per il Progetto B e server stand-by per il Progetto C. Il computer C è il server per il Progetto C e server stand-by per il Progetto A. Il cerchio è così completato. Se un computer si guasta, il sistema deve essere in grado di continuare a funzionare in modo coerente con le stazioni rimanenti. Questo modello deve essere in grado di essere espanso con qualsiasi numero desiderato di stazioni collegate.

Con la ridondanza ponderata, l'attivazione del server deve essere basata su metriche definite dall'utente. Ciò consente la nomina di un server primario sulla base di condizioni limite predefinite (come la qualità della connessione, il carico del processore e la capacità di memoria, ecc.), inclusa la commutazione flessibile del server. Con la ridondanza hardware in una rete ponderata, i criteri di valutazione determinano quale

computer assume il ruolo di server primario e quale assume il ruolo di server di standby. Questa valutazione può essere configurata liberamente e può includere diversi criteri. Ad ogni criterio vengono assegnati punti di valutazione: il peso. La somma dei punti di ponderazione decide quindi sul rispettivo ruolo del server.

Connettività

I driver mandatori e integrati nativamente nella piattaforma software per la completa realizzazione del revamping qui descritto, dovranno garantire il corretto scambio dati tra lo SCADA e i dispositivi in campo elencati in specifica. I protocolli da supportare sono i seguenti:

- IEC 61850 Client
- IEC 61850 server
- Modbus master TCP/RTU
- Modbus RTU over TCP/IP
- Bacnet IP Client (anche Trend, Scheduler)
- OCPP (colonne EV)
- SNMP Manager (v3)
- OPC UA Client
- REST API, MQTT (Driver generico per integrazione con protocolli non standard)

Questi è preferibile che possano anche funzionare in modalità “simulate” così da poter effettuare prove di vario genere prima di un utilizzo reale in campo.

Cyber security

La piattaforma software adottata deve garantire certi requisiti anche in termini di sicurezza informatica sia a livello dei protocolli implementati, sia a livello di architetture che intrinsecamente a livello di prodotto. Ciò significa che verranno accettate solamente soluzioni che vengono sviluppate seguendo e integrando gli standard internazionali che normano tali esigenze.

A livello di protocolli è indispensabile che siano disponibili e nativamente implementati il supporto TLS secondo lo standard IEC TS 62351-4:2007 / compatibility mode in accordo alla IEC 62351-4:2018 MMS Secure Association according to IEC TS 62351-4:2007 and compatibility mode according to IEC 62351-4:2018

Inoltre, le architetture implementate dovranno poter essere eventualmente validate secondo lo standard IEC 62443-4-1 (Security for industrial automation and control systems) così da poter garantire un’adeguata protezione da accessi non autorizzati, trasferimento dati crittografati, accessi regolamentati con password, personalizzazione delle porte di comunicazione, files signatures ecc. ecc.

Modularità ed espandibilità

Con l’intento di attuare in modo semplice e veloce le modifiche di routine ed eventuali espansioni future si intende adottare una piattaforma software che possieda dei concetti di modularità, organizzazione

gerarchica dei progetti, uno sviluppo object-oriented e quanto più possibile un riutilizzo delle funzionalità che vengono implementate (simboli, pagine, funzioni, …). La naturale conseguenza sarà anche quella di ottenere degli oggetti facilmente manutenibili nel tempo.

Detto ciò dovrà essere possibile:

- Avere una libreria di simboli predefiniti IEC 60617-x del settore elettro impiantistico
- Creare una libreria di simboli (es. interruttori, trasformatori,…) facilmente istanziabili e parametrizzabili a seconda dello scopo.
- Creare una gerarchia dei simboli così da ottimizzare e rendere più consistente lo sviluppo.
- Creare simboli complessi istanziabili, che racchiudano non solo elementi grafici, ma anche variabili, logiche, funzioni e pagine.
- Creare una gerarchia tra i progetti atta alla condivisione trasparente delle informazioni contenute in essi. (possibilità di creare progetti padre-figlio).

Grazie alla gerarchia tra i progetti deve essere possibile accedere, da un progetto di livello superiore, ai dati dei progetti sottostanti (pagine, allarmi, ….) così da poter facilmente creare una eventuale control room di sistemi anche geograficamente distribuiti.

Un approccio modulare deve essere implementato e quindi sfruttabile anche da un punto di vista del licensing del prodotto. Ciò significa che aggiungendo a posteriori nuove funzionalità ai sistemi queste possano essere aggiunte alle licenze esistenti senza dover riacquistare un nuovo prodotto.

Aggiornamenti sistema e compatibilità

L'adozione di piattaforme software distribuite porta a maggiori requisiti in relazione alla compatibilità delle versioni del sistema (versioni dei componenti/servizi del sistema). Questa situazione è strettamente legata al progetto di sistema modulare ed è in linea con la necessità di manutenzione "minimamente invasiva" (per esempio, nessuno spegnimento completo consentito, progetto modulare aggiornamenti e ricariche a caldo).

Il sistema deve quindi essere conforme ai seguenti requisiti di compatibilità:

- Compatibilità del progetto (compatibilità ingegneristica) in caso di una nuova versione dell'ambiente di sviluppo (il "vecchio" progetto di sviluppo può essere aperto e mantenuto in un "nuovo" ambiente di sviluppo).
- Un nuovo ambiente di sviluppo può creare sorgenti di progetto per vecchie versioni di Runtime utilizzando impostazioni del compilatore dedicate (sistema di sviluppo e sistema Runtime, retrocompatibilità)
- Una nuova versione di Runtime può eseguire sorgenti di progetto per vecchie versioni di Runtime più vecchie (sistema Runtime, retrocompatibilità)
- Una nuova versione di Runtime di un client di rete può interagire con un vecchio Runtime di un server

- Aggiornamento delle nuove funzionalità configurate durante il normale funzionamento del Runtime evitando il riavvio completo. (aggiornamento “a caldo”)

- Compatibilità del formato XML di importazione/esportazione verso versioni più recenti partendo da versioni più vecchie

- La compatibilità delle interfacce di programmazione deve essere garantita in diverse versioni. In alternativa, devono essere presenti almeno strategie e strumenti di migrazione che possano ridurre al minimo il lavoro di adattamento manuale.

Lifecycle

Il life cycle delle licenze dovrà essere dichiarato pubblicamente e dovrà avere un supporto di almeno 5 anni e un product fixing di almeno 5 anni (oppure 6 anni nel caso di offerta con contratto di aggiornamento delle licenze software).

Licensing e assistenza

Il sistema dovrà essere licenziato secondo le architetture, i driver e i moduli richiesti, inoltre dovrà essere modulabile e scalabile in base alle necessità.

Ognuna delle licenze dovrà essere corredata con la propria dongle di protezione oppure attraverso una licenza software installabile su PC fisico (o VM).

Inoltre, dovrà essere necessariamente presente il supporto tecnico al progetto da parte dell’integratore, il quale garantirà assistenza telefonica o via email in orario lavorativo (8.30-18, 5 giorni a settimana).

Aggiornamento licenze software: contratto di aggiornamento continuo all’ultima release di prodotto e supporto tecnico sulla piattaforma di sviluppo per un minimo di 3 anni dall’avvenuto collaudo

Preferibilmente, l’integratore potrà offrire un ulteriore forme di assistenza:

- Assistenza 24/7: copertura completa 365 giorni l’anno sul sistema fornito per una durata di 3 anni dall’avvenuto collaudo

Caratteristiche generali

Sistema operativo

La piattaforma software che si intende adottare deve avere i minimi requisiti hardware ed essere supportata da sistemi operativi uguali o più recenti di quelli specificati nella tabella seguente.

	Operating System	OS Build	RAM	CPU
Server Web server	Windows Server 2019 (eccetto versione Core)	10.0.17763	8GB	Quad core (4C+4T)
Client Web Client Soft PLC	Windows 10 (Home, Pro, Enterprise, Education, Pro Education, Enterprise LTSB, Enterprise LTSC, IoT Enterprise, Pro for Workstations)	1507	4GB	Dual core (2C+2T)
Engineering Studio	Windows 10 (Home, Pro, Enterprise, Education, Pro Education, Enterprise LTSB, Enterprise LTSC, IoT Enterprise, Pro for Workstations)	1507	16GB	Dual core (2c+2T)
Report engine	Windows Server 2019 (eccetto versione Core)	10.0.17763	32GB	Octa core

Vengono considerati valori aggiunti le seguenti caratteristiche opzionali.

I componenti software possono funzionare anche in modalità 64-bit in modo da ottimizzare le performance del rispettivo sistema operativo.

Inoltre lo SCADA deve poter essere eventualmente virtualizzato, sia come native hypervisor (bare-metal) che hosted hypervisor, o containerizzato sotto forma di Docker.

La qualità grafica dello SCADA deve poter essere ottimizzata in funzione delle risorse del sistema operativo. Ciò significa che attraverso un'impostazione del progetto potrò discriminare se i runtime sfrutteranno Windows nel caso di hardware poco prestanti, diversamente dovrà essere possibile optare tra DirectX Software o Hardware.

Gestione utenti

Il sistema deve supportare l'amministrazione degli utenti per il Runtime (stazione operatore, HMI) così come per il sistema di sviluppo (ambiente di configurazione del progetto). In entrambi i casi, il sistema deve garantire protezione da accessi non autorizzati e manipolazioni indesiderate. Di conseguenza, deve essere possibile con i meccanismi offerti concedere agli utenti registrati l'accesso a determinate aree e rifiutarlo ad altri. I diritti degli utenti per la visualizzazione e la manipolazione dei dati (o, nel caso di un sistema Runtime, per impostare azioni di controllo) devono poter essere amministrati selettivamente.

Ogni utente deve poter scegliere la propria password e cambiarla anche online. Se non c'è attività dell'utente per un periodo di tempo definito, questo deve portare al logout automatico.

Il sistema deve anche soddisfare i seguenti requisiti:

- Deve offrire la possibilità che solo un singolo utente o solo alcuni utenti abbiano diritti di amministratore, in modo che solo questa persona sia autorizzata a creare nuovi utenti o a bloccare il sistema e ad attivare o disattivare gli utenti.

- Deve essere possibile disattivare un utente e riattivarlo in un secondo momento. Un utente disattivato non deve essere in grado di accedere. Tuttavia, tutte le azioni che hanno fatto in passato devono essere rintracciabili.

- Se una password errata viene inserita più volte (il numero può essere impostato nel progetto di ingegneria), l'utente deve essere bloccato automaticamente. Un blocco utente può essere revocato solo da un amministratore. Questo meccanismo deve avere effetto anche per un tentativo di login tramite l'API.

- Se un nome utente errato viene inserito più volte (il numero può essere impostato nel progetto di ingegneria), l'intero sistema deve essere bloccato. Per permettere il login degli utenti, l'amministratore deve sbloccare nuovamente il sistema. Questo meccanismo deve avere effetto anche per un tentativo di login tramite l'API.

- Deve essere possibile definire la complessità della password

  - lunghezza della password
  - Numero di caratteri speciali
  - Numero di cifre
  - Numero di lettere maiuscole
  - Numero di lettere minuscole
  - Deve essere possibile stabilire una lunghezza minima per una password.

o Deve essere possibile salvare una cronologia della password.

o Deve essere possibile definire il numero di password usate in precedenza che non possono essere riutilizzate.

o Le password devono scadere dopo un certo tempo (scadenza delle password configurabile in giorni). L'utente deve cambiare la sua password al primo accesso.

o L'amministratore può creare solo utenti con un livello di autorizzazione inferiore o uguale al proprio. Nessun livello di autorizzazione superiore può essere attivato per altri utenti così da evitare una escalation di privilegi.

o Agli utenti può essere richiesto di cambiare la password.

o Non deve essere possibile per l'amministratore chiedere informazioni sulle password di altri utenti. Per questo motivo, per un utente con un nuovo account o con una password che è stata impostata dall'amministratore (password dimenticata), è costretto a cambiare la password al successivo accesso.

o Deve essere possibile creare utenti con una data di scadenza predefinita. Deve essere possibile attivare un avviso per l'utente al login quando scade.

o Se nessuna azione dell'utente viene fatta per un certo tempo configurabile, l'utente deve essere automaticamente disconnesso. Questo può essere impostato separatamente per ogni gruppo di utenti.

In alternativa, deve essere possibile utilizzare le definizioni dell'amministrazione utenti di Windows®. I livelli di autorizzazione per il sistema di controllo del processo devono essere modificabili in Microsoft Active Directory (per un dominio mancante, deve essere possibile una connessione al Microsoft AD-LDS® come alternativa). L'amministrazione utente completa dovrebbe essere definita a livello di sistema operativo. Solo l'utente Windows® deve essere registrato con nome utente e password nel sistema di controllo del processo.

La registrazione completa dell'attività dell'utente dovrebbe essere effettuata nello stesso modo come per un utente integrato. I seguenti 3 scenari dovrebbero essere possibili come relazione tra il computer degli impianti e il controller di dominio Windows:

• Il computer dell'apparecchiatura è un membro del dominio Windows. Un utente valido dal dominio di Windows è connesso al computer dell'apparecchiatura. I diritti dell'utente sono presi dal dominio collegato.

• Il computer dell'apparecchiatura è membro di un dominio di automazione speciale. Un utente valido da un altro dominio Windows (di livello superiore) è connesso al computer dell'apparecchiatura. I diritti dell'utente sono presi dal dominio collegato di livello superiore.

• Il computer dell'apparecchiatura non è membro di un dominio. Un utente valido da un dominio Windows liberamente definibile è connesso al computer dell'apparecchiatura. I diritti utente sono presi da questo dominio non collegato.

Nell’ottica di avere dei sistemi integrati in scenari LAN/WAN/Cloud, evitando quanto più possibile il ricorso all’utilizzo di VPN, ma comunque garantendo l’integrità e la sicurezza del dato, è fortemente richiesta

l'adozione di sistemi moderni e adatti a tale scopo. Le connessioni e i dati dovranno quindi essere protetti con meccanismi come TLS / SSL (Transport Layer Security, Secure Sockets Layer), certificati digitali e da servizi di autenticazione e autorizzazione accessi di tipo RBAC (Role-based access control).

Avendo poi a disposizione un meccanismo di SSO (Single Sign On) i dati e le informazioni che transiteranno sulla rete saranno nativamente criptate evitando così la modifica e il furto di informazioni sensibili.

Non ultimo occorre avere dei meccanismi, sempre nativi, di bufferizzazione delle informazioni in caso di interruzione del collegamento e la possibilità di poter gestire in autonomia gli utenti e gli accessi ai vari sistemi suddetti.

Interfaccia utente

Il sistema deve supportare il multilingua e le varie lingue che sono state progettate devono poter essere cambiate in qualsiasi momento durante il funzionamento degli impianti in modo indipendente a prescindere dalla scelta fatta sulle varie stazioni di controllo e comando. Con il cambio lingua si devono adattare anche documenti correlati come ad esempio i manuali e le istruzioni operative. In funzione della lingua scelta si devono poter adattare i font utilizzati per mostrare tutti i caratteri del linguaggio selezionato.

A seconda della lingua selezionata, o anche in maniera indipendente, deve essere possibile cambiare la gestione dei valori con unità di misura differenti. La conversione deve essere effettuata in maniera trasparente dallo strumento in campo.

La tecnologia multi-monitor deve essere nativamente supportata, così da poter facilmente realizzare sistemi di controllo (es. control room) di varia natura.

Pagine grafiche

Le pagine grafiche, che dovranno essere realizzate dal fornitore, devono corrispondere, come numero minimo, a quelle attualmente esistenti nel sistema e dovranno replicarne il funzionamento e lo scopo. Ulteriori pagine di completamente o di approfondimento potranno essere richieste dalla stazione appaltante.

Le pagine grafiche devono avere differenti scopi, è quindi necessario possedere tutti gli elementi necessari per poter integrare pagine che coprono le seguenti necessità.

- Pagine di processo
- Liste allarmi/eventi (attivi e storici)
- Trend YT, XY, curve e Gantt (dati in tempo reale e storici)
- Filtro per allarmi/eventi
- Tastiere virtuali (per valori booleani, numeri e stringhe)
- Message box
- Gestione modulo invio messaggi manutentori
- Gestione utenti, login

- Pagine per mostrare siti web HTML
- Revisione archivi storici
- Visualizzatore report
- Pagina per diagnostica variabili
- Pagine
- Notepad
- Menu contestuali

La possibilità di poter estendere e arricchire la grafica con elementi WPF (Windows® Presentation Foundation), ActiveX, grafiche vettoriali SVG, DXF e WMF è fortemente richiesta. Nell'ottica di ridurre e ottimizzare i tempi di sviluppo così come la gestione e manutenzione del nuovo sistema è necessario avere dei template pronti all'uso, così come la creazione di propri template e dei meccanismi di riutilizzo della stessa pagina per oggetti e scopi differenti.

Pagine panoramiche

Il sistema deve anche essere in grado di visualizzare schemi completi come unifilari, P&I, parchi eolici/fotovoltaici, planimetrie, mappe geografiche o layout di impianti di produzione. Deve essere possibile zoomare in questa schermata panoramica dinamicamente a Runtime. Il sistema deve anche offrire la possibilità di disporre gli elementi su questo schema e di modificare il livello di dettaglio per l'operatore in funzione del livello di zoom ("decluttering"). A seconda del livello di zoom selezionato dall'operatore dovranno essere rappresentati gli elementi progettati per quel livello di dettaglio.

Operatività sistemi

La piattaforma software deve supportare nativamente il multitouch per facilitare l'interazione con i sistemi realizzati e permettere anche operazioni di zoom in grafici, schemi unifilari e layout di varia natura. Per le operazioni di setpoint devono essere previste e integrate tastiere virtuali liberamente definibili per aspetto e contenuto.

Deve essere possibile eseguire programmi esterni attraverso l'interfaccia grafica realizzata e attraverso funzioni richiamate ciclicamente o ad eventi predefiniti. Sempre senza dover utilizzare scripting esterno occorre poter effettuare operazioni di files come copia, cancellazione e spostamento.

Guida interattiva

L'interfaccia utente deve poter essere arricchita con informazioni contestualizzate al modulo o alla funzionalità con cui si interagisce. Ad esempio pagine, procedure operative e allarmi devono poter essere integrati con informazioni di supporto.

Diagnostica

I sistemi devono venire arricchiti di un'adeguata interfaccia grafica di diagnostica utile a monitorare il normale e corretto funzionamento. Grazie all'ausilio di variabili di "sistema", al driver SNMP e altri strumenti bisognerà poter valutare le seguenti informazioni:

- Allarmi: Numero di allarmi attivi, in attesa o riconosciuti
- Dati storici: stato della registrazione/evacuazione
- Gestione utenti: utente loggato, livelli assegnati.
- Risorse hardware sul sistema host: Memoria libera nella RAM, nel database o sul disco rigido, ecc.
- Rete: Nome del server, client collegati, componenti di ridondanza, operazione di backup dopo guasto del server, statistiche sulle prestazioni della rete
- Statistiche di connessione: Informazioni sulle prestazioni del driver, qualità della connessione dati.
- Informazioni generali sul progetto e sul sistema: posizione del progetto sul disco fisso, stato generale del sistema (attivo, simulazione ecc.), versione Runtime, nome del progetto, registrazione attivo/inattivo, diversi valori di stato di diversi moduli, informazioni di diagnosi da driver di comunicazione ecc.
- SNMP Trap: Il sistema deve essere in grado di interrogare e ricevere trappole SNMP v1, v2 e v3 per essere in grado di collegare queste informazioni nel monitoraggio centrale della rete.

Gestione variabili

Con la piattaforma software adottata è necessario avere un sistema centralizzato, semplice e flessibile in cui definire in maniera consistente e coerente tutte le variabili da utilizzare nei vari moduli così da evitare definizioni multiple dello stesso dato in ambienti differenti.

Definizione

Le variabili di comunicazione con il campo devono poter essere create in differenti modalità e parametrizzabili a seconda del loro scopo. Con la piattaforma software devono poter essere definite variabili di tipi di dato semplici (IEC data types) e variabili di tipi di dato strutturati. La creazione di array di variabili semplici o strutturate deve essere possibile così come si deve poter creare tipi di dato semplici e strutturati partendo da quelli definiti nello standard IEC.

Le caratteristiche definite nei tipi di dato delle variabili è preferibile che siano trattate come oggetti che vengono istanziati di volta in volta con le variabili, così da ottimizzare lo sviluppo ed estendere automaticamente queste informazioni a tutte le variabili dello stesso tipo. Qualora dovesse essere necessario bisogna però potersi svincolare da questo legame di ereditarietà.

Le variabili devono poter essere definite attraverso un'interfaccia grafica guidata e manuale, così come mediante meccanismi di esportazione/importazione (es. csv e xml). In particolare, ove previsto dai protocolli deve essere anche possibile importare le variabili direttamente dai dispositivi (es. Bacnet, OPC UA, 61850).

Varie facilitazioni devono essere previste per facilitare la gestione delle variabili definite. Ricerca attraverso vari filtri, utilizzo di esse all'interno del progetto, cambiamento delle proprietà in modalità singola o multipla utilizzando la selezione nativa di Windows. Supportare ordinamenti e rappresentazioni differenti potendo raggruppare le variabili con determinate caratteristiche comuni.

Visualizzazione

La qualità (online o non valida) di ogni variabile deve essere visibile immediatamente e deve essere anche possibile valutarne lo stato. Se una variabile non è valida (per esempio nessuna connessione online), il sistema deve impostare automaticamente un valore di riserva predefinito e permettere di reagire a queste condizioni ed eventualmente registrarle per scopi statistici e di diagnostica. Ogni variabile deve, oltre al valore, fornire una marca temporale (interna o esterna) e uno stato che il sistema può analizzare e reagire di conseguenza. Il sistema operativo deve avere una diagnosi online delle variabili, che rende possibile per un operatore dell'impianto di controllare la qualità dei suoi dati. Per ridurre il carico generale sulla rete, i valori numerici devono avere un valore di soglia che definisce la differenza a partire dalla quale vengono trasferite le modifiche al sistema di controllo del processo. Per ogni valore numerico devono essere possibili modifiche di valore lineari o non lineari. Ci deve essere una protezione di accesso per le variabili. Deve quindi essere possibile stabilire selettivamente l'accesso in sola lettura o in lettura-scrittura di una variabile.

Allarmi

A fronte della variazione di valore delle variabili, dovranno essere generati gli allarmi opportunamente configurati. Per ognuno di questi dovrà essere possibile configurare in maniera indipendente valori limite statici/dinamici, allarmi di minimo, massimo, con soglie e tempi di ritardo. Classificarli per gruppi, classi, aree e attraverso modelli di impianto. Per ogni gruppo di allarme, classe o area bisogna poter specificare un nome, un ID, colore, funzione e una variabile di stato che identifica se questi sono attivi o meno.

Per scopi manutentivi bisogna poter temporaneamente disabilitare in maniera selettiva gruppi di allarmi.

Il riconoscimento degli allarmi (singolo e multiplo) deve supportare due stadi, l'assegnazione di un commento e di una causa da parte dell'operatore. La rappresentazione fatta attraverso liste tabellari dovranno mostrare allarmi attivi e storici specificando queste informazioni:

- Numero di allarme (ID)
- Stato dell'allarme
- Tempo attivo
- Tempo di comparsa, riconoscimento e cancellazione
- Variabile collegata
- Testo dell'allarme
- Commenti dell'utente.
- Ulteriori informazioni come utente, nome del computer, nome gruppo/classe/area allarme

I tempi specificati devono poter essere rappresentati con granularità al millisecondo e microsecondo e per i protocolli che supportano il timestamp esterno questo dovrà essere identificato in una colonna dedicata.

Deve anche essere possibile filtrare gli allarmi secondo criteri liberamente definibili (come filtro orario/settimanale/giornaliero ecc.) - periodi di tempo, priorità, gruppi di modelli di apparecchiature e testi.

Filtrare allarmi attivi o che non sono stati riconosciuti. I rispettivi filtri devono poter essere modificati e salvati sia durante la configurazione del progetto che in Runtime per mezzo dell'HMI.

Lista eventi

Il sistema deve poter essere analizzato anche attraverso una lista eventi popolata da informazioni di varia natura, come eventi di sistema, interazioni uomo-macchina. La registrazione di tali eventi e la loro rappresentazione ricalca quanto specificato per gli allarmi con l'aggiunta di una categorizzazione degli eventi.

Modellizzazione impianto

Con la piattaforma software deve essere possibile gestire la struttura degli impianti a livello di ingegneria e runtime in conformità a quanto previsto dagli standard ISA S88 e S95. A livello di ingegneria questa funzionalità dovrà essere sfruttata per operazioni di filtro, sempre con l'intento di facilitare lo sviluppo e la manutenzione dei progetti, e a livello operativo per aggregazione di allarmi, dati e filtro degli stessi. A Runtime è auspicabile avere una finestra che mostri i vari modelli liberamente definiti durante lo sviluppo e utilizzare questa rappresentazione per le operazioni di filtro. Il filtraggio gerarchico deve essere supportato per permettere di estendere le informazioni richieste ai livelli superiori.

Archiviazione

È importante fornire un sistema che garantisca l'integrità dei dati storicizzati (allarmi, eventi, valori variabili), ed eviti che questi possano essere letti o manipolati sia intenzionalmente che accidentalmente da sistemi differenti. Questo significa che è possibile usare formati proprietari di archiviazione, binari, crittografati così da garantire la sicurezza del dato.

La condivisione di tali informazioni con sistemi di terze parti deve poter essere possibile farla in differenti modalità come file .dbf, .csv, .xml o in un database compatibile con ODBC (Open Database Connectivity).

Il modulo di archiviazione integrato deve permettere la registrazione dei dati di processo in varie modalità:

- Archiviazione ciclica
- Archiviazione ad evento
- Archiviazione spontanea (su variazione del dato). E' possibile definire un'isteresi per il singolo dato archiviato.
- Archiviazione con gestione lotti

Lo sviluppatore, attraverso un assistente di configurazione o Wizard dovrà solamente selezionare le variabili da archiviare e la modalità di registrazione. Una volta fatto basterà selezionare la profondità di archiviazione, ovvero stabilire il periodo di tempo di mantenimento dei dati e il sistema dovrà essere configurato e pronto all'uso.

Sarà importante stimare e calcolare con accuratezza lo spazio necessario a regime degli archivi configurati, permettendo un corretto dimensionamento del disco per i dati.

Se il periodo di registrazione deve essere prolungato nel tempo, il sistema può generare automaticamente degli archivi per la compressione dei dati. Il sistema può raccogliere ciclicamente dei dati campione (con tempo impostabile) prelevando valori per ciascuna variabile in archivio scegliendo tra Minimo/Medio/Massimo/Somma e generando un inserimento nell'archivio in cascata.

E' possibile definire più livelli di compressione dati per ogni archivio.

Questa funzionalità permette di migliorare la leggibilità dei dati sul lungo periodo, ottimizzare l'occupazione di spazio su disco e aumentare in modo esponenziale la velocità di rilettura dei dati utilizzando trend/report.

Quando si andrà a visualizzare un trend, il sistema andrà a selezionare l'archivio opportuno per ottenere le massime performance. Il sistema sceglierà l'archivio che più corrisponde alla quantità di dati richiesta tra l'archivio principale o gli archivi in cascata.

Nell'ottica di espansioni future, sarebbe opportuno poter integrare in aggiunta agli archivi proprietari locali dei vari sistemi installati un servizio di data storage centralizzato nel quale trasferire informazioni da poter condividere non solo tra i vari sistemi della piattaforma software adottata, ma anche con sistemi di terze parti che interagiscono attraverso un'interfaccia REST API.

Servizio di notifica (Message Control)

Il sistema deve offrire un servizio di notifica attivato da un evento. Se si verifica un evento predefinito, un messaggio deve essere inviato selettivamente a una o più persone. I possibili mezzi di trasmissione per questi messaggi sono:

- Email (via Microsoft Outlook o via SMTP)
- SMS (Short Message Service) a un telefono cellulare
- Telefono (posta vocale, Text to Speech)
- VoIP: (Voice over IP) riproduzione di file audio
- Riproduzione di testo a voce

Il servizio di notifica deve essere completamente integrato nel sistema, per garantire un controllo completo e per evitare manipolazioni da parte di fattori non autorizzati (persone, programmi esterni, ecc.).

Il destinatario dei messaggi deve essere organizzato in gruppi. Se un messaggio non può essere inviato ad una persona, ci deve essere un'opzione per informare automaticamente una persona sostitutiva. Questo deve essere supportato dalla gestione delle conferme di ricezione. Una volta che il messaggio è stato inviato, deve essere creata una voce nella lista eventi.

Deve essere possibile collegare il servizio di notifica a un programma di turni di lavoro, in modo da garantire che i messaggi siano inviati solo alle persone che sono attualmente in servizio.

Quando si invia un messaggio di posta elettronica, il sistema deve supportare l'allegato di qualsiasi file desiderato.

Process recorder

Un registratore di processo integrato nel sistema deve offrire la possibilità di registrare i dati di processo e in un momento successivo, questi dati registrati possono essere riprodotti in un client che mostrerà come una sorta di moviola quanto accaduto in precedenza. Ciò significa che la grafica dovrà essere la medesima del progetto in funzione, ma animata da dati storici anziché da dati in tempo reale. Eventuali differenze legate a versioni precedenti del progetto devono essere contestualizzate nel giusto arco temporale analizzato.

Un tale modulo consiste generalmente di due componenti:

1. Registrazione dei processi

Quando si configura un progetto nel sistema, vengono attivate le variabili per la registrazione. Queste variabili sono registrate in Runtime durante il corso del processo produttivo. Il luogo di registrazione dei dati di processo deve poter essere scelto in modo flessibile.

2. Riproduzione della registrazione

I dati registrati vengono visualizzati di nuovo in Runtime sotto forma di una simulazione del processo. La riproduzione dei valori registrati viene visualizzata nelle schermate di processo esistenti. La riproduzione è controllata utilizzando un menu operativo separato.

geographic information system (GIS)

Un modulo di integrazione GIS deve offrire la possibilità di disegnare in modo semplice oggetti in un contesto geografico e collegarli facilmente a linee, variabili e funzioni dello SCADA. In questo modo sarà possibile rappresentare la distribuzione di energie o flussi di comunicazione informatici (ICT) in un sistema in funzione della loro posizione.

Cambiando dinamicamente lo stato delle linee (es. cambio colore) e degli oggetti disegnati sulla mappa in seguito al variare di valori di variabili, il sistema sarà in grado di rappresentare in tempo reale lo stato degli impianti.

Poiché la segnalazione di messaggi o allarmi in una panoramica a larga scala offre enormi vantaggi, il sistema deve supportare la visualizzazione dinamica di un fault location sullo schermo quando un tale evento si verifica. La visualizzazione è preferibilmente implementata per mezzo di un simbolo che viene mostrato nella posizione del guasto. Inoltre, per una migliore visualizzazione, l'ambiente deve essere in grado di evidenziare graficamente il fault location verificatosi. Poiché l'operatore deve generalmente zoomare quando guarda la schermata panoramica (mappa, planimetria), è necessario mostrare gli oggetti in un funzione del livello di zoom scelto, specialmente per l'ambiente di localizzazione dei guasti.

Una notifica deve poter essere riconosciuta interagendo con il simbolo che visualizza la posizione del guasto.

L'integrazione GIS del sistema SCADA deve consentire la selezione di diversi fornitori di mappe online sia in fase di progettazione che in fase di esecuzione. Dovrà, essere possibile scegliere tra le mappe di diversi fornitori (ad esempio Open Streetmap, Google, Bing, BAIDU), ma anche tra diversi tipi di visualizzazione (mappa, vista satellitare, ecc.)

L'integrazione GIS del sistema SCADA supporta sia il recupero online dei dati delle mappe che il caching locale nei casi in cui non sia disponibile una connessione Internet. Per l'importazione di massa di marcatori,

specialmente nelle visualizzazioni di mappe, il sistema deve supportare l'importazione di file codificati in 'Keyhole Markup Language' (KML, KMZ).

Soft PLC

Il sistema deve offrire un'interfaccia di programmazione conforme allo standard IEC61131-3. I programmi implementati (cyclical task) devono poter essere eseguiti in un contesto soft PLC con tempi modificabili. Il sistema deve offrire gli aiuti necessari per la creazione di programmi, nonché strumenti di diagnosi e librerie funzionali (funzioni matematiche, funzioni combinatorie, filtri di segnale, input di comando ecc.)

Il soft PLC deve essere in grado di accedere in modo trasparente alle variabili del sistema SCADA (valore reale e informazioni di stato in tempo reale, lettura e scrittura) e ai dati ricevuti da fonti di dati esterne (tramite connessioni di comunicazione). Una connessione all'hardware attraverso I/O (segnali di ingresso/uscita) deve essere possibile. Ci deve essere la possibilità di far funzionare i progetti PLC insieme (integrati) con il sistema SCADA o individualmente come componente separato di una stazione remota.

Il componente PLC può essere usato nel funzionamento locale e remoto come stazione remota per operazioni di commutazione operazioni. Per questo, il sistema deve supportare l'esecuzione di una sequenza 'Select and Execute'.

Il soft PLC integrato deve avere connessioni dirette alle interfacce che supportano Modbus, IEC 61850 client, server e GOOSE.

L'ambiente di sviluppo deve supportare un confronto integrato tra programmi PLC. A seguito di questo confronto, i cambiamenti tra le diverse versioni di progetto, sia per i programmi testuali che per quelli grafici, devono poter essere visualizzati.

Programmazione della produzione e degli impianti

Un apposito modulo dovrà consentire di eseguire azioni (per es. modifica del valore impostabile di una variabile, esecuzione di una funzione) collegate ad un determinato intervallo di tempo o in base a un modello temporale. In questo modo deve essere possibile temporizzare e gestire gli impianti (quali ad esempio le microturbine, il sistema di caccumulo, i sistemi di condizionamento e riscaldamento, ecc…) secondo calendari, turni ed eventi liberamente definibili. Queste azioni possono essere eseguite ciclicamente, oppure una sola volta, a seconda di come sono state progettate. Vengono eseguite su tempi assoluti o relativi, in funzione di modelli temporali opportunamente preconfigurati.

Il modulo dovrà essere nativamente integrato con la piattaforma software, configurabile sia a livello editor che Runtime, utilizzabile in architetture di rete, supportando la ridondanza.

Questo tipo di esigenza, appena descritta, può ad esempio essere sfruttata per una gestione intelligente di sistemi BMS e deve quindi permettere di:

- Creare gruppi di modelli orario che contengono i relativi orari e modelli tempo.
- Configurare esecuzioni di funzione e gruppi di funzioni
- Cambiare il valore di variabili a orari e tempi definiti
- Creare turni e pause

e tenere conto di:

- Cambio ora legale/solare
- Giorni festivi
- Autorizzazioni utenti definite nei progetti

Diagnostica sistemi

Il sistema SCADA deve registrare automaticamente le informazioni di diagnostica in background per la diagnosi esterna. Ci deve essere un programma disponibile per la valutazione e l'analisi di questi file LOG, che può essere usato indipendentemente dal sistema. La diagnosi remota attraverso una connessione di rete deve essere supportata.

In caso di necessità deve essere possibile creare in automatico un pacchetto di log che racchiude tutte le informazioni rilevanti del sistema operativo e della piattaforma software SCADA per poi trasmetterli al supporto tecnico così da facilitarli nell'analisi di eventuali anomalie.

Caratteristiche energetiche

Colorazione topologica

Con lo scopo principale di realizzare velocemente e in maniera consistente lo schema unifilare degli impianti è necessario avere dei meccanismi nativi di colorazione automatica degli elementi topologici rappresentati (linee, interruttori). Lo SCADA elettrico animerà lo schema unifilare realizzato in editor (WYSISYG) calcolando e adattando il colore degli elementi topologici secondo il loro stato attuale. Questi stati possono essere ad esempio non alimentato, alimentato, (semplice, multiplo, assicurato), non valido, sconosciuto, guasto a terra o corto circuito ecc. e devono essere colorati senza ulteriore programmazione o lavoro di script.

Controllo topologia

Sulla base della definizione della colorazione topologica, il sistema deve essere in grado di offrire meccanismi di protezione (come l'interblocco dei dispositivi di commutazione, l'evitamento di stati di commutazione pericolosi, determinazione di aree non alimentate, determinazione di stati di commutazione indefiniti e allargamento di aree indefinite). Deve essere possibile inoltrare informazioni su stati di commutazione potenzialmente pericolosi all'operatore e bloccare di conseguenza determinate azioni di commutazione. Tuttavia, deve essere possibile per gli utenti autorizzati riconoscere/forzare qualsiasi condizione di interblocco desiderata.

Command processing

Il sistema deve offrire possibilità di inserimento sicuro dei comandi. Deve essere possibile configurare per ogni comando due distinte variabili, una per il comando e una per il Feedback , creando una relazione tra loro. Attraverso questa relazione sarà possibile popolare correttamente la lista eventi dello SCADA e tracciare anche l'esito del comando. Deve essere possibile configurare comandi a due fasi (con conferma), tenendo conto delle funzioni specifiche del protocollo come "Select and Execute" (IEC 60870) o "Select before Operate" (IEC 61850).

Al fine di prevenire azioni di commutazione non consentite dall'utente, viene aggiunta una logica di interblocco a ogni comando. La logica di interblocco deve essere calcolata con l'aiuto degli stati di commutazione consentiti o utilizzando lo stato topologico delle linee. Deve essere possibile configurare diversi livelli utente per ogni gestione di comando separatamente.

Tutte le azioni di comando devono essere tracciate nella lista eventi di sistema.

Il sistema deve garantire che non possano essere inviati comandi simultanei verso il campo da più PC in rete (client) contemporaneamente.

Deve poter essere semplice definire dei template di comando e applicare lo stesso modello, attraverso funzioni di indicizzazione, a molti elementi di comando, centralizzando lo sviluppo degli elementi grafici e funzionali.

Command sequencers

Il sistema SCADA deve offrire la possibilità di definire un programma delle sequenze programmabili di comando. La programmazione deve poter essere effettuata nel Runtime del sistema. Deve essere previsto

un editor grafico per la programmazione delle sequenze. Tramite la gestione utenti deve essere garantito che la sequenza comandi creata sia validata e rilasciata per poter essere utilizzata da un operatore.

La programmazione delle sequenze deve essere eseguita con un metodo teach-in, cioè un registratore di macro, mentre l'area di lavoro del sistema SCADA non è collegata al processo attivo.

Token di rete

In relazione al punto relativo al Command Processing, per aumentare la sicurezza sui comandi inviati dallo SCADA, deve poter essere possibile abilitare la funzione Token di rete. La funzione deve prevedere che esista un “gettone” (token) e che, in presenza di una rete composta da Server / Standby e n Client, solo un calcolatore possa prendere possesso del “Token” e permettere di inviare comandi verso il campo. Tramite apposite segnalazioni a video sarà possibile sapere se si è in possesso del Token, richiedere e rilasciare il token, mostrare quale PC in rete ha il token attivo.

Operating security

Il sistema deve offrire meccanismi integrati per evitare situazioni incoerenti, incontrollate e potenzialmente pericolose.

I sistemi di infrastrutture energetiche di solito rappresentano applicazioni pesantemente distribuite, le quali possono essere controllate da diverse postazioni. Per questo motivo, le situazioni conflittuali, così come le interferenze (diverse stazioni di controllo vogliono controllare la stessa sezione nello stesso frangente di tempo), devono essere evitate in ogni circostanza.

Il sistema deve anche permettere la transizione a una modalità di "manutenzione sul posto" in caso di manutenzione in loco. Di conseguenza, l'apparecchiatura in manutenzione deve essere gestita esclusivamente dalla stazione di controllo locale (stazione o pannello dedicato). Tutti i tentativi di controllare questa sezione da un punto di accesso remoto devono essere rigorosamente (in modo sicuro) rifiutati.

Il blocco e lo sblocco di un dispositivo di commutazione deve essere possibile solo da un utente autenticato e abilitato nella gestione utenti del sistema SCADA e con un determinato codice di blocco. Deve essere possibile per diversi utenti impostare un blocco sullo stesso interruttore. Se uno o più blocchi sono attivi, non è più possibile effettuare azioni di commutazione. Solo quando tutti i blocchi sono stati rimossi, il dispositivo di commutazione può essere nuovamente utilizzabile.

Ci deve essere anche la possibilità di intervenire e agire sul processo da un solo computer. Tutte le altre stazioni della rete devono rimanere online come osservatori. Se necessario, si deve essere in grado di richiedere un accesso operativo.

Funzioni di alto livello per la rete elettrica

Localizzazione guasti nella rete elettrica

Deve essere presente una funzionalità nativa che, sulla base delle informazioni disponibili dalla protezioni elettriche in campo, segnala tramite una speciale colorazione (configurata tramite il modulo di colorazione topologica) i segmenti della rete interessati da messa a terra o cortocircuito.

In caso di situazioni con un'alta probabilità di guasto a terra (come durante i temporali), deve essere possibile scollegare temporaneamente il modello topologico dal meccanismo di allarme per consentire all'utente di controllare la situazione, per esempio tramite una commutazione di prova, per verificare che ci sia effettivamente un guasto a terra. È così possibile una localizzazione più precisa dei guasti. Una volta che i controlli sono stati effettuati, l'operatore deve poter continuare con il monitoraggio e la visualizzazione degli errori basati sul modello.

La funzionalità sopra descritta deve essere gestita in maniera identica per l'analisi di eventuali corto circuiti.

Localizzazione di guasti basata su impedenza

Potrebbe essere prevista l'integrazione di dispositivi di protezione con funzionalità di localizzazione dei guasti integrata: dovrebbe essere possibile leggere il valore misurato (Ohm, km, %) della posizione del guasto e visualizzare attraverso un marker di errore la posizione corretta del guasto nello schema unifilare del sistema SCADA. È preferibile che questo modello di calcolo possa fornire anche proprietà e metodi per una valutazione esterna dei guasti e della distribuzione attraverso delle API. Durante la fase di engineering dovranno essere inseriti, nello schema unifilare le informazioni riguardanti impedenza e lunghezza della singola tratta, conoscere e stabilire i parametri di funzionamento dei cavi (corrente supportata). Il sistema dovrà , come nel caso precedente , essere alimentato da variabili provenienti dai dispositivi di protezione del campo.

Calcolo Load flow,state estimator e (N-1) calculation

Il sistema dovrebbe essere in grado di eseguire un calcolo load flow state estimator e N-1 calculation per reti elettriche trifase attraverso un tool integrato e facilmente configurabile. Il compito di un sistema di Load Flow è di ottimizzare una rete di produzione e distribuzione energia (microgrid), aiutando l'operatore in fase di conduzione ad analizzare il carico attuale della rete, ed analizzare eventuali sovraccarichi o sbilanciamenti della rete utilizzando il metodo diretto Newton- Raphson. Il calcolo N-1 può essere usato per esaminare se una rete può mantenere la qualità del servizio o altri contratti di fornitura di energia che sono regolati attraverso accordi sul livello di servizio nel caso in cui un componente della rete si guastasse. In questo caso i componenti della rete (linee e trasformatori) vengono rimossi dal calcolo uno per uno e viene ricalcolato il carico sulla rete rimanente:

- Se la linea o il trasformatore è l'unica connessione tra due bus (bridge) non c'è nessun altro componente di rete disponibile e non sono disponibili risultati

- Nel caso in cui siano disponibili connessioni multiple tra due bus, una di queste connessioni viene rimossa e il carico sui componenti di rete rimanenti viene mostrato come risultato.

Caratteristiche reportistica

Base

Il sistema SCADA deve avere un modulo per la reportistica da utilizzare per creare documentazione, l'analisi e la rappresentazione dei dati di processo basata su dati in tempo reale e dati storici locali. Questi report, liberamente definibili dall'utente, sono atti a mostrare liste di allarmi, eventi, valori degli archivi e valori online (al momento della creazione) sia in forma tabellare che grafica.

Per la creazione di questi report statistici è indispensabile avere uno strumento che faciliti la creazione attraverso una procedura guidata così da ottenere velocemente quanto desiderato. È quindi plausibile che il modulo sia nativamente integrato con la piattaforma software così da sfruttare agevolmente variabili, archivi, raggruppamenti logici (gruppi, classe, aree) e i modelli di impianto precedentemente definiti. È importante poter sfruttare come filtro anche gli stati delle variabili.

I template dei report creati attraverso il wizard è preferibile che siano editabili eventualmente anche con programmi esterni (es. Microsoft Report Builder) attraverso i quali deve essere possibile estenderne le funzionalità previste.

Avanzata

In aggiunta alle possibilità di reportistica attuabili grazie al modulo base, deve essere possibile soddisfare esigenze più complesse ed estese avendo a disposizione un modulo avanzato che sia indipendente dalla SCADA, di tipo client-server, e quindi fruibile attraverso un comune browser così da renderlo disponibile ad una platea ben più ampia. Resta inteso che lo strumento con cui creare questi report deve essere di facile apprendimento e utilizzo, evitando nella maniera più assoluta il ricorso a codice custom. I dati da poter utilizzare per i calcoli statistici devono essere sia quelli attuali (provenienti dallo SCADA) che storici (evacuati dallo SCADA al DB della reportistica) e questi devono poter essere comparati con filtri differenti in modo semplice e chiaro.

Lo strumento di reportistica desiderato fornisce modelli di report pronti all'uso, ma allo stesso tempo, consente di realizzare report personalizzati dal design grafico moderno e facilmente intuibile; permette di utilizzare la lingua preferita e di adattarli esattamente alle esigenze individuali dei membri del team coinvolti nel processo di analisi. Pertanto, occorre anche poter discriminare i report disponibili, in base al ruolo del fruitore e ai permessi attribuiti ai report pubblicati sulla piattaforma.

Il sistema deve essere scalabile e permettere analisi combinando dati provenienti anche da progetti o plessi differenti.

Le funzioni di filtro avanzate di cui dispone lo strumento di reportistica devono permettere di analizzare i dati in modo interattivo e sulla base di molteplici parametri, di seguito solo alcuni esempi:

- impianti: ad esempio, tipologia di impianto (es. fotovoltaici, microturbine, ecc…), parte della rete (quadro, ecc…)
- tempo: mese, settimana, turno, ora, da/a
- Lunghezza o numero: per es. di interruzioni o allarmi

•

E comunque in ogni caso, è importante analizzare dettagliatamente i dati facendo uso delle funzioni di drill-down e “Drill-Through”.

Caratteristiche principali

Altre caratteristiche principali che il prodotto deve possedere sono:

Indipendenza: dato che queste necessità di reportistica spesso sono legate a figure diverse da quelle coinvolte nello sviluppo e nella gestione di una SCADA, deve essere possibile utilizzare l’ambiente di sviluppo separatamente da quel contesto ed essere in grado di creare e modificare in autonomia, senza un integratore, i report desiderati.

Connettività: oltre a dover sfruttare i driver di connessione disponibili nella piattaforma SCADA, servirà dover potere attingere anche a dati presenti in database di terze parti, permettendo così una fusione dei dati mostrati nei reports prodotti. La corretta interpretazione delle tabelle di dati può essere effettuata grazie a un Wizard o manualmente. Possono essere usati Microsoft SQL Server e connessioni ODBC Server.

Pronto all‘uso e adattabile: nella piattaforma devono essere nativamente disponibili una moltitudine di template che permettono di creare rapidamente una reportistica avanzata e completa. I report sono poi modificabili in tutte le loro parti, permettendo un’analisi completa e customizzata del sistema in esame. All’utente è data anche la possibilità di crearsi template personalizzati, al fine di rendere la generazione di report personalizzati la più veloce possibile.

Web-based: per la visualizzazione dei report basta un semplice Browser, integrabile anche all’interno del supervisore. L’accesso alla pagina web permette di creare report dinamici dove con dinamici si intende che i parametri che definiscono il report (il tipo di aggregazione somma, minimo, massimo ecc), la relazione tra le singole variabili, il filtro temporale, la durata dell’aggregazione (ore, minuti, giorni, mesi, ecc)) possono essere impostati real time dall’operatore.

Generazione automatica di report: deve essere possibile creare report a evento in modo schedulato, esportandoli in Excel, Word, PDF, ecc.

Invio automatico schedulato: deve essere possibile inviare via mail o pubblicare i report in cartelle comuni a evento o in modo schedulato.

Gestione utenti: la gestione utenti può essere interna al sistema oppure sfruttando il servizio di Microsoft Active Directory.

Stampa ed esportazione: la reportistica creata può essere stampata o esportata in vari formati (PDF, html, Excel, Word, .csv, ecc.)

Aggregazione dinamica dei dati: deve essere possibile effettuare aggregazione a posteriori dei dati archiviati. I dati così aggregati possono essere utilizzati per la realizzazione di reportistica di analisi dell’impianto (consumi per ore giornaliere di luce, valutazione di curve di durate del carico giornaliero per impianto, ecc.).

Creazione di archivi con dati aggregati: inoltre deve essere possibile creare in SQL archivi di dati aggregati, sulla base dei dati non aggregati già presenti. Questi possono poi essere utilizzati per la creazione di ulteriore reportistica e analisi

Temi template

Come premesso nel paragrafo precedente è mandatorio che siano presenti numerosi template che possano facilitare e velocizzare la distribuzione nella piattaforma dei report desiderati. Questi template dovrebbero poter soddisfare le seguenti tipologie di analisi.

- Analisi di allarmi ed eventi
- Analisi con formule personalizzate
- Analisi classi di efficienza
- Analisi gestione dati energetici
- Analisi estese dati storici
-
- ISO 50001 (es. carpet plot, Sankey, ecc. Ecc.)
- Analisi predittiva
- Analisi OEE
- Analisi statistiche
- Analisi obbiettivi attuali
-

Di seguito alcuni template spiegati in dettaglio:

- Analisi Allarmi: contiene una collezione di report per la rappresentazione diretta o aggregata di dati riguardanti gli allarmi. I report in questa classe consentono di eseguire analisi statistiche degli allarmi, permettendo di eseguire inoltre un'aggregazione di allarmi parametrizzabile. Le analisi vengono poi presentate sotto forma di tabelle o in modo grafico.

- Analisi con Formule Personalizzate: I modelli di report di questo tema permettono di implementare formule personalizzate di analisi, consentendo una piena libertà in termini di correlazione di dati e funzioni di aggregazione. I risultati vengono poi visualizzati in grafici e tabelle.

- ISO 50001: dovranno essere previsti report speciali per far fronte alle esigenze legate ai Sistemi di Gestione dell'Energia, come per esempio il Diagramma di Sankey, la Curva di Durata del Carico, il Carpet Plot e il Diagramma di Gantt. Tutto ciò per permettere una visualizzazione grafica completa dei consumi energetici e aiutare ad individuare i potenziali di risparmio.

- Il Diagramma di Sankey permette di visualizzare in maniera chiara, i flussi delle risorse come per esempio il consumo di elettricità. Il diagramma può essere facilmente configurato tramite un wizard che offre molte possibilità di visualizzazione grafica.

- La Curva di Durata del Carico permette di visualizzare i consumi di tutto l'anno sotto forma di line chart o area chart. Il filtro tempo può essere configurato liberamente; possono essere usati i valori di media, minimo o massimo.

- Il Carpet Plot permette di visualizzare valori misurati in un report cronologico e facilita l'individuazione di irregolarità e la possibilità di ottimizzazioni..

- Il Diagramma di Gantt fornisce dettagli sulle performance e sulla disponibilità dell'impianto o parti di esso.

- Analisi Obiettivo – Effettivo: i report di questo tema permettono di eseguire un confronto tra i valori target di alcune grandezze con i loro valori effettivi. I valori target possono essere letti da archivi esterni o attribuiti direttamente alle singole variabili.

- Analisi OEE: I modelli report di questo tema calcolano gli indicatori di efficienza generale di impianto. Questi indicatori includono analisi dell'indice OEE (Overall Equipment Effectiveness), prestazioni, disponibilità e qualità.

- Analisi di dati archiviati: questa classe di modelli di report è una collezione di report per la rappresentazione diretta o aggregata di dati storici, permettendo di associare ai dati storici valori di prezzo, contatori di produzione, valori standard e modelli di impianto. I dati possono essere poi rappresentati in modo grafico o in formato tabellare.

-

-

Analisi predittiva

Ultimo, ma non per importanza, occorre avere una piattaforma che permetta di effettuare delle analisi predittive anche con strumenti informatici che si prestano a tale scopo e che oggi giorno sono largamente utilizzati sia in ambito accademico che industriale. Ciò significa che oltre agli strumenti e funzionalità nativamente integrate a raggiungere tali scopi, viene richiesta la possibilità di potersi interfacciare in modo bidirezionale a linguaggi di programmazione Python e interfacce REST API. I risultati di tali analisi potrebbero poi confluire, una volta rielaborati, nel modulo di reportistica o addirittura a livello di SCADA.

Condivisione dati vs terzi (Process Gateway)

Per differenti attività di ricerca è necessario poter condividere facilmente dati in tempo reale e storici residenti nello SCADA tramite OPC UA Server, Rest API, SQL, etc..

Il sistema sarà utilizzato per l'inoltro di dati da sistemi di livello inferiore a sistemi di livello superiore e viceversa (funzionalità gateway). Per questo motivo, il sistema deve essere in grado di stabilire connessioni di comunicazione con sistemi di livello superiore utilizzando i seguenti standard di comunicazione:

- OPC UA Server

o Il gateway offre OPC UA Data Access a variabili configurabili di connessioni a valle variabili interne in direzione di lettura o di scrittura.

o Il gateway espone un accesso OPC UA alle variabili dell'Historian

o Il gateway espone allarmi OPC UA allarmi ed eventi

o Il gateway espone l'accesso allo storico allarmi ed eventi

o Il gateway offre l'autenticazione OPC UA dall'utente

o Il gateway offre la modalità di autenticazione OPC UA Sign and Sign&Encrypt

- REST API

o Dati in tempo reale, allarmi ed eventi

o Dati storici, allarmi ed eventi

o Trasmissione dati in sicurezza (TLS, SSL, certificati digitali, autenticazione richiesta)

o Comandi (ad esempio set point)

- MODBUS Slave