REGIONE MARCHE

PROVINCIA DI FERMO

COMUNE DI FERMO

IMPIANTO DI TRATTAMENTO ANAEROBICO DELLA FRAZIONE ORGANICA DEI RIFIUTI SOLIDI URBANI PER LA PRODUZIONE DI BIOMETANO

CIG: 9880245C18 – CUP: F62F18000070004

PROGETTO ESECUTIVO

NOME ELABORATO

RELAZIONE IMPIANTO DI AUTOMAZIONE E GESTIONE

CODIFICA ELABORATO	**23008-OW-C-81-RS-011-HA1-1**

CLASSE **8.1**

IMPIANTO AUTOMAZIONE E CONTROLLO - RELAZIONI

N. TAVOLA **8.1.1**

FORMATO **A4**

SCALA **/**

REV	DATA	DESCRIZIONE	ESEGUITO	VERIFICATO	APPROVATO
01	19/12/2024	SECONDA EMISSIONE	F. MOCCIARO	C. BUTTICE'	R. MARTELLO
00	25/09/2024	PRIMA EMISSIONE	F. MOCCIARO	C. BUTTICE'	R. MARTELLO

Committente

CITTA' DI FERMO
Settore IV e V
Lavori Pubblici, Protezione Civile, Ambiente, Urbanistica, Patrimonio, Contratti e Appalti
Via Mazzini 4
63900 – Fermo (FM)

DOTT. **Mauro Fortuna**
RUP

Progettista indicato

OWAC ENGINEERING COMPANY

Via Resuttana 360
90142 -PALERMO

OWAC Engineering Company S.R.L
ING. **Rocco Martello**
Direttore Tecnico

UNI EN ISO 9001:2015 N. 30233/14/S
UNI EN ISO 45001:2018 N. OHS-4849
UNI EN ISO 14001:2015 N. EMS-9477/S
UNI/PDR 74 :2019 N. SGBIM-01/23
UNI/PdR 74:2019 N. 21042BIM

Mandataria

EdilAlta

Via del Cardoncello 22
70022 – Altamura (BA)

EDILALTA S.R.L.
DOTT. **Angelantonio Disabato**
Socio

Mandante

Anaergia
Fueling a Sustainable World

Via Bassa di Casalmoro 3
46041 – Asola (MN)

ANAERGIA S.R.L.
DOTT. **Andrea Parisi**
Institore

Sommario

1. DESCRIZIONE DEL PROGETTO OGGETTO DELL'OPERA

1.1. PREMESSA

La presente relazione è relativa al sistema di automazione e gestione dell'impianto di trattamento anaerobico della FORSU per la produzione di biometano, localizzato in C.da San Biagio del Comune di Fermo, in prossimità del Centro Integrato per la Gestione dei Rifiuti Urbani (CIGRU) gestito dalla società Fermo Asite S.r.l., ed autorizzato con Determina n. 61 del 31/01/2022 e s.m.i. del Settore III della Provincia di Fermo.

Lo scopo di questo documento è fornire una descrizione completa di tutte le informazioni necessaria a sviluppare la progettazione esecutiva del sistema di automazione e controllo del processo di digestione anaerobica finalizzata alla produzione di biometano.

La digestione anaerobica è un processo biologico di degradazione del substrato organico in assenza di ossigeno libero. La degradazione avviene ad opera di batteri che ottengono l'ossigeno necessario per le loro funzioni vitali a partire dalla biomassa.

L'impianto sarà realizzato in c.da San Biagio in continuità con l'attuale impianto di smaltimento rifiuti C.I.G.R.U. gestito dalla FERMO ASITE.

In sintesi l'impianto rappresenta l'implementazione e l'efficientamento del CIGRU con particolare riferimento alla minimizzazione degli impatti legati al trattamento delle matrici organiche; l'impianto prevede infatti:

- Il pre-trattamento della FORSU conferita al fine di rendere il rifiuto compatibile con i successivi trattamenti;
- La digestione anaerobica delle matrici organiche del rifiuto per la produzione di biogas;
- Il post-trattamento del digestato prodotto, al fine di ottenere acqua depurata da un lato (tramite l'impianto di depurazione *in situ* previsto) e fertilizzanti conformi alla normativa italiana ed europea dall'altro lato;
- Il post-trattamento del biogas per la produzione di biometano, da utilizzare nel settore dei trasporti tramite compressione su carri bombolai.

L'impianto, con una potenzialità di trattamento di 35.000 t/anno di FORSU, consente la produzione di circa 3.000.000 m^3/anno di biometano e circa 6.000 t/anno di fertilizzanti.

Nel seguito si riportano le metodologie e le elaborazioni effettuate per il dimensionamento delle opere idrauliche dell'impianto (reti di raccolta delle acque meteoriche, vasca di prima pioggia, opere per l'invarianza idraulica, ecc.).

1.2. NORMATIVA DI RIFERIMENTO

La progettazione dell'impianto elettrico e di automazione deve essere eseguito tenendo presenti la seguenti normative:

- Legge n. 186/1968
- D.Lgs. 81/08 In materia di tutela della salute e della sicurezza nei luoghi di lavoro, integrato dal D.Lgs. 106/09
- Legge 18.10.1977 n. 791 " Attuazione della direttiva CEE relativa alle garanzie di sicurezza che deve possedere il materiale elettrico destinato ad essere utilizzato entro alcuni limiti di tensione".
- Direttiva Bassa Tensione 73/23 CEE
- Direttiva compatibilità elettromagnetica 89/336 CEE
- Immunità alle interferenze secondo EN50082-2 (95)
- Emissioni di interferenze secondo EN50081-2 (94) Le norme tecniche seguite sono quelle dei Comitato Elettrotecnico Italiano, e in particolare:
- CEI 64-8 (2012-06): Impianti elettrici utilizzatori a tensione nominale non superiore a 1000V in corrente alternata ed a 1500 V in corrente continua.
- CEI 11-1: Impianti di produzione, trasmissione e distribuzione di energia elettrica.
- CEI C.T. 3 Segni grafici (tutte le norme)
- CEI 17-13 Apparecchiature assiemate di protezione e di manovra per bassa tensione. (Quadri B.T.)
- CEI 81-10/1: "Principi generali"

- CEI 81-10/2: "Valutazione del rischio"
- CEI 81-10/3: "Danno materiale alle strutture e pericolo per le persone"
- CEI 81-10/4: "Impianti elettrici ed elettronici interni alle strutture"
- CEI 0-2 Guida per la definizione della documentazione di progetto degli impianti elettrici.
- CEI EN 55011 - Apparecchi industriali, scientifici e medicali - Caratteristiche di radiodisturbo - Limiti e metodi di misura
- CEI EN 55022 - Apparecchi per la tecnologia dell'informazione - Caratteristiche di radiodisturbo - Limiti e metodi di misura
- CEI EN 61000-6-2 - Compatibilità elettromagnetica (EMC) - Parte 6-2: Norme generiche - Immunità per gli ambienti industriali
- CEI EN 61000-6-4 - Compatibilità elettromagnetica (EMC) - Parte 6-4: Norme generiche - Emissione per gli ambienti industriali
- CEI EN 61000-4 - Compatibilità elettromagnetica (EMC) - Part 4: Parte 4: Tecniche di prova e di misura
- CEI EN 61386-21 - Sistemi di tubi e accessori per installazioni elettriche - Parte 21: Prescrizioni particolari per sistemi di tubi rigidi e accessori
- CEI EN 60068-3-3 Metodi di prova sismica per apparecchiature.
- CEI EN 60068-2-6 Prove ambientali. Parte 2: Prove - Prova Fc: Vibrazioni (sinusoidali).
- CEI EN 60068-2-57 Prove climatiche e meccaniche fondamentali. Parte 2-57: Prove - Prova Ff: Vibrazioni - Metodo con oscillogrammi.
- CEI EN 61587-2 Strutture meccaniche per apparecchiature elettroniche - Prove per la IEC 60917 e IEC 60297 - Prove sismiche per armadi e telai.
- CEI EN 61131 - Controllori programmabili
- CEI EN 60654-1 - Condizioni di funzionamento per apparecchi di misura e di controllo nei processi industriali - Parte 1: Condizioni climatiche
- CEI EN 61069 - Controllo e misura dei processi industriali - Valutazione delle proprietà di un sistema per un suo accertamento

- CEI EN 61508 - Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza
- CEI EN 61511 - Sicurezza funzionale - Sistemi strumentali di sicurezza per il settore dell'industria di processo
- CEI EN 61158 - Reti di comunicazione industriali - Specificazioni del bus di campo
- CEI EN 62382 - Verifica della funzionalità elettrica e dei collegamenti fra strumenti
- CEI EN 60770 - Trasmettitori impiegati nei sistemi di controllo dei processi industriali
- CEI EN 60534 - Valvole di regolazione nei processi industriali
- CEI EN 60987 - Centrali elettronucleari - Strumentazione e controllo importanti per la sicurezza - Prescrizioni per la progettazione hardware di sistemi computerizzati
- CEI EN 60880 - Centrali elettronucleari - Strumentazione e controllo importanti per la sicurezza - Aspetti software di sistemi computerizzati che elaborano funzioni di categoria A
- CEI EN 62138 - Centrali elettronucleari - Strumentazione e controllo importanti per la sicurezza - Aspetti software di sistemi computerizzati che elaborano funzioni di categoria B o C
- CEI EN 61226 - Centrali elettronucleari - Strumentazione e controllo importanti per la sicurezza - Classificazione delle funzioni di strumentazione e di controllo
- CEI EN 50262 - Pressacavo metrici per installazioni elettriche
- CEI EN 60352-2 - Connessioni senza saldatura- Parte2 - connessioni aggraffate
- CEI EN 60512 - Connettori per apparecchiature elettroniche
- CEI EN 60529 - Gradi di protezione degli involucri (Codice IP)
- CEI EN 60664 - Coordinamento dell'isolamento per le apparecchiature nei sistemi a bassa tensione
- CEI EN 61034-1 - Misura della densità del fumo emesso dai cavi che

bruciano in condizioni definite

- CEI EN 50267-2-1 - Metodi di prova comuni per cavi in condizioni di incendio Norme IEC e, in particolare:
- IEC 61513 - Nuclear Power Plants - I&C for Systems Important to Safety – General requirements for systems.
- IEC 60780 (CEI 45-60) - Nuclear Power Plants – Electrical equipment of the Safety System - Qualification.
- IEC 60980 (CEI 45-62) - Recommended practices for seismic qualification of electrical equipment of the Safety System for nuclear generating stations Direttive Europee, Leggi e Decreti e, in particolare:
- DIRETTIVA "BASSA TENSIONE" 2006/95/CE del parlamento europeo e del consiglio e successive modifiche e aggiornamenti
- DIRETTIVA "COMPATIBILITA' ELETTROMAGNETICA - EMC" 2004/108/CE del parlamento europeo e del consiglio e successive modifiche e aggiornamenti
- Legge 186/68: Disposizioni concernenti la produzione di materiali, apparecchiature, macchinari installazioni e impianti elettrici ed elettronici"
- D.LGS 81/08 - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro
- Decreto 22 gennaio 2008, n. 37 - Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività' di installazione degli impianti all'interno degli edifici (ex 46/90) e s.m. e i.
- Decreto del M.I. del 10 marzo 1998, Criteri generali di sicurezza antincendio e per la gestione dell'emergenza nei luoghi di lavoro
- Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio (NIS2), recante misure per la sicurezza delle reti e dei sistemi IT e OT

1.3. DOCUMENTI DI RIFERIMENTO IN PROGETTO

All'interno del presente documento verrà esposta una descrizione dettagliata e

completa di tutte le informazioni tecniche necessarie a sviluppare il sistema software di controllo e automazione dell'impianto di digestione anaerobica da FORSU.

Per I dettagli sui dispositivi e sulle parti specifiche riferirsi ai documenti tecnici che seguono:

- 8.2.1-23008-OW-C-82-DD-034-HA7-0-PLANIMETRIA GENERALE LAYOUT STRUMENTAZIONE IN CAMPO
- 8.2.2-23008-OW-C-82-DD-037-HA4-1-SCHEMA A BLOCCHI RETE DATI

1.4. ACRONIMI

CPU	Unità di processo principale di un controllore logico programmabile
DCS	Sistema di Controllo Distribuito
RIO	Unità di controllo remoto Ingressi/uscite del DCS
RTU	Unità Terminale Remota (Remote Terminal Unit)
SCADA	Software di Supervisione, Controllo ed Acquisizione Dati
ETHERNET	Standard ISO/IEC7IEEE per il trasferimento dati
HMI	Interfaccio operatore (Human Machine Interface)
I/O	Ingressi e Uscite
LAN	Local Area Network
TCP/IP	Protocollo di collegamento dati (Transmission Control Protocol/Internet Protocol)
PID	Regolatore con azione Proporzionale, Integrativa e Derivativa.
PLC	Controllore Logico Programmabile
SCD	Sistemi di Controllo Dedicati
SRV	Server
UPS	Gruppo di Continuità (Uninterruptible Power System)
TVCC	Telecamere a Circuito Chiuso
SIL	Livello di sicurezza (Safety Integrity Level)

WKS WorkStation

CAMPO Strumenti, sensori, attuatori e quadri elettrici

Bus di CAMPO Bus di Campo (FieldBus) è il termine fissato in ambito IEC per indicare, in un processo automatizzato, lo standard di comunicazione "seriale" tra il DCS e I diversi dispositivi costituenti il processo quali strumentazioni, attuatori, inverter, sensori, schede di I/O remote e altri dispositivi elettronici a microprocessore.

2. DESCRIZIONE GENERALE IMPIANTO

2.1. INFRASTRUTTURA IT

L'intero impianto di supervisione e controllo (automazione, building automation, monitoraggio consumi, etc.) utilizza un software SCADA principale ed è progettato e concepito per consentire la piena integrazione ed interfacciabilità di tutte le macchine ed apparecchiature presenti nel sito.

Sarà presente un'unica infrastruttura di comunicazione di rete (cablata in fibra ottica/rame/wireless) a cui tutti I quadri package, le apparecchiature e sistemi informatizzati faranno capo, fermo restando le necessità operative mirate alla segmentazione della rete utile a garantire un alto standard di isolamento.

Anche a tale scopo si farà uso di HOST VIRTUALI (da opa in poi VH) utili a garantire l'operatività d'impianto ed a razionalizzare l'eventuale accesso dall'esterno, ai fini manutentivi e/o di intervento, da parte dei fornitori. L'hardware e il software del sistema saranno collaudati sul campo e aggiornati rispetto la data di emissione del presente documento. Il sistema deve consentire le massime possibilità di aggiornamento hardware e software. La modularità del sistema e la logica di progettazione devono salvaguardare l'architettura originale, anche in caso di future modifiche del sistema.

L'apparato VH sarà in grado di funzionare, in caso di guasto all'impianto di condizionamento, a una temperatura compresa tra 0° C e 50° C con un'umidità del 70% (non condensate). Le condizioni ambientali saranno prese in considerazione per il normale funzionamento del sistema (24°C ± 2°C) ad un'umidità relativa del 60%. I rack offriranno protezione contro le comuni interferenze industriali a radiofrequenza ed elettromagnetiche previste nell'ambiente e saranno conformi alla

norma IEC 61000-4.

I VH saranno alimentati tramite due linee, 240V, 50Hz derivate dal sistema UPS, mentre i sistemi ausiliari dei rack per i VH (ventilatori, sistema di raffreddamento, lampade, etc.) saranno alimentati da una linea 230V, 50Hz a sorgente non privilegiata.

Il collegamento con i sistemi remoti sarà realizzato considerando una tipologie di fibra multimodale 50/125 micron OM4 per distanze fino a 2 km e monomodale 9/125 micron per distanze superiori a 2km.

Anche I sistemi bus per la gestione dell'illuminazione o quelli per la domotica generale saranno comunque dotati di gateway IP che li renderanno interrogabili e comandabili all'interno della stessa infrastruttura IT.

La progettazione delle opere e stato effettuata tenendo conto di tutte le esigenze impiantistiche inerenti a:

- Tipologia di strumentazione da controllare (analogica, digitale o seriale)
- Motori elettrici da controllare e/o comandare
- Valvole motorizzate da controllare e/o comandare
- Valvole pneumatiche da controllare e/o comandare
- Package da visualizzare
- Connessioni seriali da visualizzare, controllare/comandare

La reale tipologia degli impianti è quella risultante dalla presente relazione tecnica e dagli elaborati di progetto allegati.

2.2. AVAILABILITY

L'obiettivo di questa fornitura è aumentare il più possibile la percentuale di disponibilità annuale dei servizi OT e portare la disponibilità di almeno tutti i server di processo al livello "cinque nove" (99,999%).

2.3. CYBERSECURITY

Ogni dispositivo OT che produce e gestisce dati deve essere configurato in conformità ai principi e alle misure di controllo previsti dal National Framework for

Cybersecurity and Data Protection, nonché rispetto alla recente Direttiva (UE) 2016/1148 del Parlamento europeo denominata NIS2.

Come requisito generale relativo ai sistemi operativi Windows, l'uso del protocollo SMB deve essere evitato per qualsiasi VM configurata. La finalità ed i vantaggi di una progettazione NIS2 compliant sono riconducibili principalmente ai seguenti punti:

- Salvaguardia della vita umana;
- Protezione dei dati (anche storici) e dei flussi di dati;
- Business continuity dell'operatività IT e OT;

L'approccio alla gestione della sicurezza informatica prevede l'integrazione tra sicurezza predittiva, preventiva e proattiva. La sicurezza predittiva si sviluppa attraverso l'attività di Threat Intelligence, e consiste nella raccolta e analisi di dati per identificare in anticipo le minacce potenziali o effettive all'infrastruttura IT e OT; la sicurezza preventiva agisce in termini di analisi del rischio tecnologico, umano e di processo. La sicurezza proattiva permette l'adozione degli approcci relativi alla security by detection e alla security by reaction.

2.4. SEGMENTAZIONE DELLE RETI IT E OT

Questo approccio è essenziale per evitare che minacce informatiche che colpiscono la rete IT possano propagarsi ai sistemi di controllo industriale (OT), che gestiscono processi critici. La segmentazione è ottenuta tramite una combinazione di separazione fisica delle reti e protezioni logiche (come firewall e segmentazione VLAN).

- Rete IT: Include i sistemi aziendali, come i server per l'elaborazione dei dati, i NAS per il backup, e i dispositivi di accesso remoto sicuri. Questa rete può essere connessa a Internet per supportare le attività aziendali, come l'accesso al cloud e la gestione amministrativa. Tuttavia, tutte le connessioni tra la rete IT e la rete OT devono passare attraverso firewall e sistemi di monitoraggio IDS/IPS per garantire che solo il traffico autorizzato possa transitare tra le due reti.

- Rete OT: Comprende tutti i dispositivi e i sistemi che controllano i processi industriali, come i PLC (Programmable Logic Controllers), i DCS (Distributed Control System), i sistemi SCADA e i dispositivi sul campo (sensori, attuatori, HMI). La rete OT deve essere segmentata ulteriormente al suo interno per garantire che un potenziale attacco non possa compromettere l'intera infrastruttura.

La segmentazione rigorosa tra IT e OT ha la finalità di ridurre la superficie di attacco e minimizzare le possibilità che un'intrusione nella rete IT possa influenzare i sistemi OT ed evitare, in tal modo, i cosiddetti "movimenti laterali" di un attacco informatico.

Firewall e Sistemi IDS/IPS

I firewall svolgono un ruolo cruciale nel bloccare il traffico non autorizzato e garantire che solo gli utenti e i dispositivi legittimi possano accedere ai sistemi OT. I firewall devono essere configurati per segmentare fisicamente le reti e filtrare il traffico basato su protocolli sicuri e regole di accesso prestabilite.

Oltre ai firewall, l'architettura di cybersecurity deve includere sistemi di Intrusion Detection (IDS) e Intrusion Prevention (IPS). Questi sistemi monitorano costantemente il traffico di rete alla ricerca di attività anomale o comportamenti sospetti, come tentativi di accesso non autorizzato o trasferimenti di dati insoliti. Gli IDS sono passivi e registrano gli eventi sospetti per successiva analisi, mentre gli IPS sono attivi e possono bloccare in tempo reale gli attacchi rilevati.

IDS e IPS sono strumenti critici per la protezione in tempo reale della rete industriale da minacce informatiche. Sistemi come Snort o Suricata possono essere utilizzati per monitorare il traffico in tempo reale (PCAP - packet capture), individuare anomalie e agire tempestivamente. L'integrazione con i firewall consente una protezione multilivello. Questi software includono, tra le altre, alcune funzionalità come il Multithreading, network-based intrusion detection systems (NIDS) e intrusion prevention systems (IPS).

Autenticazione e Accesso Sicuro

L'accesso ai sistemi OT deve essere ristretto e consentito solo a personale autorizzato, seguendo una politica di least privilege (minimo privilegio), che garantisce che gli utenti abbiano accesso solo ai sistemi e ai dati necessari per il loro ruolo. Tutti gli accessi remoti devono avvenire tramite VPN sicure che cifrano il traffico e garantiscono l'integrità dei dati. L'accesso remoto deve essere concesso solo previa autenticazione forte, come l'autenticazione multifattoriale (MFA), che richiede una combinazione di più fattori (password e token, oppure impronte digitali e chiavi di sicurezza). La gestione degli accessi deve essere basata su ruoli e responsabilità (RBAC - Role-Based Access Control). Gli amministratori di rete e il personale tecnico devono avere accesso a determinate risorse e funzioni, mentre l'accesso ai dati sensibili deve essere strettamente limitato. Questo garantisce che solo il personale strettamente autorizzato possa accedere a dati critici e funzioni chiave dell'impianto.

Monitoraggio e Logging

I log devono essere conservati e analizzati regolarmente per individuare eventuali attività anomale. L'adozione di sistemi SIEM (Security Information and Event Management) consente di centralizzare e analizzare i log provenienti da diversi dispositivi (firewall, IDS, server). Gli eventi sospetti vengono classificati e segnalati in tempo reale, consentendo interventi tempestivi.

Il monitoraggio continuo è una componente imprescindibile, che garantisce l'opportunità di rispondere prontamente a potenziali minacce e fornire report dettagliati in caso di violazione della sicurezza.

Cifratura dei Dati

I dati scambiati tra la rete IT e la rete OT, così come i dati trasmessi via VPN o conservati nei sistemi di backup, devono essere protetti da cifratura avanzata. La cifratura end-to-end garantisce che i dati siano leggibili solo da destinatari autorizzati, rendendo difficile l'intercettazione e la manipolazione da parte di attori malevoli.

2.5. PIANO DI BACKUP E RIPRISTINO

Il Piano di Backup è una componente critica per la sicurezza e la resilienza del sistema industriale, è essenziale garantire che i dati critici e le configurazioni dei sistemi siano protetti contro guasti, attacchi informatici o errori operativi.

Un backup efficace deve prevedere la copia e la protezione di tutti i dati chiave, inclusi:

• Configurazioni dei PLC e SCADA: Parametri operativi, logiche di controllo, e impostazioni di rete devono essere salvati regolarmente, dato che eventuali modifiche non documentate o perdite di configurazione possono compromettere l'intero processo di automazione.

• Dati di processo e di produzione: I dati storici riguardanti la produzione, come le quantità di biogas e biometano prodotti, devono essere regolarmente salvati per poter monitorare l'efficienza del processo nel tempo.

• Backup delle infrastrutture IT e OT: I sistemi di gestione e supervisione, come i server che ospitano il SCADA e il DCS, devono essere inclusi nel piano di backup per garantire che eventuali guasti possano essere ripristinati senza perdita di dati critici. Un buon piano di backup si basa su diverse strategie di backup per garantire la massima protezione e disponibilità dei dati:

• Backup completo che crea una copia completa di tutti i dati e configurazioni del sistema a cadenza mensile;

• Backup incrementale che copia solo i dati che sono stati modificati o aggiunti dall'ultimo backup completo o incrementale a cadenza giornaliera.

Strategia di Archiviazione

Si è scelto di adottare una strategia di archiviazione che assicuri la protezione e la disponibilità dei dati anche in caso di guasti hardware o attacchi informatici:

• NAS (Network Attached Storage): I dati di backup dovrebbero essere salvati su sistemi NAS, dispositivi di archiviazione collegati alla rete che offrono una piattaforma centralizzata e sicura per la gestione dei backup. Questi sistemi devono essere ridondanti, con dischi in configurazione RAID per garantire che eventuali guasti hardware non compromettano la disponibilità dei dati.

• Backup off-site: Una copia dei backup dovrebbe essere conservata off-site (fuori dal sito), idealmente in una struttura cloud o in un data center remoto, per proteggere i dati da eventi fisici come incendi o calamità naturali che potrebbero colpire l'impianto.

Backup e Ripristino dei Sistemi SCADA e DCS

I sistemi di automazione e controllo (SCADA e DCS) sono il cuore del funzionamento dell'impianto, si prevede un piano di backup dedicato per questi sistemi:

• Backup delle configurazioni di rete e dei dispositivi: I parametri di rete, come gli indirizzi IP dei dispositivi, le configurazioni dei firewall, e le impostazioni dei server di supervisione;

• Backup periodico del database SCADA: Il database SCADA, che contiene i dati di monitoraggio e di produzione, deve essere copiato e archiviato a cadenza giornalira;

• Backup delle logiche PLC: Le logiche di controllo dei PLC, che gestiscono i processi operativi dell'impianto, devono essere salvate sia localmente sui server OT che nel sistema di backup off-site.

Tempi di Ripristino (RTO) e Obiettivo del Punto di Ripristino (RPO)

Il piano di backup include anche i tempi di ripristino e il punto temporale da cui ripristinare i dati per garantire la continuità delle operazioni in caso di guasto.

• RTO (Recovery Time Objective) rappresenta il tempo massimo accettabile per il ripristino del sistema dopo un guasto. Per i sistemi critici come SCADA e PLC, l'RTO viene fissato a 2 ore per ridurre al minimo i tempi di inattività dell'impianto.

• RPO (Recovery Point Objective) definisce l'intervallo massimo di dati che

possono essere persi in seguito a un guasto. Idealmente, il sistema dovrebbe garantire un RPO di 30 minuti, assicurando che al massimo solo i dati prodotti in questo lasso di tempo possano essere persi. Questo obiettivo può essere raggiunto attraverso backup incrementali frequenti e sistemi di archiviazione in tempo reale.

Piano di Disaster Recovery

Il Piano di Disaster Recovery descrive le azioni da intraprendere per ripristinare rapidamente i sistemi critici in seguito a un guasto o un attacco informatico.

Grazie al sistema di monitoraggio che identifica rapidamente un guasto (ad esempio, un crash di un server SCADA, incendio, inondazione) o un attacco informatico. Gli incidenti devono essere classificati in base alla gravità e all'impatto sui processi produttivi, con una chiara scala di priorità: Alta, Media, Bassa. Una volta identificato l'incidente, il passo successivo è l'isolamento del problema per impedire ulteriori danni. Ad esempio, nel caso di un attacco informatico, il traffico di rete sospetto deve essere bloccato immediatamente tramite il firewall e i sistemi IDS/IPS. Nel caso di un guasto hardware, i sistemi colpiti devono essere scollegati per evitare propagazioni di guasti (ad esempio, danni ai server di backup).

La fase successiva prevede il ripristino dei dati dai backup più recenti. Se si tratta di dati di produzione o di configurazioni SCADA, è fondamentale utilizzare backup validati e testati. Il ripristino deve essere eseguito in ordine di priorità: prima i sistemi critici come SCADA e PLC, poi i sistemi IT secondari. Nel caso di ripristino di un sistema critico come il DCS, i tecnici devono verificare che tutti i sensori, attuatori e le logiche di controllo siano operative prima di riportare l'impianto in produzione. Dopo il ripristino, tutti i sistemi devono essere verificati e sottoposti a test di funzionalità per garantire che siano stati ripristinati correttamente e siano operativi. I log del sistema devono essere controllati per assicurarsi che non vi siano errori o avvisi critici.

Una volta risolto l'incidente, è importante condurre una post-mortem analysis per comprendere l'origine del problema, valutare l'efficacia del piano di recovery e individuare aree di miglioramento. Questo feedback aiuterà a ottimizzare i futuri piani di disaster recovery e ridurre ulteriormente il rischio di downtime.

Test Periodici del Piano di Disaster Recovery

I piani di disaster recovery andranno testati regolarmente per garantire la loro efficacia in situazioni reali e per consentire al personale incaricato di aumentare il grado di consapevolezza e confidenza con le procedure necessarie. I test dovrebbero includere simulazioni di scenari di guasto (ad esempio, crash del sistema SCADA) per verificare che il personale e i sistemi siano pronti a ripristinare l'operatività entro gli obiettivi RTO e RPO definiti.

2.6. INCIDENT RESPONSE PLAN (PIANO DI RISPOSTA AGLI INCIDENTI)

Un Incident Response Plan (IRP), o Piano di Risposta agli Incidenti, è fondamentale per minimizzare i danni causati da attacchi informatici, malfunzionamenti hardware o software, o da errori umani, garantendo nel contempo la continuità operativa, l'integrità, la disponibilità o la riservatezza dei sistemi IT e OT.

Fasi Principali del Piano di Risposta agli Incidenti

Il piano di risposta agli incidenti è suddiviso in sei fasi che permettono di rilevare e gestire un incidente in maniera rapida ed efficace. Di seguito una descrizione dettagliata delle fasi:

1. Preparazione

La fase di preparazione è una delle più importanti del ciclo di gestione degli incidenti, poiché stabilisce le basi per affrontare le emergenze. L'obiettivo è garantire che l'organizzazione sia pronta a reagire rapidamente e in maniera efficace a qualsiasi incidente informatico. Questa fase prevede la formazione del personale su come riconoscere e rispondere a un incidente, la formazione deve riguardare non solo gli operatori tecnici, ma anche il personale non IT che potrebbe rilevare comportamenti anomali; questa considerazione ammette la definizione di ruoli e responsabilità come ad esempio, alcuni membri saranno responsabili del rilevamento, altri dell'isolamento del problema e altri ancora della comunicazione con le autorità.

Gli strumenti di monitoraggio e rilevamento (sistemi IDS/IPS), firewall, e strumenti

di monitoraggio dei log devono essere configurati e ottimizzati per rilevare attività sospette in tempo reale. È importante che il team di risposta abbia familiarità con questi strumenti e sappia utilizzarli correttamente. A tal fine eseguire test e simulazioni periodiche aiuta a identificare eventuali punti deboli nel piano di risposta e a migliorare la prontezza operativa in caso di incidente reale. Questi test devono simulare scenari di attacchi informatici o guasti ai sistemi di automazione.

2. Rilevamento e Identificazione

La fase di rilevamento è fondamentale per identificare tempestivamente un incidente di sicurezza informatica e attivare il piano di risposta. Un incidente può manifestarsi in molti modi, tra cui comportamenti anomali dei sistemi, tentativi di accesso non autorizzati, malfunzionamenti dei dispositivi di controllo o avvisi generati dai sistemi IDS/IPS. Il monitoraggio costante dei log di sistema, delle reti IT e OT e degli strumenti di sicurezza è essenziale per rilevare qualsiasi attività sospetta. Gli strumenti di monitoraggio devono essere in grado di generare alert automatici e inviarli al team di sicurezza. Una volta rilevato un possibile incidente, il team deve valutare la natura dell'evento e classificare la gravità dell'incidente, basandosi sull'impatto potenziale sui sistemi critici e sui dati. Tutti gli incidenti devono poi essere documentati in dettaglio, includendo informazioni come data e ora dell'incidente, descrizione dell'anomalia, sistemi coinvolti, potenziali cause e azioni intraprese. Questo aiuta a tracciare il progresso dell'analisi e facilita la risoluzione dell'incidente, nonché il continuo sviluppo e implementazione di miglioramenti al piano d'azione.

3. Contenimento e Isolamento

La fase di contenimento è cruciale per ridurre al minimo i danni provocati da un incidente. Il contenimento può includere l'isolamento di specifici sistemi o segmenti di rete per impedire che l'incidente si diffonda ad altre parti dell'infrastruttura. Nel caso di un attacco informatico o di un guasto critico, il primo passo è isolare i sistemi compromessi. Ad esempio, se viene rilevata una compromissione della rete OT, si può procedere al blocco del traffico tra le reti IT e OT tramite firewall. Dopo aver isolato il sistema, il team deve avviare misure di contenimento a lungo termine, come l'analisi del malware o la modifica delle regole di accesso, per evitare che

l'incidente si ripeta. Anche durante il contenimento, è importante mantenere la continuità delle operazioni critiche (se possibile) per minimizzare l'impatto sull'operatività dell'impianto.

4. Eradicazione e Rimozione

La fase di eradicazione si concentra sulla rimozione definitiva della causa dell'incidente e sull'assicurarsi che i sistemi compromessi non siano più vulnerabili. Prima di procedere alla rimozione, è essenziale eseguire un'analisi approfondita per determinare la causa principale dell'incidente. Ad esempio, se un attacco informatico è stato causato da una vulnerabilità non risolta, è necessario risolvere questa vulnerabilità (se possibile) prima di ripristinare i sistemi. Se l'incidente è stato causato da un'intrusione o da malware, bisogna procedere con la rimozione di tutte le componenti malevole, aggiornando o reinstallando i sistemi compromessi. Durante questa fase, è essenziale applicare tutte le patch di sicurezza necessarie e aggiornare i sistemi con le ultime versioni del software per evitare future compromissioni.

5. Ripristino

La fase di ripristino si concentra sulla riattivazione dei sistemi compromessi e sul ripristino delle normali operazioni in modo sicuro. Una volta eliminata la minaccia, i sistemi possono essere ripristinati dai backup più recenti. È fondamentale verificare che i sistemi ripristinati siano integri e non presentino vulnerabilità. Dopo il ripristino, è necessario eseguire un monitoraggio approfondito per garantire che i sistemi siano completamente funzionanti e che non vi siano segni di ulteriori compromissioni. Eventuali attività sospette devono essere segnalate immediatamente.

6. Post-Mortem e Lezioni Apprese

La fase di post-mortem è essenziale per analizzare l'efficacia del piano di risposta all'incidente e identificare eventuali aree di miglioramento. Dopo aver risolto l'incidente, il team deve condurre una revisione dettagliata per determinare cosa ha funzionato bene e cosa no. Quali sono state le cause dell'incidente? Il piano di

risposta è stato eseguito correttamente? C'è stata una corretta comunicazione tra i team coinvolti? sulla base dei risultati della valutazione, il piano di risposta deve essere aggiornato. Ciò può includere l'aggiunta di nuove procedure, l'ottimizzazione del flusso di comunicazione, o l'adozione di strumenti di monitoraggio più efficaci.

Moduli e Registrazione degli Incidenti

Il piano di risposta agli incidenti deve includere moduli standardizzati per la registrazione di tutte le fasi di gestione dell'incidente, tra cui:

- Modulo di identificazione dell'incidente: In cui vengono registrati i dettagli del problema, inclusi i sistemi coinvolti e la natura dell'incidente.
- Modulo di contenimento e ripristino: Che documenta tutte le azioni intraprese per isolare e risolvere l'incidente.
- Rapporto finale dell'incidente: Che include una sintesi completa dell'evento, le cause, le azioni intraprese, e le lezioni apprese.

Comunicazione e Notifica

In conformità con la normativa NIS2, è obbligatorio notificare alle autorità competenti qualsiasi incidente di sicurezza che possa compromettere i servizi essenziali. Il piano di risposta deve includere una procedura di notifica per garantire che gli incidenti vengano segnalati entro i termini stabiliti dalla legge. Il team di risposta deve comunicare con tutti i reparti coinvolti, garantendo che le persone chiave siano rese edotte dell'escursus e degli esiti di tutte le fasi dell'incidente informatico.

2.7. TRAINING E CONSAPEVOLEZZA DEL PERSONALE

La formazione del personale è un aspetto chiave per prevenire attacchi informatici. La normativa NIS2 richiede che ogni operatore coinvolto nella gestione dei sistemi critici riceva un'adeguata formazione in materia di sicurezza informatica.

Programma di Formazione:

1. Cybersecurity Awareness:
   - Formazione obbligatoria per tutto il personale, con focus su minacce comuni (phishing, malware).
   - Phishing Simulation: Esecuzione di test simulati per rilevare la reattività del personale.
2. Gestione degli Accessi:
   - Addestramento sull'uso delle credenziali sicure e sull'importanza dell'autenticazione a più fattori.
   - Simulazioni di casi di compromissione dell'accesso.
3. Risposta agli Incidenti:
   - Simulazioni periodiche di attacchi informatici per verificare la preparazione e la prontezza degli operatori nel seguire il piano di risposta agli incidenti.
4. Verifica della Preparazione:
   - Test di valutazione delle conoscenze acquisite e misurazione del livello di consapevolezza attraverso questionari e prove pratiche.

3. ARCHITETTURA E PRINCIPI DI FUNZIONAMENTO DELL'IMPIANTO DI AUTOMAZIONE

3.1. DESCRIZIONE DEL SISTEMA DI CONTROLLO

L'impianto di automazione si occuperà della gestione e della supervisione del processo di produzione di biometano.

Dovrà quindi controllare tutti I processi e le lavorazioni di processo composto dalle seguenti macro-fasi:

- Ricezione e stoccaggio FORSU;
- Pretrattamenti FORSU (deferrizzatore, n. 2 bioseparatori e dissabbiatore);
- Digestione anaerobica (n. 2 serbatoi di idrolisi e n. 2 digestori anaerobici);
- Separazione solido – liquido (filtropressa e centrifuga);

- Purificazione del biogas – upgrading (trattamento di desolforazione ed essiccazione seguito da sistema di upgrading).

Il sistema di automazione è in grado di realizzare le molteplici funzioni necessarie al comando ed al controllo del processo industriale, al fine di conseguire il funzionamento automatico o manuale (ad es. in caso di manutenzione) dell'impianto e di permettere una conduzione performante, affidabile e sicura dello stesso. L'architettura è studiata affinchè ogni componente dell'impianto possa operare in modalità sia automatica che manuale.

Rientra tra I processi controllati anche la gestione dell'impianto di depurazione.

Il sistema è progettato per il raggiungimento delle seguenti funzioni minime:

- Programmazione, gestione e controllo delle missioni di lavoro del carroponte;
- Programmazione, gestione e controllo dei processi di digestione anaerobica. Principali parametri controllati:
  - ✓ Temperature, livelli, pressioni digestori;
  - ✓ Quantità di materiale trattati e rese produttive;
  - ✓ Quantità, pressione e qualità biogas;
  - ✓ Attuazione valvole e pompe;
- Programmazione, gestione e controllo del sistema di trattamento aria (ventilatori, scrubber e biofiltri). Principali parametri controllati:
  - ✓ Temperatura, pressioni e umidità;
  - ✓ Bagnatura biofiltri;
  - ✓ pH acqua lavaggio scrubber.
- Avvio, fermata e controllo dello stato di tutte le macchine (pretrattamento, separazione solido/liquido, raffinazione, sistemi di pompaggio, etc..), incluse sequenze logiche di avviamento e arresto e sequenze di interblocco;
- Visualizzazione allarmi, monitoraggio consumi elettrici, etc.
- Controllo stati macchine e segnalazioni di allarme da quadri di campo;
- Controllo di temperature, portate e pressioni (sensori in campo);

- Comando di pompe, motori, elettrovalvole;
- Invio di segnalazioni a quadri in campo:
- Interfacciamento dei PLC a bordo macchina per lettura dei parametri di funzionamento della stessa;
- Comando e gestione degli impianti di estrazione aria;
- Assicurare le azioni di cui sopra in completa sicurezza ed operatività;
- Garantire la massima continuità possibile di servizio dell'impianto;
- Migliorare l'efficacia delle strategie di conduzione attraverso un robusto controllo dei parametri di processo con l'adozione di logiche ottimizzate;
- Rendere possibile l'eventuale telecontrollo dei dati dell'impianto da remoto;
- Migliorare l'efficacia della manutenzione, applicando criteri di tipo preventivo nell'elaborazione delle informazioni diagnostiche.

Per realizzare l'automazione, il DCS (Sistema Controllo Distribuito) riceve I segnali di stato, di soglia e di misura, provenienti dagli strumenti in campo ed invia I comandi ai dispositivi, quali motori elettrici, valvole o attuatori in genere.

I "segnali convenzionali" sono trasmessi come variazioni di tensione (0-10V) o corrente (4-20mA) dagli strumenti alle schede I/O del DCS, tramite un singolo cavo a due fili in rame per ciascun segnale analogico, mentre I "segnali del bus di campo" sono trasmessi come informazioni digitali per mezzo di un protocollo di comunicazione (RTU RS485 Modbus), tramite un singolo cavo a due fili per molteplici segnali.

Linterfacciamento dei segnali I/O con il DCS è realizzato mediante schede di I/O convenzionali (contatti, 4-20mA) e schede per bus di campo (RTU RS485 Modbus) o di interfacciamente TCP/IP o fibra ottica nel caso dei collegamenti LAN.

Il DCS è fisicamente costituito da quadri elettrici di automazione o armadi rack posizionato nelle sale quadro o nelle cabine elettriche dell'impianto, ciascuno dei quali, per mezzo delle proprie unità di controllo (CPU), esegue le logiche di una diversa sezione del processo; le CPU sono in grado di operare in completa autonomia, in modo tale che un guasto ad una qualsiasi di esse non comprometta il funzionamento complessivo del DCS.

A ciascun quadro principale del DCS sono collegati uno o più sotto quadri di I/O

remoti contenenti le schede per I/O convenzionali e schede per bus di campo, posizionati nelle sale quadri o in campo in prossimità dell'elettrostrumentazione da interfacciare.

A supporto delle operazioni di supervisione, l'impianto sarà dotati di sistema TVCC, ovvero telecamere a circuito chiuso interrogabili dagli schermi della sala controllo per monitorare le principali zone di lavorazione del processo, riducendo la presenza di personale a diretto contratto con I rifiuti.

3.2. DISTRIBUZIONE

L'impianto in oggetto avrà come distribuzione in campo il seguente assetto:

N. 1 Rack denominato RACK_UFFICI (19'' da 42U a pavimento) posizionato nella palazzina uffici, al piano terra nella sala dei quadri elettrici, che sarà destinato ad ospitare l'hardware utile alle connessioni dall'esterno verso il mondo OT, in questo rack saranno presenti i router che forniscono le connessioni di impianto da e verso il mondo Internet; i firewall e gli switch di tipo managed che gestiranno e instraderanno le suddette connessioni. In particolare saranno presenti:

- i Firewall e gli switch di tipo managed per gestire e porre in essere la segregazione delle connessioni così da segmentare e separare, anche fisicamente, le connessioni da e verso l'esterno in direzione OT e le connessioni verso il campo.
- un Wireless LAN Controller per la gestione senza soluzione di continuità delle reti AP Wi-Fi;
- il centralino VOISPEED per la gestione della fonia IP Based;
- i Server sui quali far girare i Virtual Host utili a garantire l'intero funzionamento di impianto sia per il comparto IT che per quello OT.
- Il NAS Engine utile a garantire il Backup di tutti i sistemi ed il NAS Storage che ospiterà materialmente i dischi;
- un PC per la distribuzione, la configurazione e l'aggiornamento dei client presenti;
- un pc dedicato al disaster recovery;

- patch panel multimodale a 48 porte;

- N.1 Rack denominato RACK_PRE (19'' da 42U a pavimento), posizionato all'interno della Cabina C1_bis e includerà:
  - PLC in configurazione ridondata;
  - Connessione ai package;
  - Schede I/O con 20% di spare per ogni tipologia di segnale;
  - Doppia alimentazione 230Vca da UPS;
  - HMI Touchscreen fronte quadro da 22";
  - In sezione separata, ma nello stesso quadro:
    - PLC failsafe per ESD (minimo SIL2);
    - Schede I/O failsafe con 20% di spare per ogni tipologia di segnale ESD;
    - Doppia alimentazione 230Vca da UPS;
- N.1 Rack denominato RACK-DIGESTORE (19'' da 24U a pavimento), posizionato nei pressi della sala pompe del biodigestore:
  - PLC in configurazione ridondata;
  - Connessione ai package;
  - Schede I/O con 20% di spare per ogni tipologia di segnale;
  - Doppia alimentazione 230Vca da UPS;
  - HMI Touchscreen fronte quadro da 22";
  - In sezione separata, ma nello stesso quadro:
    - PLC failsafe per ESD (minimo SIL2);
    - Schede I/O failsafe con 20% di spare per ogni tipologia di segnale ESD;
    - Doppia alimentazione 230Vca da UPS;
- N.1 Rack denominato RACK-REFLUI (19'' da 42U a pavimento), posizionato nel locale quadri del trattamento reflui:
  - PLC in configurazione ridondata;
  - Connessione ai package;
  - Schede I/O con 20% di spare per ogni tipologia di segnale;

- Doppia alimentazione 230Vca da UPS;
- HMI Touchscreen fronte quadro da 22";
- In sezione separata, ma nello stesso quadro:
  - PLC failsafe per ESD (minimo SIL2);
  - Schede I/O failsafe con 20% di spare per ogni tipologia di segnale ESD;
  - Doppia alimentazione 230Vca da UPS;

- N.1 Rack denominato RACK-C2 (19'' da 42U a pavimento), posizionato nel locale quadri del trattamento reflui:
  - PLC in configurazione ridondata;
  - Connessione ai package;
  - Schede I/O con 20% di spare per ogni tipologia di segnale;
  - Doppia alimentazione 230Vca da UPS;
  - HMI Touchscreen fronte quadro da 22";
  - In sezione separata, ma nello stesso quadro:
    - PLC failsafe per ESD (minimo SIL2);
    - Schede I/O failsafe con 20% di spare per ogni tipologia di segnale ESD;
    - Doppia alimentazione 230Vca da UPS;

Dovrà essere previsto un sistema di aerazione forzata, completo di filtri aria, gestito da termostato interno con termometro digitale. Il quadro dovrà inoltre essere dotato di illuminazione interna e tasca porta schemi nella parte interna di una delle portelle. L'accessibilità dell'armadio dovrà essere garantita sia dal fronte che dal retro, mediante portelle incernierate con chiusura a chiave. Sono richieste a fronte quadro spie di presenza tensione di tutti i livelli (es. 24Vdc, 110Vac, 230Vac, tensione da UPS). Si dovrà prevedere un selettore a chiave locale/remoto, sempre a fronte quadro, per la selezione della modalità di comando da touchscreen o da supervisione, gestito mediante segnale cablato a PLC e ulteriore pulsante fronte quadro di abilitazione ai comandi da locale.

Due alimentatori posti in parallelo, ognuno in grado di sopportare il 100% del carico richiesto, per la regolazione e alimentati dalla linea di alimentazione privilegiata. Le

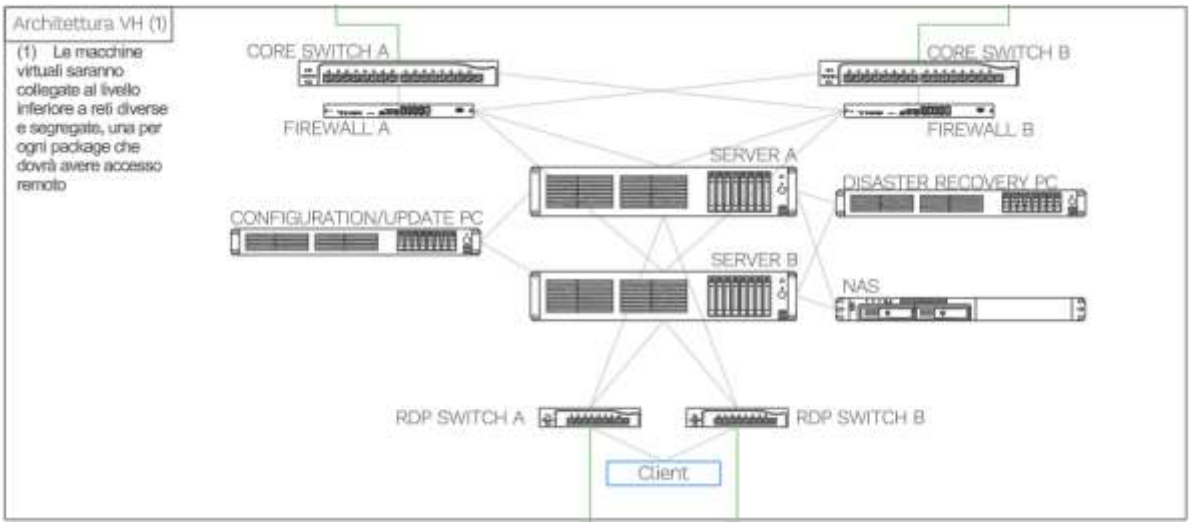
schede I/O di interfaccia con il campo dovranno prevedere uno spare del 20% per ciascuna tipologia di segnale (AI, AO, DI, DO).Ciascuna CPU dovrà essere collegata singolarmente all'armadio di rete presente in Sala Controllo, senza l'ausilio di hub o switch installati all'interno del quadro. Inoltre ciascuna CPU dovrà essere collegata, mediante comunicazione dedicata, al Touch Panel su fronte quadro e a tutti i sistemi periferici.

Una sezione separata, ma sempre all'interno dello stesso quadro, dovrà essere dedicata alla parte di sicurezza ESD certificata SIL2 minimo. Anche in questo caso le schede I/O di interfaccia con il campo dovranno prevedere uno spare del 20% per ciascuna tipologia di segnale (AI, AO, DI, DO). Le morsettiere di interfaccia con la strumentazione in campo dovranno essere separate da quelle relative alla sezione non di sicurezza.

3.3. ARCHITETTURA SALA CONTROLLO

Il sistema, montato in rack da 19'', è costituito da:

- N°2 Core switches
- N°2 Firewalls
- N°2 Server HPE ProLiant DL380 or SYNETO HYPER Series 3000 o equipollenti
- Server di configurazione, ripristino, Disaster ricovery
- N°2 RDP switches per la connessione dei thin client
- N° 3 thin clients a doppio schermo con tastiere e mouse
- NAS (Network Attached Storage)



Dettaglio dell'architettura di Virtual Host estratto dall'elaborato 8.2.2-23008-OW-C-82-DD-037-HA4-1-SCHEMA A BLOCCHI RETE DATI.

3.4. SPECIFICHE MINIME SERVER:

- 16 core @ 2.4 GHz o superiori
- Minimum 8TB HDD plus SDD for cache.
- Minimum 256 GB RAM (preferibile 512 GB)
- 2 x 10GbE RJ45 + 1 x IPMI RJ45 ports
- HPE Integrated Lights-Out (iLO) oppure SYNETO OS Ultime versioni
- Doppia linea di alimentazione 230Vac

3.5. RDP E CORE SWITCHES

Gli Switch saranno di marca HPE, DELL, CISCO. Gli switch core dovranno avere almeno 24 porte RJ45 configurabili ciascuno e connessioni in fibra ottica monomodale o multimodale. Da includere in fornitura N°20 SFP multimodale, N°4 monomodale, N°10 SPF RJ45. Gli switch RDP dovranno avere almeno 12 porte RJ45 ciascuno, con funzionalità almeno Layer 2 e dovranno gestire connessioni a 100MBPS e 1Gbps. Sul lato Field Connection, è preferibile uno switch firewall con soluzione integrata in grado di segregare le reti come da architettura proposta. Gli switch dovranno avere una doppia linea di alimentazione a 230Vac.

3.6. FIREWALL

Il firewall dovrà essere di marca Fortinet o Cisco e dovrà garantire collegamenti di almeno 1Gbps.

3.7. THIN CLIENTS

I thin client devono essere dotati di doppio monitor. Le porte USB non necessarie per il collegamento di mouse e tastiera devono essere evitate o chiuse meccanicamente per evitare qualsiasi connessione a chiavi USB con potenziale rischio di virus. I thin client dovranno essere di marca HP o DELL o equipollenti, i monitor saranno LCD da almeno 27", la tastiera e il mouse saranno inclusi nella fornitura.

CONFIGURATION AND RESTORE COMPUTER

Un computer per il ripristino e la configurazione sarà incluso nell'ambito del lavoro e sarà installato all'interno del RACK_CED.

NAS

Almeno una unità Rack Synology, HP o DELL ad alte prestazioni come archiviazione per i servizi sopracitati di configurazione, ripristino, backup, disaster recovery.

SEGNALI I/O

Gli I/O riportati sono la quantità indicativa alla quale andrà applicata la riserva del 20%. I segnali ridondanti da/verso il campo non dovranno essere collegati allo stesso modulo I/O. Si prevedono 6 nodi principali e che identificano i DCS:

- "A-PRET" dedicato al pretrattamento
- "B-BIO1" dedicato a Scrubber/Biofiltro zona pretrattamento
- "C-DIGE" dedicato alla sezione di Digestione Anaerobica
- "D-WWTP" dedicato alla sezione di Depurazione e Dewatering
- "E-UPGR" dedicato alla sezione di Upgrading del Biogas
- "F-BIO2" dedicato a Scrubber/Biofiltro zona Upgrading

Nodo	DI	DO	AI	AO	Link Scada	Totale I/O
A-PRET	164	106	3	0	90	273
B-BIO1	4	2	2	1	50	9
C-DIGE	35	24	16	12	500	87
D-WWTP	10	6	6	3	203	25
E-UPGR	9	12	5	4	550	30
F-BIO2	4	2	2	1	50	9
Safety	47	44	7	5	103	103
Totale	**273**	**196**	**41**	**26**	**1546**	**526**

3.8. SISTEMA DI SUPERVISIONE SCADA GENERALE DI IMPIANTO

Il Sistema di Supervisione sarà costituito da una piattaforma SCADA completa di tutte le licenze e gli applicativi necessari a realizzare le funzionalità descritte di seguito:

- fornitura delle opportune licenze client e server con numero di tag da definire;
- fornitura delle licenze, se necessarie, per realizzare un sistema di assistenza remota;
- verifica e approvvigionamento licenze/driver per la comunicazione con i sistemi sottesi;
- fornitura di eventuali moduli software/licenze aggiuntive per implementare le funzionalità di generazione e download dei trend e liste allarmi/eventi secondo le specifiche funzionali richieste di seguito;

Sono inoltre incluse tutte le ulteriori licenze necessarie al rispetto dei requisiti di cui al presente elaborato, a titolo di esempio e non esaustivo:

- Licenze sistema operativo WinServer22 LTSC per server; Win11 PRO per i client; (quantità da definire)
- Licenza Antivirus Symantec endpoint protection;
- Licenze per motore di storicizzazione eventi e misure;
- Licenza server sistema supervisione;
- Licenze client supervisione;
- Driver/licenze per interfacciamento apparati esterni.

Funzionalità del sistema di supervisione

Il sistema di supervisione espleterà le seguenti funzionalità principali:

- monitoraggio e controllo continuo del funzionamento di tutte le apparecchiature facenti parte degli impianti;
- visualizzazione, storicizzazione e gestione degli allarmi e degli eventi;
- visualizzazione, storicizzazione delle misure;
- valutazione dei principali parametri di funzionamento e prestazionali di sala (consumi specifici ed utilizzi dei principali vettori) e delle singole macchine (vibrazioni, temperature, ecc.);

In generale dovranno essere messe sotto trend almeno tutte le variabili analogiche di ingresso e di uscita legate alle regolazioni (sia PID che a soglie) in modo da permettere all'operatore di impostare trend personalizzati su qualsiasi variabile.

Dovranno inoltre essere storicizzati anche i comandi (manuali ed automatici) e gli stati delle utenze nonché i passaggi auto/man. Il log eventi dovrà in ogni caso essere condiviso con Fenice in fase di realizzazione al fine di permetterne una efficace ottimizzazione. Inoltre, dovranno essere predisposti trend predefiniti per ciascun sottosistema controllato.

Interfaccia operatore

I pannelli HMI devono avere uno "switch software" che permette di prendere il comando da locale inibendo i controlli dall'altro pannello e dallo SCADA principale, facendo apparire su ogni pagina grafica un messaggio nel caso di inibizione. Resta il fatto che lo SCADA centrale ha la priorità e può riprendersi il controllo da solo, inibendo i pannelli HMI.

Ogni operatore sarà abilitato allo svolgimento almeno delle seguenti azioni:

- monitorare variabili di processo analogiche e stati di attuatori ed utenze (valvole, motori, ecc.);
- comandare apertura/chiusura di valvole ed accensione/spegnimento di motori;
- selezionare procedure in Automatico/Manuale ove previsto;
- selezionare utenze ove previsto;
- richiamare regolatori sulla stessa pagina di sinottico interessata ed interagire con essi per espletare sequenze di AUTO/MAN, modulazione dell'uscita in MAN, impostare Target di Rampa, o verificare la regolazione, impostare Set Point, etc.;
- verificare la disponibilità dei comandi per le utenze;
- visualizzare/riconoscere allarmi di Sistema e/o di Processo;
- resettare eventuali anomalie sui comandi o blocchi di apparati;
- visualizzare ore di funzionamento per motori ed utenze in genere;
- visualizzare tempi di attesa per le operazioni in corso;
- monitorare i consumi e le produzioni dei vettori;

Saranno inoltre implementati collegamenti diretti tra le pagine video (ad esempio mediante click sulle descrizioni delle direzioni delle tubazioni, oppure su parti di impianto) senza necessità di ricorrere obbligatoriamente ai menu generali delle

pagine video.

Sarà possibile per gli operatori espletare anche queste ulteriori funzioni:

- monitorare Trend delle variabili di processo controllate;
- visualizzare (ma non modificare, la modifica sarà possibile solo sotto password) i parametri di tuning sui vari regolatori (Guadagno, Integrale, ecc.); tali parametri saranno modificabili solo con apposito livello di privilegio;
- visualizzare le soglie di allarme per tipologia, con relativi valori d'isteresi;
- impostare, ove previsto, soglie di intervento delle logiche di tipo on-off (senza che queste ultime siano necessariamente legate a soglie preimpostate di allarme).
- operare una diagnostica dell'hardware, con rilievo di eventuali anomalie su ognuna delle schede, CPU, alimentatori, bus di comunicazione, con possibilità di riconoscimento dettagliato delle stesse;
- monitorare le CPU in Runtime con relativo carico di buffer e di memoria RAM sia utente che di programma;

Allarmi e diagnostica di sistema

Andrà fatta una netta distinzione tra l'analisi dello stato dell'hardware di macchina con quella inerente alle anomalie di processo o dispositivi di campo.

Dalla visione di tutte le pagine proposte sarà evidente l'esistenza di un Banner Allarmi in ogni pagina. Qui saranno visualizzate tutte le anomalie. Gli Allarmi potranno essere riconosciuti e quindi cancellati se non più presenti.

Deve essere prevista anche la segnalazione di ogni anomalia relativa all'hardware e alla mancanza di collegamento con la supervisione e/o con la postazione locale. In tale condizione, in particolare, i valori visualizzati non devono rimanere congelati, ma deve essere chiaramente indicata l'anomalia.

Deve essere infine prevista una pagina allarmi con le funzionalità di:

- elenco allarmi attivi;
- riconoscimento allarmi;
- tacitazione allarmi;

- cancellazione allarmi dall'elenco (non dallo storico);

Sicurezza del sistema

Su tutte le macchine oggetto del presente Appalto dovrà essere effettuato quanto segue:

- disabilitazione, in modalità operatore, dell'accesso alla barra di Windows;
- disabilitazione, in modalità operatore, delle porte USB;
- disabilitazione, in modalità operatore, del lettore/masterizzatore DVD;
- disabilitazione, in modalità operatore, di eventuali altre porte di comunicazione non utilizzate per la normale operatività del sistema;

La riabilitazione delle funzionalità di cui sopra potrà essere effettuata solo mediante accesso al sistema operativo con utente e password di amministratore.

3.9. REGISTRAZIONE DEI DATI

Per tutte le variabili di ingresso e uscita analogiche (misure e comandi) deve essere prevista la registrazione in modo da poter generare trend in qualsiasi momento e su qualsiasi di esse.

Dovranno essere predisposti i seguenti trend:

- trend di tutte le variabili, suddivise per vettore e abilitabili/disabilitabili in visualizzazione singolarmente;
- trend delle variabili analogiche di ingresso e uscita relative a motori sotto inverter e valvole di regolazione;
- trend di tutte le misure di portata e misure per compensazione (temperatura e pressione) e relativi calcoli di potenza ed energia ove presenti suddivisi per sistema (P&ID);
- trend di tutte le variabili analogiche di ingresso di ciascuna macchina (motori, assorbitore);

Si richiede che vengano storicizzati anche i comandi ed i feedback di stato. Per quanto riguarda i comandi dovranno essere storicizzabili sia quelli dati da

supervisione che quelli risultanti da logica automatica, in pratica quindi dovranno essere storicizzati i DO di comando effettivi uscenti da PLC a campo.

Per tutti i segnali analogici di ingresso e uscita (anche quelli non facenti parte dei trend predefiniti di cui sopra) dovranno poi essere generati a scelta dell'operatore, e memorizzati (in modo da poterli richiamare successivamente senza re-impostarli), trend personalizzati.

Ogni trend (predefinito o personalizzato) dovrà poter essere esportato in formato .csv a partire da un arco temporale di inizio e fine impostabile dall'operatore e con una scansione temporale a scelta (un dato ogni secondo, minuto, ora).

I file così generati saranno salvati in una cartella di rete condivisa da definire in modo da essere prelevati da una seconda macchina (da definire) senza l'ausilio di dispositivi USB o unità di memorizzazione ottiche.

Diagnostica del sistema e della comunicazione

La diagnostica del sistema prevede la realizzazione di pagine video che permettono la diagnostica di ogni singolo sistema di controllo. In aggiunta si richiede un sistema tipo watch dog che effettui il monitoraggio in continuo dello stato della comunicazione tra:

- server e ciascun client;
- server e PLC in campo;
- touch screen e PLC;
- comunicazioni modbus tra PLC e utenze;
- rete profinet;
- server/pannello verso dispositivi modbus acquisiti tramite rete ethernet.

Nel caso in cui vi sia la perdita di comunicazione tra client e server, sul client dovrà essere chiaramente visibile l'anomalia con apposito allarme o pop-up.

Nel caso in cui vi sia la perdita di comunicazione tra server e PLC in campo, su ciascun client, sulla postazione locale e sul server (qualora su quest'ultimo vi siano pagine video in esecuzione) dovrà comparire apposito allarme o pop-up.

Per ogni tipologia di dati, la tabella seguente può essere presa come riferimento per le tempistiche di campionamento.

SEZIONE	DESCRIZIONE	UNITA'	TEMPO DI CAMPIONAMENTO
Livelli	serbatoi	cm	60 s
Flussi	Portata gas	Nm3/h	15 s
	Portata liquidi	m3/h	15 s
Flussi totali	liquidi	m3	10 s
Pressioni	Pressioni gas e liquidi	Mbar(g)	15 s
temperature	temperatura	°C	1 min
Analisi (se presenti)	Ph, redox, OD, SS, etc.	In U.M.	15 s
Corrente ed energia	corrente	A	60 s
	potenza	kW	60 s
	energia	kWh	60 s
	Energia attiva	kWh	60 s
Comandi analogici e feedback	PID OP, comando modulazione valvole	%	15 s, su cambiamento di comando manuale

I dati registrati sono usati per plottare I trend di andamento (pagine grafiche).

PAGINA
Pretrattamento (una o più pagine)
Digestione anaerobica (una o più pagine)
Flussi (una o più pagine)
Flussi totali (una o più pagine)
Livelli (una o più pagine)
Multimetri
Motori (una o più pagine)
Ultra filtrazione (una o più pagine)
Upgrading (una o più pagine)
Trattamento aria (una o più pagine)

3.10. REPORT GIORNALIERO E MENSILE

Al termine di ogni giornata il software deve creare un report giornaliere che visualizza I dati più importanti della giornata.

Elenco eventi

Il sistema di supervisione creerà un log distinto dal log allarmi che registrerà i seguenti eventi:

- stato di marcia/arresto motori ed utenze in genere;
- comando marcia/arresto motori (sia in AUTO che in MAN) ed utenze in genere;
- stato auto/man utenze;
- stato valvole aperta/chiusa/in movimento;
- comando apertura/chiusura valvole (sia in AUTO che in MAN);
- variazione set-point regolatori;

Al fine di ottimizzare l'elaborazione dei dati si intende, per questo log eventi, che devono essere registrati tutti gli stati e comandi all'atto dell'avvio del sistema e, conseguentemente, i soli cambi di stato o comando senza la necessità di acquisire

continuamente le variabili. Il log eventi così generato sarà esportabile in formato compatibile con Office (.csv, .txt, .xml, ecc.) e coprirà un arco temporale di un giorno, dopodiché verrà salvato con nome file in cui sia visibile giorno, mese e anno di riferimento e sarà generato un nuovo file di log eventi per il nuovo giorno.

Il log eventi potrà essere visualizzato su pagina video ed esportato ma in nessun caso modificato o cancellato anche solo parzialmente.

Log allarmi

Il sistema di supervisione registrerà e visualizzerà in continuo gli allarmi provenienti dai sistemi di controllo.

Per ciascun allarme dovrà essere visualizzato lo stato (attivo, non attivo, riconosciuto, tacitato) in apposita pagina video.

Anche per gli allarmi dovrà essere predisposto un sistema di archiviazione file esportabile in formato compatibile con Office (.csv, .txt, .xml, ecc.) e che copra un arco temporale di un giorno, dopodiché verrà salvato con nome file in cui sia visibile giorno, mese e anno di riferimento e sarà generato un nuovo file di log eventi per il nuovo giorno. Nel log allarmi dovranno essere registrate anche, oltre agli allarmi stessi, le operazioni di riconoscimento, tacitazione, cancellazione a video.

Per tutte le variabili analogiche di ingresso dovranno potere essere configurati dall'operatore opportuni allarmi LL, L, H, HH da trattare secondo le stesse modalità previste per gli altri allarmi (registrazione su log allarmi).

Il log allarmi potrà essere visualizzato su pagina video ed esportato ma in nessun caso potrà essere modificato o cancellato anche solo parzialmente, mentre sarà possibile visivamente cancellare dalla sola pagina video gli allarmi una volta riconosciuti.

3.11. GRUPPO ELETTROGENO DI BACKUP

Il software SCADA deve essere progettato con una modalità di blackout ed una modalità di backup. Il sistema di automazione, essendo l'impianto equipaggiato con un generatore di backup (gruppo elettrogeno), riceverà ulteriori segnali DI.

3.11.1. Modalità Blackout – Assenza del consenso remoto

Nei casi di blackout dell'impianto (mancanza alimentazione da rete), I PLC dell'impianto dovranno escludere i segnali di consenso remoto. In assenza del consenso remoto, per tutti gli elementi del sistema, con nessuna eccezione:

- Tutte le richieste di avvio automatico o manuale dei motori (incluse le valvole motorizzate) saranno resettate;
- Tutti i comandi automatici alle valvole saranno resettati;
- I consensi, gli avvi e gli start di attivazione package, se presenti saranno resettati. Gli stop di emergenza non saranno dati;
- Le membrane saranno forzate a SPEGNIMENTO sequenziale.

I comandi in manuale sono possibili ma non sortiranno effetto, con l'eccezione dei dispositivi sotto UPS. Tutti gli strumenti ed i controllori (PLC, messaggi di sistema, etc.) dovranno quindi continuare nel loro funzionamento.

3.11.2. Modalità BACKUP (emergenza)

Nei casi di assenza di energia dalla rete elettrica principale, l'alimentazione avverrà tramite gruppo elettrogeno da 350kW che non coprirà l'intero assorbimento dell'impianto ma coprirà solo la sezione di biodigestione, una parte del pretrattamento e la rete di supervisione della sala controllo.

I PLC di impianto dovrebbero mandare i segnali di consenso remoto e i DI addizionali per la modalità generatore di backup. Ciò consentirà l'esecuzione delle sole sequenze prioritarie se presenti, attraverso l'energia fornita dal gruppo elettrogeno di emergenza.

Nel caso sporadico del transitorio da modalità standard e di backup, tutti i componenti del sistema saranno gestiti come descritto nei paragrafi seguenti.

I comandi in manuale saranno possibili. Tutti gli strumenti ed i controllori (PLC, messaggi di sistema, etc.) continueranno nel loro funzionamento normale.

Dopo il transitorio dalla modalità di Backup completata, ogni sequenza può essere riavviata in modalità semiautomatica (es. con lo start da comando SCADA).

L'avvio automatico dei singoli componenti sarà possibile se richiesto dalla sequenza semiautomatica e non da altre richieste automatiche temporizzate, o da livelli, o parametri similari.

L'energia disponibile nella modalità generatore di emergenza sarà bastevole solo per alcune sequenze. Queste operazioni dovranno essere supervisionate costantemente da un operatore che conosce le procedure di emergenzae i limiti del generatore di backup (gruppo elettrogeno).

3.11.3. Modalità STANDARD

Nel caso di presenza di consenso remoti e assenza di DI per la modalità di backup, la modalità standard sarà attivata (funzionamento normale). Questo sarà valido finchè la modalità di backup sarà disattiva, ad esempio al ritorno dell'alimentazione da rete elettrica principale.

Dopo 5 secondi dall'avvio della modalità standard, saranno ripristinati i comandi di reset dei quadri macchina package, se presenti, in modo tale da ripristinare i loro moduli di sicurezza e dei VFD (inverter).

3.11.4. STOP DI EMERGENZA

I dispositivi di arresto d'emergenza devono poter consentire all'operatore di arrestare le funzioni pericolose della macchina il più rapidamente possibile nel caso in cui, nonostante si siano adottate altre misure di protezione, si verifichino situazioni o eventi pericolosi. Il dispositivo di arresto d'emergenza non rappresenta una protezione in sé, ragion per i dispositivi di arresto di emergenza devono rappresentare una soluzione di riserva di altre misure di protezione, come i ripari e i dispositivi di protezione, e non sostituirsi ad esse. Tuttavia, il comando d'arresto d'emergenza deve poter consentire all'operatore di impedire che una situazione pericolosa causi un incidente, o per lo meno di ridurre la gravità delle conseguenze di tale incidente. Un comando di emergenza deve anche poter consentire all'operatore di impedire che la macchina sia danneggiata a causa del malfunzionamento.

3.12. STRUTTURA DEL SISTEMA DCS

Il DCS è costituito da unità di controllo collegate tra loro da una rete LAN unica e ridondante (LAN di controllo processo) alla quale sono connessi anche I server e le stazioni HMI.

Le diverse unità di controllo sono in grado di operare in modo completamente autonomo, in maliera tale che un guasto di un un'unità non comprometta il funzionamento complessivo del DCS.

In particolare, il sistrema di controllo è strutturato con nr. 3 postazioni di automazione con logia programmabile (PLC) ed autonome nel funzionamento da installare nei 3 quadri principali di impianto:

- UC1.0-PRE da installare nel RACK-PRE presente nel locale quadri Cabina C1bis
- UC2.0-DIGE da installare nel RACK-DIGESTORE adiacente alla sala pompe
- UC3.0-REFLUI da installare nel RACK-REFLUI presente nel locale quadri trattamento reflui
- UC4.0-UPGR da installare nel RACK-C2 presente nel locale quadri cabina C2

Ciascuna delle unità di controllo intelligenti sopra gestirà in maniera autonoma (tramite comunicazione su rete LAN) le unità remote per l'acquisizione dei segnali e comandi dagli altri quadri di impianto, ovvero:

- UC1.1-PRE-CARROPONTE (CRA-20010)
- UC1.2-PRE-LACERASACCHI (BAO-21010)
- UC1.3-PRE-DEFERRIZZATORE (MAD-23010)
- UC1.4-PRE-TRAMOGGIA (FHO-21020)
- UC1.5-PRE-BIOSEPARATORE (PKG-25010)
- UC1.6-PRE-BIOSEPARATORE (OPE-25010)
- UC1.7-PRE-VASCA-MISCELAZIONE (PKG-25010)
- UC1.8-PRE-DISSABBIATORE (PKG-25010)
- UC2.1-DIGE-IDROLISI (TK-40010)
- UC2.2-DIGE-IDROLISI (TK-40110)
- UC2.3-DIGE-DIGESTORE (TK-41010)
- UC2.4-DIGE-DIGESTORE (TK-42010)

- UC3.1-REFLUI-PRESSA-VITE
- UC3.2-REFLUI-CENTRIFUGA (CEN-52010)
- UC3.3-REFLUI-POLIPREPARATORE (PKG-08010)
- UC3.4-REFLUI-ULTRAFILTRAZIONE
- UC3.5-REFLUI-OSMOSI-INVERSA
- UC3.6-REFLUI-SCAMBIATORE
- UC3.7-REFLUI-TORRE
- UC3.7-REFLUI-EVAPORATORE
- UC4.1-UPGR-BIOGAS-CONDITIONING (PKG-71010)
- UC4.2-UPGR-BIOGAS-UPGRADING (PKG-74010)
- UC4.3-UPGR-BIOGAS-ANALYSIS (PKG-75010)
- UC4.4-UPGR-BIOGAS-COMPRESSOR (PKG-75020)

Tutte le unità di controllo, potranno comunque interrogare qualsiasi altra unità remota in quanto tutto il sistema farà capo ad un'unica rete LAN interna all'impianto. Il sistema sarà supervisionato da una sala controllo ove è ubicata la postazione operatore che fungerà da interfaccia grafica (HMI) tra l'operatore ed il DCS di impianto. La postazione sarà dotata di un software di supervisione controllo ed acquisizione dati (SCADA) tramite il quale l'operatore terrà sotto controllo tutti I parametri (misure, stati, condizioni di allarme) di tutti I processi di impianto.

3.13. INTEGRAZIONE DEI SISTEMI DI CONTROLLO DEDICATI (QUADRI PACKAGE)

L'impianto di automazione

Il livello di integrazione del DCS in progetto coi sistemi di controllo dedicati (SCD) specifici per alcune macchine e/o sezioni di impianto (es. Scrubber, Upgrading, Digestori etc.), è tale da permettere il comando ed il controllo dei sistemi dedicati, in forma chiara ed efficiente.

L'utilizzo di sistemi di controllo dedicati, per realizzare l'automazione di alcune parti

dell'impianto, è applicato nei seguenti casi:

- Quando il fornitore è specialista nella costruzione della parte di impianto che realizza;
- Per ragioni di know-how e di integrità della fornitura;
- Per piccoli package, che arrivano in sito già completamente collaudati;

4. DESCRIZIONE DELLE APPARECCHIATURE

4.1. PESATURA AUTOMEZZI

Per monitorare i flussi di materiale in entrata/uscita tramite gli automezzi viene utilizzato un ponte di pesatura connesso situato all'ingresso dell'impianto. Dopo la misura, i camion in arrivo si dirigono verso la zona di pretrattamento nell'area di scarico dove il rifiuto organico viene scaricato in una Piattaforma di ricezione, da cui viene caricato verso il pretrattamento tramite carroponte. Prima di uscire dall'area di scarico, le ruote degli automezzi vengono pulite da un sistema di lavaggio dedicato. Gli indicatori luminosi sul ponte di pesatura e nell'area di scarico vengono visualizzati nel'interfaccia SCADA della sala controllo per comunicare con gli autisti degli automezzi.

4.2. PRETRATTAMENTO

Il sistema di preselezione opera una prima cernita di trattamento del rifiuto organico tramite l'apertura sei sacchetti e la separazione magnetica. Il sistema di alimentazione liquida completa la separazione delle sostanze organiche mediante rimozione della sabbia, fornendo la materia prima liquida per il serbatoio di stoccaggio ed in seguito ai digestori, prevedendo anche il flusso di ricircolo per la separazione organica. Il sistema è composto da bioseparazione composto da due bioseparatori ed un dissabbiatore.

4.3. PRETRATTAMENTO PERCOLATO

Il percolato raccolto dalle griglie della fossa di ricezione e dal pretrattamento è

raccolto per gravità in vasche/silos e da loro verso un serbatoio buffer di raccolta (a causa dell'alto contenuto di depositi organici) o nei digestori tramite pompe sommerse.

4.4. SERBATOIO BUFFER

La materia prima liquida proveniente dalla sezione di pretrattamento viene miscelato e mandato tramite una pompa di mandata la quale alimenta direttamente il digestore primario. Il biogas prodotto dalla digestione anaerobica viene convogliato attraverso le tubazioni del biogas verso il sistema di Upgrading del biogas, munito di torcia di emergenza.

4.5. DIGESTORE PRIMARIO

I digestori primari sono a tenuta stagna e sono dotati di cupole gasometriche che garantiscono un congruo volume di buffer preliminare all'invio del biogas prodotto alla sezione di purificazione e upgrading a biometano (migliorando anche l'efficienza di trattamento di quest'ultima sezione e riducendone i costi operativi legati al consumo di energia elettrica potendo contare su un biogas più stabile in termini di concentrazione dei singoli componenti e di portata).

4.6. STOCCAGGIO GAS

I digestori vengono riscaldati e miscelati in modo da mantenere il liquido di processo fluido ed omogeneo. Il biogas prodotto dalla digestione anaerobica viene immagazzinato attraverso il volume variabile sottostante le membrane e convogliato nelle tubazioni biogas, che collega ciascun serbatoio con gli altri e con le utenze (Sistema di upgrading del biogas e Torcia di emergenza). Mentre, per ciò che concerne il digestato, questo viene avviato alla fase di separazione solido liquido, mediante filtropressa seguita da una centrifuga.

4.7. LOCALE DI POMPAGGIO E SEPARATORE

Il sistema centrale di pompaggio è composto dalle tubazioni e dalle attrezzature necessarie a gestire i trasferimenti del liquido di processo tra i serbatoi e la

filtropressa, per la separazione del dgiestato dal digestato solido. La frazione liquida proveniente dal separatore viene raccolta nel serbatoio del filtrato FSP, mentre la frazione solida viene consegnata ad un deposito per usi esterni.

4.8. SISTEMA DI TRATAMENTO ARIA – SCRUBBER/BIOFILTRO

Il capannone di stoccaggio rifiuti in ingresso e pretrattamento dei rifiuti è mantenuto in depressione. L'aria interna viene aspirata da un ventilatore e, prima di essere immessa in atmosfera, viene trattata mediante un biofiltro preceduto da uno scrubber.

4.9. TRATTAMENTO BIOGAS E TORCIA

La sezione di produzione del biometano è composta da:

- Sistema di pretrattamento del biogas grezzo:
  - Torre scrubber per la rimozione di H2S;
  - Essiccazione e filtrazione, composto da:
    - Un filtro a coalescenza;
    - Un gruppo frigo e scambiatore di calore per l'essiccazione;
    - Una soffiante multistadio;
    - Due filtri a carboni attivi;
    - Un filtro antipolvere;
- Sistema di upgrading del biogas a biometanoCompressione del biogas a media pressione, così costituito:
  - Un filtro a carboni in aspirazione;
  - Uno scambiatore HR per il recupero di calore;
  - Un dry-cooler ad acqua;
  - Un chiller per il lato biogas;
- Sistema di Upgrading a membrane, formato da un sistema containerizzato all'interno del quale sono allestiti i tre skid di membrane per i tre stadi del processo;

- Compressione booster del biometano ad alta pressione, costituito da:
  - Un filtro in aspirazione;
  - Uno scambiatore di calore gas/acqua per raffreddamento;
  - Un dry-cooler;
- Unità di analisi e misura, costituita da un gas cromatografo e una cabina di regolazione e misura (Re.Mi.) per la consegna finale.

Il pacco torcia di emergenza è collegato alla linea del gas e viene utilizzato per bruciare il biogas quando la sua pressione è elevata, per evitare l'apertura delle valvole di sicurezza sui serbatoi.

I sistemi appena descritti rappresentano dei sistemi package, il fornitore provvede a fornire l'integrazione al DCS di impianto tramite schermate SCADA dedicate.

4.10. CARICAMENTO CARRI BOMBOLAI

l biometano proveniente dall'upgrading entra nello skid di analisi:

• Se la qualità soddisfa i parametri per la distribuzione, il gas viene inviato alla cabina REMI per la misurazione della portata prima dell'immissione in carri bombolai;

• Se la qualità non soddisfa i requisiti, il biometano viene rimandato ai digestori.

La selezione della destinazione del biometano è attuata da una valvola a 3 vie posta nel pacco di analisi e ricircolo.

4.11. SISTEMA DI RISCALDAMENTO

I serbatoi riscaldati sono dotati di serpentine interne e collegati all'impianto di riscaldamento. È costituito da un anello digestore, con diramazioni dedicate per ciascun serbatoio e da una valvola miscelatrice generale a tre vie utilizzata per la regolazione dell'acqua calda inviata ai serbatoi. Il riscaldamento viene effettuato mediante una caldaia con proprio circuito.

5. DIMENSIONAMENTO PAGINE VIDEO SISTEMA SCADA DCS

5.1. SOFTWARE DI CONTROLLO

Le logiche di controllo sono realizzate con blocchi funzionali di tipo grafico, il DCS possiede una libreria completa con le seguenti funzioni:

- Funzioni logiche: and, or, ex-or, not, timer, watch dog, sequencing, S-R memory, jump condizionato, etc;
- Funzioni temporali: filtro, lead/lag, dead time, rampe di variazione;
- Funzioni di selezione: low, High, override, switch;
- Funzioni di controllo: algoritmi PID standard e multivariabile, ratio, bias, anti reset windup, guadagno adattivo, feed-forward, setpoint e output tracking (bumpless trasfer), limitazione del set-point e dell'uscita, rampa;
- Funzioni digitali: controllo congruenza segnali digitali triplicati, generazione comandi impulsivi etc.

5.2. SOFTWARE HMI

La progettazione del software SCADA del DCS è eseguita considerando I seguenti fondamenti:

- Chiarezza di lettura dello stato dei componenti dell'impianto;
- Chiarezza di lettura delle variabili analogiche e delle indicazioni di allarme;
- La facilità di manovra per il comando e la regolazione;
- L'uniformità della rappresentazione delle informazioni.

L'interazione uomo-macchina, per tutte le funzioni di gestione dell'impianto, è orientata al modello object-actio (selezione oggetto e successiva scelta dell'azione da effettuare).

La conferma di azioni critiche è ottenuta attraverso messaggistica chiara ed attraverso meccanismi di conferma.

Nelle apparecchiature HMI il software applicativo ed I testi delle pagine sinottiche sono esclusivamente in lingua italiana.

5.3. PAGINE SINOTTICHE

Le pagine sinottiche costituiscono la rappresentazione grafica dei componenti dell'impianto e sono sviluppate a partire dai P&ID.

La navigazione tra le pagine avverrà per mezzo di un indice strutturato e tramite collegamenti diretti.

Le pagine sinottiche sono suddivise nelle seguenti tipologie:

- Operative: sono le pagine sinottiche che consentono all'operatore di interagine con l'impianto, grazie agli oggetti dinamici ivi contenuti, vengono visualizzate le informazioni sullo stato di funzionamento del processo e consentono all'operatore il completo controllo dello stesso;
- Di dettaglio: Visualizzano tutte le informazioni specifiche di una singola apparecchiatura e ne consentono la modifica di tutti I parametri (set-point, soglie, coefficienti di tuning etc.);
- Di sequenza: sono dedicate al monitoraggio a alla gestione di ciascuna sequenza;
- Dati storici: forniscono una rappresentazione tabellare e grafica dei dati archiviati dal sistema.

Per I dispositivi interfacciati al DCS, tutti gli stati di interblocco, anomalia, funzionamento locale/manuale, sono visualizzati nelle pagine sinottiche senza che sia necessario aprire I faceplate con I dettagli.

Dalla stazione Operatore è possibile gestire sessioni multiple di HMI, ognuna delle quali utilizzerà un proprio monitor, visaluzzando in ciascun schermo differenti pagine sinottiche.

5.4. DESCRIZIONE POP-UP UTENZE, MISURE

In generale ogni utenza o misura gestita dal sistema d'automazione ha una propria maschera web di gestione. Qui, sono raggruppate tutte le segnalazioni, i comandi, le misure, le soglie, ecc, che fanno parte dell'utenza o della misura stessa.

Questo in generale è diverso se si tratta di utenza o di misura.

5.4.1. Pop-Up utenze

il cursore nella pagina video quando passa sopra alla grafica della macchina si trasforma da freccina verde, indicando quindi la possibilità di cliccare. Cliccando col mouse si apre quindi il pannellino, che è così composto:

- nella parte estrema in alto viene riportato l'item della macchina;
- pulsanti per inserire la macchina in automatico, ciòè gestibile dal PLC, per il funzionamento in manuale da supervisione con i relativi pulsanti di marcia, arresto, apri, chiudi, ecc;
- maschera per la visualizzazione della corrente assorbita (se disponibile), e/o della frequenza di lavoro (se disponibile);
- pulsante per il reset a distanza della macchina;
- visualizzazione degli stati, allarmi.

Vi sono poi i pannellini delle utenze che non sono gestite dal sistema d'automazione, ma che s'interfacciano con questo per il riporto di stati e allarmi. In questi sono unicamente visualizzate tali segnalazioni. Manca chiaramente tutta la parte dei pulsanti di comando.

Figura 1: Utenza normale

Figura 2: Utenza Package

5.4.2. Pop-Up misure

Il cursore nella pagina video quando passa sopra alla grafica della misura, si trasforma in freccina verde, indicando quindi la possibilità di cliccare. Cliccando col mouse si apre quindi il pannellino, che è così composto:

- nella parte estrema in alto è riportato l'item della misura;
- nella parte sinistra del pannellino è raffigurata una barra luminosa progressiva 0-100% della misura;
- nella parte destra vi sono quattro soglie impostabili, extra minimo, minimo, massimo, extra massimo, abilitabili a piacere, le quali generano allarme.

Attenzione, allarmi generati da tali soglie non provocano nulla sulla gestione della logica funzionale processata dal PLC. Servono solo come avvertimento o promemoria all'operatore in supervisione. Nella parte bassa vi è il pulsante "by-pass misura da campo" e la finestra per inserire il nuovo valore da operatore. Tale possibilità è stata creata per ovviare ad eventuali rotture dei sensori di misura e poter comunque procedere col processo.

Nel momento in cui l'operatore decide di utilizzare tale possibilità è lui responsabile di quello che può accadere, considerando che in campo non ha più il sensore ma che il valore di misura è stato fissato da lui stesso. In ogni modo, per ricordare all'operatore tale by-pass, la grafica nella pagina video della misura cambia colore e viene attivata segnalazione di avviso generica del reparto;nella parte bassa vi è poi la finestra con l'indicazione del valore di misura e dell'unità ingegneristica;

nell'estremità in basso del pop-up vi sono riportate le diciture degli allarmi di misura.

Figura 3: Maschera misure sensori

5.5. ORE DI FUNZIONAMENTO

Nei vari PLC per ogni utenza sono programmati dei contatori delle ore di funzionamento a 32 Bit con una risoluzione di 6 minuti. Questi contatori vengono visualizzati in supervisione nei appositi pop-up utenze. Inoltre queste vengono date a disposizione al programma per la gestione della manutenzioni.

5.6. ERRORE DI MANCATA RISPOSTA

Il PLC per ogni uscita digitale che va comandare un utenza va a verificare il corretto funzionamento di questo. Cioè vuol dire che dando il comando di marcia ad una utenza questa entro un certo tempo deve segnalare il funzionamento tramite un apposito ingresso digitale. Trascorso il tempo massimo l'utenza va in allarme di mancata marcia. Questo controllo è attivo anche per l'arresto dell'utenza. Il tempo massimo è impostabile per ogni utenza nell'apposito panello pop-up dell'utenza.

5.7. MISURE DI LIVELLO

Per le misure di livello montate nei pozzi e serbatoi il valore misurato deve essere rappresentato nelle pagine grafiche sia come distanza (m) che come volume (m^3). Per questo il Software PLC utilizza delle curve di linearizzazione.

5.8. MISURE DI PORTATA

Per tutte le misure di portata i PLC contengono un contatore assoluto (32 Bit) e due contatori giornalieri (16 Bit) uno per il giorno corrente e uno per il giorno precedente. Questi valori di conteggio vengono rappresentati nei panelli pop-up delle relative misure e messa a disposizione al software per l'archiviazione dei dati.

6. SISTEMA TVCC DI PROCESSO

6.1. SORVEGLIANZA DELLE ZONE DI PROCESSO (TVCC)

L'implementazione di un sistema di videosorveglianza ben strutturato, permette di monitorare tutte le fasi del processo, prevenire incidenti, controllare l'accesso e garantire la sicurezza. Grazie a queste tecnologie, è possibile migliorare la gestione

delle operazioni e assicurare un ambiente di lavoro più sicuro e controllato. L'integrazione del sistema di videosorveglianza in una sala controllo dedicata e un DVR per la videoregistrazione aggiunge ulteriori livelli di sicurezza e controllo, garantendo un monitoraggio continuo e un archivio storico degli eventi rilevati.

6.2. ARCHITETTURA TVCC

L'architettura di videosorveglianza dell'impianto prevede diverse macrocategorie di telecamere, ciascuna con un ruolo specifico:

1. Telecamera per la Lettura delle Targhe
   - Numero: 1
   - **Scopo**: Monitorare l'accesso dei mezzi che entrano nell'impianto per il conferimento dei rifiuti.
   - **Posizione**: Ingresso dell'impianto.
   - **Tecnologia**: Telecamera con tecnologia ANPR (Automatic Number Plate Recognition) per la lettura automatica delle targhe.

3. Telecamere di Processo
   - Numero: 12
   - **Scopo**: Sorvegliare tutte le fasi del processo di trattamento dei rifiuti, dalla ricezione alla purificazione del biogas.
   - **Posizione**: Distribuite lungo tutte le macro-fasi del processo, inclusi i pretrattamenti, la digestione anaerobica, e la separazione solido-liquido.

4. Telecamere di Sicurezza Esterna e Perimetrale
   - Numero: 6
   - **Scopo**: Garantire la sicurezza perimetrale dell'impianto, prevenire intrusioni e atti di vandalismo.
   - **Posizione**: Aree esterne e punti di accesso perimetrale.

L'impianto TVCC è fisicamente costituito da 1 Armadio ubicato in Sala Controllo, al

quali sono interfacciate tutte le telecamere posizionate in campo nelle zone più idonee alla sorveglianza di processo.

I monitor del sistema TVCC sono collocati in apposita postazione in sala controllo.

L'integrazione del TVCC nel sistema DCS attraverso l'infrastruttura FIBRA/LAN, consente all'operatore di turno di visualizzare una o più immagini di una qualsiasi telecamera anche dalla postazione operatore DCS (postazione di supervisione e controllo del processo).

Il sistema TVCC di processo è costituito dai seguenti componenti:

- TVR con capacità di archiviazione di 8Tb a 32 Canali
- Workstation Camera che supporta fino a 4 monitor con risolizione 4k
- Switch Industriali PoE++ sia indoor che outdoor
- Licenze software di utilizzo

Da ciascuna stazione HMI è possibile gestire tutte le funzionalità del TVCC, in particolare:

- Visualizzare una o più immagini di una qualsiasi telecamere;
- Effettuare l'associazione telecamera e monitor del TVCC;
- Effettuare la gestione dello Zoom, del brandeggio e del preset per ciascuna telecamera;
- Consultare I dati storici quali immagini e informazioni di diagnostica.