COMMITTENTE:

RFI RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE

PROGETTAZIONE:

ITALFERR
GRUPPO FERROVIE DELLO STATO ITALIANE

U.O. Energia e impianti di trazione elettrica

PROGETTO DEFINITIVO

RADDOPPIO DELLA LINEA GENOVA – VENTIMIGLIA
TRATTA FINALE LIGURE – ANDORA

SISTEMA STES GALLERIE

Andora - S.Lorenzo - Relazione sistema Comando e Controllo, progettazione e certificazioni funzioni di sicurezza

SCALA: -

COMMESSA	LOTTO	FASE	ENTE	TIPO DOC.	OPERA/DISCIPLINA	PROGR.	REV.
IV0I	00	D	18	RO	SM0000	002	A

Rev.	Descrizione	Redatto	Data	Verificato	Data	Approvato	Data	Autorizzato Data
A	Emissione esecutiva	M. Colombo	Febbraio 2022	A. Sperduto	Febbraio 2022	G. Fadda	Febbraio 2022	Guido Guidi Beffarini Febbraio 2022

ITALFERR S.p.A. U.O. Coordinamento Tecnico Ing. Guido Guidi Beffarini Ordine Ingegneri Provincia di Roma n° 17812

File: IV0I00D18ROSM0000002A.doc | n. Elab.:

INDICE

1. OGGETTO

La presente relazione è stata ricavata dalla corrispondente relazione generale facente parte della documentazione "as built" del progetto ed esecuzione del Raddoppio della Linea Genova-Ventimiglia, tratto Andora – S.Lorenzo a Mare:

IV1A 03 B ZZ RO LC0004 001A – RELAZIONE SISTEMA COMANDO E CONTROLLO, PROGETTAZIONE E CERTIFICAZIONE FUNZIONI DI SICUREZZA

Dal momento che gli interventi previsti a progetto, sono dovuti alle modifiche del ferro nella stazione di Andora, determinano solo interventi di adeguamento agli impianti MATS esistenti, l'Appaltatore sarà tenuto ad utilizzare, anche per gli impianti di nuova realizzazione, la stessa tecnologia oggi presente in campo. Difatti l'appaltatore, per effetto delle modifiche che apporterà al sistema MATS esistente, dovrà rinnovare la certificazione del sistema SIL3 rivolgendosi pertanto allo stesso fornitore del sistema esistente.

Oggetto del presente elaborato è la descrizione del sistema di automazione dedicato al sezionamento e messa a terra di sicurezza delle Gallerie della linea Genova-Ventimiglia tratto Andora-S. Lorenzo al Mare.

In questo elaborato si vogliono descrivere le caratteristiche principali delle apparecchiature Hardware, le funzionalità del sistema e le funzioni accessibili all'operatore.

2. GENERALITA' DEL SISTEMA AUTOMAZIONE

L'implementazione di un sistema di automazione per la supervisione del sezionamento e messa a terra delle Gallerie a suo tempo realizzato deriva dalle seguenti considerazioni:

- Disponibilità di una rete in fibra ottica monomodale all'interno della *Galleria*, prevista per la supervisione di tutti i sistemi di sicurezza della galleria.
- Possibilità di evitare lunghi e costosi cablaggi in galleria per i sezionatori MAT e le apparecchiature connesse al sistema di messa a terra di sicurezza;
- Sviluppo di un sistema innovativo, inserito nella specifica RFI DTC DNS EE SP IFS 177 A (2008) "*Sezionamento della linea di contatto e messa a terra di sicurezza per gallerie ferroviarie*", che prevede che possa essere valutata l'opportunità di realizzare sistemi di controllo remoto in sicurezza.

In particolare è stato previsto di realizzare questo sistema inserendo alcune funzioni di sicurezza, da certificare SIL3, secondo le norme di cui al paragrafo 4 del presente elaborato.

E' previsto inoltre che l'intero sistema locale di messa a terra (hardware, software, quadri e apparecchiature), venga, per le sue funzioni di sicurezza, certificato SIL 3 secondo le normative CEI-EN 61508 Ed. 2011 (serie) e CEI-EN 61511 Ed. 2006 (serie) da ente indipendente.

Pertanto anche le integrazioni al sistema che sono l'oggetto del presente progetto determinano la ri-certificazione dei singoli sistemi di galleria coinvolti nell'adeguamento

Visti i contenuti specifici di questa attività, sarà documentato all'ente certificatore indipendente di aver già sviluppato lavori analoghi e di essere conforme a quanto previsto nella CEI-EN 61508-1 ed 2011, paragrafo 6.2.15.

3. DEFINIZIONI E ABBREVIAZIONI

- *MAT* - Messa a terra
- Q_{GPLC} - Quadro generale PLC. Quadro in cui sono contenute le apparecchiature di automazione principali che processano le informazioni provenienti dai siti in campo e che comunicano attraverso schede di DI/DO con il terminale periferico di telecomando
- Q_{MAT} - Quadro sezionatore di terra. Quadro in cui sono contenute tutte le apparecchiature per il comando e controllo locale dei sezionatori MAT
- Q_{PE} – Quadro pulsante di emergenza. Quadro di comando dei sezionatori di terra.
- Q_{CCR} - Quadro di controllo continuità del collegamento dei sezionatori MAT alla rotaia. Quadro in cui sono contenute tutte le apparecchiature per la funzione di controllo dell'integrità dei collegamenti del polo del sezionatore MAT alla rotaia
- Q_{PLC} - Quadro automazione che contiene tutti i relè e le apparecchiature di automazione per l'interfaccia dei sezionatori MAT, del rilevatore di tensione e del dispositivo di controllo di continuità del collegamento alla rotaia con il quadro Q_{GPLC} e di conseguenza con il terminale periferico di telecomando. Tale quadro è posizionato al fianco del quadro Q_{MAT}
- *Rete Ethernet di sicurezza in galleria* - Rete Ethernet in fibra ottica monomodale realizzata per le interfacce tra i QPLC e QGPLC.
- *SIL* – (*Safety Integrity Level*) Livello di sicurezza integrato
- *Switch PLC* – Switch industriale interno ai quadri Q_{PLC} e Q_{GPLC} che interfaccia tutte le apparecchiature di ogni sito (PLC, monitor, interfaccia DI/DO – Ethernet).
- *RTU – (Remote Terminal Unit)* Terminale periferico di telecomando tradizionale in uso da parte di RFI per la scambio segnali tra il DOTE e le apparecchiature TE lungo linea

4. NORME DI RIFERIMENTO

Oltre alle Norme già specificate nell'elaborato *"Relazione generale di sistema*", di seguito ripetute:

Decreto Ministeriale 28 Ottobre 2005 "*Sicurezza nelle gallerie ferroviarie*"

CEI EN 50122-1 – ed. 3/1998	*Applicazioni ferroviarie – Installazioni fisse – Parte 1 Provvedimenti di protezione concernenti la sicurezza elettrica e la messa a terra*
CEI EN 50123-Serie	*Applicazioni ferroviarie, tranviarie, filotramviarie e metropolitane - Impianti fissi – Apparecchiature a corrente continua.*
CEI EN 50123-1 – ed. 9/2003	*Parte 1: Generalità*
CEI EN 50123–3	*Interruttori di manovra sezionatori e sezionatori in corrente continua per interno.*
CEI EN 50123-4 – ed. 10/2003	*Interruttori di manovra sezionatori e sezionatori in corrente continua per esterno.*
CEI EN 50123-7-1 – ed. 11/2003	*Applicazioni ferroviarie – Installazioni fisse – Apparecchiature a corrente continua - Parte 7 Apparecchi di misura, comando e protezione per uso specifico in sistemi di trazione a corrente continua - Sezione 1: Guida applicativa*
CEI EN 50123-7-3 – ed. 11/2003	*Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane - Impianti fissi - Apparecchiatura a corrente continua Parte 7: Apparecchi di misura, comando e protezione per uso specifico in sistemi di trazione a corrente continua Sezione 3: Trasduttori di tensione isolanti e altri apparecchi di misura della tensione*
CEI EN 50124-1 ed. 09/2001	*Applicazioni ferroviarie, tranviarie, filotramviarie, metropolitane – Coordinamento degli isolamenti – Parte1: Requisiti di base – Distanze in aria e distanze superficiali per tutta l'apparecchiatura elettrica ed elettronica*
CEI EN 50124-1/A1/A2 – ed. 2005	*Applicazioni ferroviarie, tranviarie, filotramviarie, metropolitane - Coordinamento degli isolamenti Parte 1: Requisiti base - Distanze in aria e distanze superficiali per tutta l'apparecchiatura elettrica ed elettronica*
CEI EN 50152-2 ed. 02/2008	*Applicazioni ferroviarie – Installazioni fisse – Prescrizioni particolari per apparecchiature a corrente alternata – Parte2: Sezionatori, sezionatori di terra e interruttori per corrente monofase con U_m superiore a 1 kV*

CEI EN 50163 ed. 2/2006	*Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane - Tensioni di alimentazione dei sistemi di trazione*
CEI EN 50163/A1 – ed. 2008	*Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane - Tensioni di alimentazione dei sistemi di trazione*
CEI EN 60068-2 serie	*Prove climatiche e meccaniche fondamentali Parte 2: Prove*
CEI EN 60255-21 serie	*Relè elettrici – Parte 21 – Prove di vibrazione, urti, scosse e tenuta sismica applicabili ai relè di misura e ai dispositivi di protezione*
CEI EN 60439 serie	*Apparecchiature assiemate di protezione e di manovra per bassa tensione (quadri BT)*
CEI EN 60529- ed. 6/1997	*Grado di protezione degli involucri (Codice IP)*
CEI EN 60664-1 ed. 4/2008	*Coordinamento dell'isolamento per le apparecchiature nei sistemi a bassa tensione - Parte 1: Principi, prescrizioni e prove*
CEI EN 60694 ed. 11/1997	*Prescrizioni comuni per l'apparecchiatura di manovra e di comando ad alta tensione*
CEI EN 60694/A1/A2 – ed. 7/2002	*Prescrizioni comuni per l'apparecchiatura di manovra e di comando ad alta tensione*
CEI EN 60870-2-1 ed. 10/1997	*Sistemi ed apparecchiature di telecontrollo - Parte 2: condizioni di funzionamento - Sezione 1: condizioni ambientali e di alimentazione*
CEI EN 60870-2-2 ed. 9/1997	*Sistemi ed apparecchiature di telecontrollo - Parte 2: condizioni di funzionamento - Sezione 2: Condizioni ambientali (influenze climatiche, meccaniche e altre influenze non elettriche)*
CEI EN 61000-4 serie	*Compatibilità elettromagnetica (EMC) Parte 4: Tecniche di prova e di misura*
CEI EN 61810-1 ed. 11/2008	*Relè elementari elettromeccanici - Parte 1: Prescrizioni generali*
CEI EN 61508 serie ed. 2011	"*Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza"*
CEI EN 61511 ed. 2009	*"Sicurezza funzionale - Sistemi strumentali di sicurezza per il settore dell'industria di processo*

Parte 1: Struttura, definizioni, sistema, prescrizioni per l'hardware e il software"

MIL-HDBK-217F *Reliability prediction of electronic equipment (28/02/1995)*

ISO 2081 *Metallic coatings – Electroplated coatings of zinc on iron*

CEI 20-22 serie *Prove d'incendio su cavi elettrici*

RFI DTC DNS EE SP IFS 177 A (2008) *Sezionamento della linea di contatto e messa a terra di sicurezza per gallerie ferroviarie*

RFI DMA IM TE SP IFS 081A (2008) *Quadro di sezionamento per la messa in sicurezza delle gallerie del sistema a 3 kV d.c.*

RFI DMA IM TE SP IFS 082A (2008) *Dispositivo fisso di corto circuito e messa a terra in sicurezza delle gallerie del sistema a 3 kV d.c.*

RFI DMA IM LA SSE 360 (2005) *Unità periferiche di protezione e automazione – Specifica generale*

RFI TCTS ST TL 05 003 B *Specifica tecnica impianti di telecomunicazione per la sicurezza nelle gallerie ferroviarie TT597*

le apparecchiature di automazione dovranno essere conformi alle seguenti Norme e alle Norme e specifiche citate nei vari paragrafi di questo elaborato:

CEI EN 61131-1 ed. 5/2004 "*Controllori programmabili - Parte 1: Informazioni generali"*

CEI EN 61131-2 ed. 5/2010 "*Controllori programmabili - Parte 2: Specificazioni e prove delle apparecchiature"*

CEI EN 61131-5 ed. 1/2002 "*Controllori programmabili - Parte 5: Comunicazioni"*

CEI EN 61326-2-1 ed. 12/2006 "*Apparecchi elettrici di misura, controllo e laboratorio - Prescrizioni di compatibilità elettromagnetica - Parte 2-1: Prescrizioni particolari - Configurazioni di prova, condizioni di esercizio e criteri di accettazione per apparecchiature di prova e di misura sensibili per applicazioni non protette per l'EMC"*

CEI EN 61326-1 ed. 3/2007 "*Apparecchi elettrici di misura, controllo e laboratorio - Prescrizioni di compatibilità elettromagnetica - Parte 1: Prescrizioni generali"*

CEI EN 61000-6-4 ed. 11/2007 "*Compatibilità elettromagnetica (EMC) - Parte 6-4: Norme generiche - Emissione per gli ambienti industriali"*

CEI EN 61000-6-2 ed. 10/2006 "*Compatibilità elettromagnetica (EMC) - Parte 6-2: Norme generiche - Immunità per gli ambienti industriali"*

CEI EN 60870-5-104 ed. 7/2007	"*Sistemi ed apparecchiature di telecontrollo - Parte 5-104: Protocolli di trasmissione - Accesso alla rete usando profili normalizzati di trasporto per IEC 60870-5-101"*
CEI EN 61508 serie ed. 2/2011	"*Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza"*
CEI EN 61511 serie ed. 2/2007	"*Sicurezza funzionale - Sistemi strumentali di sicurezza per il settore dell'industria di processo*

5. DESCRIZIONE DEL SISTEMA

Il sistema è composto da un quadro contenente un PLC, denominato Q_{GPLC} collegato ad un PC di tipo industriale che funge da supervisione locale del sistema.

Il QGPLC sarà collegato alla rete in F.O insieme alle 2 unità remote, ubicate all'interno dei quadri QPLC, poste in corrispondenza dei due imbocchi.

Ad ogni QPLC, dovranno essere riportati i segnali provenienti dai sezionatori di terra MAT e dalle eventuali apparecchiature connesse al funzionamento del sistema di sezionamento e messa a terra di sicurezza.

Per questa funzione ogni QPLC dovrà essere provvisto di schede di acquisizione di segnali e di schede di uscita; inoltre in ogni sito dovrà essere disponibile un pannello operatore, per permettere la visualizzazione degli stati di tutti i sezionatori MAT della Galleria.

La comunicazione tra le apparecchiature posizionate nel QGPLC e i QPLC avverrà utilizzando il protocollo Ethernet I/P tramite la fibra ottica monomodale presente in galleria. Il sistema di automazione che gestisce la supervisione e il controllo del sistema di messa a terra di sicurezza prevede un'architettura indicata nell'elaborato:

- IV0I00D18DXSM0000011 - Architettura Comando e Controllo

Grazie a questo sistema di automazione gli enti per la messa in sicurezza della galleria saranno comandati, controllati e supervisionati, in condizioni di normale funzionamento, dal posto centrale di comando DOTE attraverso la RTU periferica e il quadro QGPLC.

L'interfaccia tra il sistema PLC ed il terminale periferico di telecomando RTU sarà, verosimilmente, di tipo seriale; il protocollo di comunicazione tra sistema PLC e Terminale periferico di telecomando TE sarà il tipo normalizzato 101.

La messa a terra della galleria potrà avvenire anche per mezzo di comandi diretti sui quadri QMAT situati presso i due accessi alla galleria, modalità quest'ultima che può essere impiegata in condizioni di degrado del sistema in mancato funzionamento del sistema di telecomando (DOTE o RTU).

6. CRITERI DI PROGETTO DEL SISTEMA DI AUTOMAZIONE

Sono qui elencati i criteri generali che dovranno essere rispettati per lo sviluppo e la realizzazione di questo progetto:

- Impiego di tecnologie consolidate, attuali, flessibili, pronte ad evoluzioni e necessità future;
- Utilizzo di reti "aperte" e standard, in particolare hardware di rete basato su Ethernet secondo IEEE 802.3;
- Ridotto numero della tipologia dei componenti adottati e applicazione di soluzioni modulari con conseguente ridotta quantità del numero di parti di ricambio;
- Elevato grado d'isolamento e resistenza a shock e vibrazioni per i moduli di I/O e gli switch;
- Omogeneità delle apparecchiature per poter impiegare un unico strumento di configurazione, programmazione, diagnostica;
- Inizializzazione della comunicazione e trasferimento dati (frame dati minimo 500 byte) sia tramite interrogazione ciclica (polling) che in maniera autonoma (a cambiamento di stato) e ad intervalli di tempo predefiniti senza alcuna interrogazione da parte dei PLC ubicati nel Q_{GPLC};
- Scelta di una tecnologia che permette la rimozione di tutti i moduli sotto tensione;
- Possibilità di diagnosticare gli stati delle singole apparecchiature/schede e delle infrastrutture di rete da parte del Q_{GPLC};
- Copertura delle distanze previste dal progetto;
- Rendere accessibile all'esterno tutti i dati raccolti dal sistema di automazione del sistema MAT dalle varie apparecchiature tramite software commerciali.

7. CARATTERISTICHE TECNICHE

7.1 CARATTERISTICHE DEL SOFTWARE DEL SISTEMA DI AUTOMAZIONE E PRESCRIZIONI PER LA PROGETTAZIONE

Il protocollo del software dovrà essere di tipo “safe” su protocollo Ethernet, adatto all’uso per sistemi di sicurezza certificati SIL3, progettato per conservare l’integrità dei dati durante la comunicazione su rete Ethernet e indipendente quindi dall’architettura della rete in fibra ottica della Galleria e dal tipo di Switch PLC, che possono quindi essere non certificati. Inoltre questo protocollo dovrà essere immune rispetto alla presenza di altri dati non “safe” trasmessi sia dal sistema PLC stesso che da altri sottosistemi che utilizzano la stessa rete Ethernet. Il programma sarà costituito da funzioni di sicurezza e funzioni standard. Le funzioni di sicurezza saranno contenute nelle task dedicate all’esecuzione delle logiche legate al sistema di messa a terra che verranno sviluppate secondo i requisiti SIL 3. Il tempo di esecuzione delle task di sicurezza sarà monitorato mediante apposito watchdog interno impostabile dall’utente. Se la task di sicurezza non verrà eseguita entro il tempo fissato dal watchdog, si genererà un errore irreversibile di sistema e tutti gli output si porteranno automaticamente nella posizione di sicurezza. Le 2 CPU del sistema ubicate nel rack del Q_{GPLC} saranno dedicate all’esecuzione di funzioni standard e di sicurezza. Il sistema comprenderà inoltre I/O relativi alle funzioni di sicurezza e I/O relativi a funzioni standard che saranno trasmessi sulla stessa rete Ethernet senza riduzione del livello di sicurezza delle funzioni di sicurezza.

All’interno del software dovranno essere distinte le funzioni di sicurezza dalle funzioni standard utilizzando task, programmi, routine e variabili separate (per esempio un programma di sicurezza non potrà contenere routine standard ma solo routine di sicurezza). Le routine di sicurezza possono impiegare solo **istruzioni certificate di sicurezza.**

Si noti che, si dovrà prevedere in generale che le funzioni di sicurezza SIL 3 necessitino di incorporare ingressi multipli per sensori e dispositivi doppi di ingresso oltre che ad uscite doppie collegate in serie ed attuatori doppi, tutto questo dove necessario ai fini del calcolo del SIL.

Nello sviluppo del software di sicurezza dovrà essere impiegato personale debitamente qualificato e con esperienza nei sistemi di sicurezza. Il progettista nella preparazione del software svilupperà una specifica della funzione di sicurezza con una descrizione dettagliate che include:

- Sequenza operativa;
- Diagrammi di flusso e dei tempi;
- Diagrammi sequenziali;
- Descrizione del programma;
- Descrizione dei punti da controllare con definizione degli ingressi, delle uscite, degli schemi di cablaggio;
- Principio di funzionamento;
- Tabella delle condizioni degli input e output da controllare con diagrammi delle sequenze e tempi;
- Analisi dei circuiti di campo e determinazione delle ridondanze necessarie per il livello SIL3;
- Posizionamento di sicurezza o a riposo rispettivamente per attuatori e sensori.

Oltre a tutte le verifiche e prove previste dall’ente certificatore indipendente, dovrà essere preparato un apposito piano di test per verificare il task di sicurezza. La prova dovrà essere eseguita simulando i sensori e gli attuatori in campo (prova di sistema).

7.2 SISTEMA DI AUTOMAZIONE UNITA' CENTRALE (Q_{GPLC})

Nel Q_{GPLC} saranno installati 2 (due) rack con a bordo le schede PLC la cui configurazione di dettaglio evidenziata nell'elaborato:

- IV0I00D18DXSM0000011 - Architettura Comando e Controllo

Si noti che il PLC dovrà essere provvisto di una scheda di sincronizzazione per acquisire un segnale orario NTP da rete, in modo tale da ottenere una "marcatura oraria" dei vari eventi sincronizzata relativi a tutte le apparecchiature del sistema.

7.3 SISTEMA DI AUTOMAZIONE UNITA' PERIFERICA (Q_{PLC})

Le caratteristiche tecniche delle unità locali dovranno essere le seguenti:

- Gestione di ingressi discreti e uscite digitali in numero differente in funzione del sito;
- Scheda di rete per la comunicazione su rete Ethernet. Il protocollo di comunicazione su Ethernet sarà di provata affidabilità, di larga diffusione e compatibile direttamente con i PLC;
- Espansione per la gestione eventuale di una seconda porta di comunicazione Ethernet per un eventuale back-up di comunicazione o per il collegamento eventuale di I/O remoti da realizzarsi su un network Ethernet differente da quello primario;
- Diagnostica per prevenire eventuali assegnazioni dello stesso IP node a due nodi della rete;
- Schede d'interfaccia per la connessione degli ingressi ed uscite locali discrete con livello d'isolamento di almeno $2kV_{cc}$;

la configurazione di dettaglio del PLC è evidenziata nell'elaborato:

IV0I00D18DXSM0000011A - Architettura Comando e Controllo

7.4 APPARATI DI COMUNICAZIONE QPLC

Per la gestione della comunicazione attraverso gli altri quadri Q_{PLC} e con il quadro Q_{GPLC}, ogni quadro sarà equipaggiato con uno switch con le caratteristiche conformi alla S.T. RFI "Impianti di telecomunicazione per la sicurezza nelle gallerie ferroviarie TT 597.

7.5 SISTEMA DI SUPERVISIONE

Il sistema di Supervisione Locale sarà costituito da un **Personal Computer Industriale** interfacciato con il QGPLC e la relativa stampante. Per mezzo di questa interfaccia saranno svolte operazioni di monitoraggio del sistema di messa a terra di sicurezza.

Dal punto di vista reti di comunicazione, questo Personal Computer sarà :

- Connesso su proprio switch ai PLC del quadro Q_{GPLC} e connesso quindi alla rete in fibra ottica per la sicurezza in galleria.

- Connesso al Terminale periferico di telecomando attraverso una scheda dedicata con protocollo di comunicazione di tipo cablato attraverso schede di I/O dedicate nel Q_{GPLC}.

Tramite opportuno software di sviluppo saranno implementate l'applicazione grafica e le applicazioni di comunicazione che consentiranno la:

- Rappresentazione a videosinottico dello schema elettrico unifilare relativo all'impianto elettrico con animazione dello stato dei singoli componenti controllati;
- Rappresentazione a videosinottico delle segnalazioni acquisite dal sistema.

Inoltre dovranno essere disponibili tutte le funzionalità di cui al capitolo 8 di questo elaborato.

Il comando dei sezionatori MAT direttamente da PC non dovrà essere previsto direttamente, ma il software dovrà già essere predisposto per l'eventuale attivazione della funzione previo l'inserimento di password.

8. FUNZIONI DEL SISTEMA DI AUTOMAZIONE

Le funzioni che il sistema di automazione dovrà garantire sono le seguenti:

Interfaccia con terminale periferico di telecomando di tutte le apparecchiature legate al sistema di messa a terra di sicurezza localizzate negli imbocchi e negli accessi di emergenza. In questo modo dalla postazione D.O.T.E. del PCS dovrà essere possibile comandare, controllare e supervisionare tutte le apparecchiature del sistema di sezionamento e di messa a terra di sicurezza di tutta la Galleria.

- Visualizzazione sul PC locale collegato al Q_{GPLC} degli stati dei sezionatori MAT e delle apparecchiature a corredo del sistema (rilevatore RV, Q_{CCR}, ecc.) di tutta la *Galleria*;
- Visualizzazione sul PC locale collegato al Q_{GPLC} degli allarmi e delle informazioni diagnostiche delle apparecchiature collegate al sistema di automazione. Il sistema dovrà essere in grado di segnalare con appositi allarmi sia a video che al terminale periferico di telecomando il superamento di soglie di attenzione per la manutenzione (ad esempio superamento del numero di manovre del sezionatore MAT) in modo di aumentare la disponibilità del sistema;
- Registrazione degli eventi su pagina allarme locale con una disponibilità di memoria complessiva equivalente pari mediamente al numero di allarmi che si verificano negli ultimi 12 mesi;
- Capacità di autodiagnostica. Il sistema dovrà essere in grado di fornire sia a monitor dell'unità centrale di supervisione che comunicandolo al terminale periferico di telecomando, tutte le indicazioni sul suo stato, segnalando in tempo reale qualsiasi guasto si possa verificare su di una qualunque scheda che lo compone sia a livello centrale che periferico, con indicazione precisa della scheda guasta e del sito in cui essa è ubicata;
- Visualizzazione su tutti i monitor delle unità remote di tutti gli stati dei sezionatori MAT della *Galleria* con aggiornamento in "real time" (è accettato un ritardo massimo di 2 s). Per questa funzionalità, il PC locale collegato al Q_{GPLC} dovrà essere in grado di ricevere la sincronizzazione oraria da un sistema esterno di riferimento.

Si noti che per tutte le funzioni di visualizzazione/interfaccia sia nel PC collegato al Q_{GPLC} che nei singoli monitor a bordo dei Q_{PLC}, dovranno essere predisposte delle pagine video "attive" a colori per facilitare l'operatore; nel dettaglio nel PC collegato al Q_{GPLC}, dovranno essere presenti: una pagina che rappresenta tutto lo schema TE della *Galleria* + una pagina allarmi/eventi (con riferimento temporale), una pagina che indica la configurazione della rete di controllo con riportati gli eventuali allarmi hardware, delle pagine allarmi dedicate per ognuna delle singole apparecchiature (sezionatori MAT, Q_{CCR}, RV) in cui saranno rappresentati allarmi e dati diagnostici. Nei monitor remoti dovranno essere presenti: una pagina che rappresenta tutto lo schema TE della *Galleria*, una pagina allarmi/eventi del sito.

Dovranno essere possibili diversi livelli accessibilità al software a cui corrisponde l'accessibilità a funzioni protette (configurazione, modifica, comando).

9. COMPOSIZIONE DEL SISTEMA DI AUTOMAZIONE

Dall'analisi del numero dei sezionatori MAT e delle apparecchiature ad essi connessi in ogni sito è scaturito il fabbisogno di tutte le schede I/O necessarie per l'integrazione del sistema.

Nei seguenti elaborati i dettagli:

- IV0I00D18DXSM0000012- Schema quadro QMAT galleria 8 Collecervo/S.Simone - T85-T86
- IV0I00D18DXSM0000013- Schema quadro QPLC galleria 8 Collecervo/S.Simone - T85-T86

forniranno maggiori dettagli sulla schematica elettrica in cui i sistemi dovranno essere inseriti (ad esempio alimentazioni, relè di interfaccia, ecc.).

10. CARATTERISTICHE APPARECCHIATURE IMPIEGATE

Oltre a quanto già indicato nel progetto circa funzionalità e prestazioni del sistema di automazione vengono qui indicate le caratteristiche che sono richieste alle apparecchiature del sistema di automazione (PLC):

1) **Impiego di tutte le apparecchiature per il sistema di automazione, sia del quadro Q_{GPLC} che del Q_{PLC}, e di relè di interfaccia, certificati SIL 3; In alternativa a questi ultimi, relè di interfaccia che consentano di essere impiegati per un progetto SIL3.** Si noti che con riferimento alle apparecchiature attualmente non certificate SIL3 esterne ai quadri Q_{GPLC} e Q_{PLC}, quali sezionatori di terra, Q_{CCR}, Q_{MAT} e relè di tensione, dovranno essere adottate delle modalità di collegamento ridondanti al fine di poter comunque ottenere il livello di sicurezza integrato pari a SIL3 per le funzioni indicate al paragrafo 11 di questo documento

2) Condizioni di funzionamento limite (certificati di prova secondo CEI-EN [IEC] 60068-2/1/2/6/14/27/30, nella revisione più recente):

- Temperatura di funzionamento: -20÷55 °C, 3°C al minuto

  (CEI- EN [IEC] 60068-2-14, prova Nb variazione di temperatura)

  (CEI- EN [IEC] 60068-2-1, prova Ad, freddo)

  (CEI- EN [IEC] 60068-2-2, prova Bd, caldo secco);

- Temperatura di immagazzinaggio: -40÷85 °C

  (CEI- EN [IEC] 60068-2-14, prova Na, 3 ore, 2 cicli)

  (CEI- EN [IEC] 60068-2-1, prova Ab, freddo)

  (CEI- EN [IEC] 60068-2-2, prova Bb, caldo secco);

- Umidità relativa: 5÷95 %, in assenza di condensa, temperatura 15÷55 °C

  (CEI- EN [IEC] 60068-2-30, prova Db, caldo umido)

- Urto durante il funzionamento: 30 g, 11 ms, 6 urti su ciascuno dei 3 assi

  (CEI- EN [IEC] 60068-2-27, prova Ea, urti);

- Urto in condizioni di non funzionamento:

  50 g, 11 ms, 6 urti su ciascuno dei 3 assi;

  (CEI- EN [IEC] 60068-2-27, prova Ea, urti);

- Vibrazioni: 5g, 10÷500 Hz

  (CEI- EN [IEC] 60068-2-6, prova Fc, vibrazioni sinusoidali).

3) CPU:

- Capacità di gestire task continue, periodiche e ad eventi;

- Numero minimo di task in grado di gestire: 32;

- Numero di programmi per ogni task: 100;

- Ogni evento può essere associato ad una task;

- Memoria disponibile 2 MB non volatile;

- Capacità di controllo di almeno 250 connessioni (siti).

4) Scheda Ethernet:

- Velocità di comunicazione: 100 Mbps;

- Capacità di gestire 64 connessioni TCP/IP e 128 con moduli I/O.

5) Schede input digitali:

- Tensione di alimentazione 24V_{cc};
- Intervallo di tensione accettato senza degrado delle prestazioni:19,5÷31V_{cc};
- Ritardo segnale predefinito: 0,25 µs;
- Prova di isolamento: 2 kV_{cc}, 1 minuto;
- Corrente di ingresso minima per l'attivazione del segnale: 1,5 mA;
- Potenza dissipata: 6,2 W a 31V_{cc}.

6) Schede output digitali:

-Schede a relè con contatti di uscita liberi da tensione e isolati singolarmente;

- Corrente nominale per ogni uscita: 3 A a 250 V_{ca};
- Potenza dissipata: 5,0 W a 31V_{cc};
- Prova di isolamento: 2 kV_{cc}, 1 minuto;
- Durata meccanica dei contatti:10.000.000 cicli in assenza di carico, 100.000 a carico nominale.

7) Software inseribili nei quadri Q_{GPLC} e Q_{PLC}:

- Le apparecchiature devono avere caratteristiche ambientali, elettriche e meccaniche identiche agli switch PLC con l'aggiunta della presenza delle funzione P.O.E. (Power Over Ethernet).

Si noti che il collegamento di tutti gli ingressi e le uscite delle schede I/O dovrà essere realizzato attraverso connettori per una facile rimozione delle schede.

Tutte le apparecchiature del sistema di automazione dovranno essere certificate conformi ai seguenti standard:

- IEC 61508 (categoria SIL 3) per utilizzo in funzioni "energized to trip" e "de-energized to trip"
- IEC 61511 (2007)
- EN ISO 13849-1 (2008) (categoria PL e)
- EN 62061 (2011)
- EN 50156-1 (2004)
- EN 61131-2 (2010)
- EN 61000-6-2 (2006)
- EN 61000-6-4 (2007)
- EN 54-2 (1997)/A1(2007)
- NFPA 85 (2011)
- NFPA 86 (2011)

10.1 LOGICHE DI FUNZIONAMENTO Q_{MAT}

In questo paragrafo sarà denominato “quadro locale” il QMAT di cui si preme fisicamente il pulsante a fungo e “quadri remoti” gli altri QMAT.

Sui quadri QMAT è previsto un Pulsante di chiusura a fungo PC adeguatamente protetto contro la pressione intempestiva attraverso una protezione a scatola piombabile. Dal “quadro locale” si attiva la chiusura di tutti i sezionatori di terra della Galleria. Questa funzione verrà eseguita dal sistema di automazione, sia per i “quadri remoti” sia per il “quadro locale”.

Il pulsante di chiusura sarà del tipo con ripristino a chiave. Nel normale funzionamento, la chiave non sarà sul quadro, per cui, una volta premuto un qualunque pulsante, esso resterà in posizione, inibendo, in tal modo, qualsiasi manovra di apertura da remoto (D.O.T.E.). A pulsante premuto sarà possibile eseguire una manovra elettrica di apertura solo dal selettore manulae a bordo del sinottico del QMAT o in ultima analisi della cassa di manovra del sezionatore, la manovella per la manovra manuale sarà alloggiata nella rispettiva cassa di manovra.

Dal Pulsante di Chiusura PC del “quadro locale” la manovra è sempre consentita, ad eccezione dell’interblocco dato dal “BLOCCO del sistema di Controllo Continuità Collegamento al Binario (QCCR)”, in caso non sia riscontrata la continuità di questo collegamento a binario. In tal caso la manovra dovrà comunque essere possibile, per tutti i sezionatori di cui non si è riscontrato tale blocco.

Se in qualunque condizione uno dei “quadri remoti” si troverà con il selettore “Locale-Distante” posizionato su “Locale”, il comando di messa a terra dei sezionatori MAT di quel sito non sarà eseguito.

La lampada di segnalazione di avvenuta messa a terra verde sarà di tipo a led multiplo e si accenderà solamente quando tutti i sezionatori MAT della Galleria saranno nello stato di chiuso con l’aggiunta della verifica positiva (collegamento a rotaia presente) della segnalazione del collegamento a rotaia (QCCR).

11. PROGETTAZIONE DEL SISTEMA E CERTIFICAZIONE DELLE FUNZIONI DI SICUREZZA

Le funzioni di sicurezza di cui si richiede la certificazione sono le seguenti:

a) **Funzione di comando dei sezionatori MAT dell'intera galleria da pulsante del Q_{MAT} (funzione a comando in eccitazione)**
Questa funzione comprenderà: pulsanti a fungo dei Q_{MAT}, sistema di automazione, switch PLC, relè, contattori di uscita, alimentatori e alimentazioni.

b) **Funzione di feedback di posizione di chiuso di tutti i sezionatori di terra (luce verde sul fronte dei Q_{MAT})**
Questa funzione comprenderà: contatti di stato dei sezionatori di messa a terra, sistema di automazione, Q_{CCR}, switch PLC, relè, alimentatori e alimentazioni.

c) **"Funzione luce verde errata**
Questa funzione comprenderà: contatti di stato dei sezionatori di messa a terra, sistema di automazione, Q_{CCR}, switch PLC, relè, alimentatori e alimentazioni.

Si richiede, poi, che venga calcolato il PFH di intervento spurio di anche un solosezionatore di terra, con messa a terra intempestiva della linea di contatto. Il valore del PFH [h^{-1}] risultante dovrà essere ≥ 10^{-9} e < 10^{-8}.

Anche questo calcolo, **seppur non associato ad una funzione di sicurezza**, deve essere oggetto di verifica da parte dell'ente certificatore indipendente.

Il limite entro cui sarà valutata la funzione di sicurezza di cui al punto a, sarà costituito dai contattori di chiusura contenuti nel quadro QMAT, senza considerare la meccanica del sezionatore di terra MAT.

Le apparecchiature coinvolte nelle funzioni da certificare SIL3, seppur diversamente indicato nei vari schemi dei quadri, dovranno essere opportunamente ridondate e impiegate in logiche idonee ad ottenere la certificazione SIL3 per le funzioni sopra elencate. Trattandosi di funzioni realizzate anche con comandi in eccitazione dovranno essere adottati tutti i provvedimenti necessari ad incrementare la copertura diagnostica del sistema. Si citano a titolo di esemplificativo ma non esaustivo: il controllo del circuito dei contatti dei pulsanti di emergenza del Q_{MAT} , il controllo dell'integrità dei circuiti di uscita a lancio della funzione di comando (Funzione a), il controllo dell'integrità del motore del sezionatore, il controllo del led della lampada verde (Funzione b).

Per questa attività di progettazione e certificazione a carico dell''Appaltatore saranno necessarie due differenti figure:

- Il team progettista, che predisporrà il sistema di messa a terra MAT e sarà responsabile del suo corretto sviluppo e completamento fino alla messa in servizio.
- Il rappresentante dell'ente certificatore indipendente, che avrà il compito di verificare e validare quanto progettato e realizzato dal team progettista, e in particolare di certificare SIL3 le 3 funzioni di sicurezza sopra definite secondo le norme CEI EN 61508 e CEI EN 61511 a riferimento. L'ente certificatore indipendente dovrà necessariamente essere un organismo riconosciuto da ANSF (Agenzia Nazionale Sicurezza Ferroviaria) quale verificatore indipendente di sicurezza o perlomeno dovrà aver già intrapreso formale iter per tale riconoscimento.

Infatti, come già indicato, tutto il sistema di automazione dovrà essere progettato e costruito con l'obiettivo di raggiungere il livello di sicurezza integrato SIL3 per le funzioni di sicurezza indicate in questo elaborato. Questo obiettivo dovrà essere raggiunto senza che siano necessarie modifiche alla rete in fibra ottica della galleria, alle modalità di collegamento dei PLC alla rete di riferimento.

La realizzazione e il corretto funzionamento di funzioni safety (SIL3) deve essere indipendente dalla presenza in rete di altri dati non safety appartenenti allo stesso PLC e/o ad altri sottosistemi.

Le macrofasi dell'attività di progettazione sono le seguenti:

- Redazione del progetto di dettaglio (hardware e software) e installazione del sistema di automazione di tutto il sistema MAT secondo le normative a riferimento e in particolare: CEI EN 50126-1, CEI EN 61508 (serie) e CEI EN 61511-1 (serie);
- Predisposizione del software di funzionamento del sistema e delle funzioni di sicurezza con prove del software;
- Prove intermedie di collaudo in fabbrica, di messa in servizio e di attivazione in campo;
- Assistenza all'ente di certificazione a tutte le attività di verifica del progetto e di prova fino all'emissione della certificazione SIL.

La realizzazione del sistema verrà come detto verificata e valutata da un rappresentante di ente certificatore indipendente. Ciò al fine di certificare il livello di SIL effettivamente realizzato delle funzioni di sicurezza indicate in questo elaborato.

L'ente certificatore ha l'obiettivo di eseguire una Valutazione della Sicurezza Funzionale dei sistemi di sicurezza (Functional Safety Assessment) e di rilasciare una "Attestazione di conformità" (certificato) alle clausole delle norme CENELEC 61508 Ed. 2 (seconda Edizione: 2011) ed CENELEC 61511 Ed. 1, ove applicabili.

L'"Attestazione di conformità" (certificato) verrà rilasciata sulla base del Rapporto Tecnico di riferimento redatto a seguito della Verifica e Validazione indipendente (Functional Safety Assessment) dei sistemi strumentati di sicurezza (SIS) nella configurazione proposta dal team progettista in accordo alle clausole delle CENELEC 61508 Ed. 2 ed CENELEC 61511 Ed. 1 (ove applicabili) e Guida CEI 65-186. Fermo restando l'obiettivo di certificare SIL 3 il progetto del sistema di automazione (relè di interfaccia inclusi), il Rapporto tecnico dovrà contenere eventuali raccomandazioni per interventi tecnico/procedurali per migliorare ulteriormente gli obiettivi di sicurezza funzionale.

Questa survey da parte di ente di certificazione indipendente sulla esecuzione delle attività comporterà per il team progettista la necessità di suddividere le fasi di progettazione e realizzazione nei seguenti step:

1. Sviluppo preliminare del progetto e dell'architettura del software;
2. Definizione e ripartizione dei "Requisiti globali di Sicurezza del Sistema" (Safety Requirements Specification" – SRS), dei "Criteri globali di accettazione della sicurezza", dei "Requisiti funzionali della sicurezza" e della "Gestione della sicurezza". Per quanto al software, definizione delle specifiche delle funzioni standard e delle funzioni di sicurezza oggetto della certificazione SIL3 della messa a terra di sicurezza (funzioni Safety). Definizione delle modalità di collegamento safety tra gli enti componenti il sistema MAT;
3. Scrittura di un (functional) "Safety Plan" dedicato in accordo al capitolo 5 delle IEC 61511, includendo le situazioni pericolose, la giustificazione delle scelte di progetto collegate con la sicurezza, il controllo dei sub fornitori, Preparazione del dossier della sicurezza;
4. Sviluppo dei "Safety Requirements Specification";
5. Meeting con Italferr per discutere i dettagli dell'SRS e del Safety Plan del progetto;
6. Modifiche al Safety Plan ed all'SRS come definito nel meeting;
7. Scrittura di un hardware concept design (subsistem design) per il SIS (sistema strumentale di sicurezza) e verifica;
8. Meeting con Italferr per discutere i dettagli dell'HW concept design e del progetto;
9. Modifiche all'HW concept design;
10. Calcolo del SIL per le funzioni safety e del PFH per l'intervento spurio di un solo sezionatore di messa a terra;
11. Scrittura dell'application software concept design;
12. Controllo dell'application software concept design;
13. Effettuazione del validation test nelle modalità concordate con Italferr e l'ente certificatore.

Per tutte queste fasi il team progettista dell'Appaltatore dovrà produrre i documenti corrispondenti. Inoltre, sempre ai fini dell'attività di certificazione, l'Appaltatore dovrà in generale produrre la seguente documentazione tecnica e fornire i dati qui specificati (nel corso delle attività verrà stabilito l'esatto elenco con l'ente certificatore):

a) Documentazione tecnica di progetto: Descrizioni di processo funzionale, Matrici Causa/effetto, Architettura del progetto e schemi funzionali con relativa descrizione operativa e requisiti di sicurezza funzionale, schemi topografici e costruttivi (Rif. CEI-EN 61511-1, §10.3), loops diagram, specifiche componenti e sottosistemi che costituiscono il sistema di messa a terra;
b) Dati relativi ai ratei di guasto (dati estratti dai test di prova periodica dal campo, rapporti tecnici di conformità alle Norme utilizzate, Manuali operativi dei componenti e sottosistemi, Manuali di Manutenzione, ecc.) dei componenti utilizzati nel progetto ed informazioni sul software applicativo relativo alle funzioni e logiche di sicurezza implementate nel Logic Solver (tipologia e numero di applicazioni simili installate e periodo operativo);
c) Specificazione in termini qualitativi e quantitativi dei limiti di Batteria dell'Impianto, definizione delle funzioni di sicurezza;
d) Specifiche di prova del FAT e del SAT.

Sulla base di questa documentazione l'ente certificatore indipendente avrà a suo carico di sviluppare la sua azione che includerà:

1. Valutazione della idoneità della società e del team progettista che eseguirà lo sviluppo del progetto;
2. Meeting con definizione di tutte le attività da sviluppare insieme ai rappresentanti Italferr e al team progettista Appaltatore;
3. Analisi dei dati di campo ai fini della stima dei failure rates e delle specifiche di sicurezza funzionale, "Pre-verifica e successiva "Verifica" (calcolo) del SIL e PFDavg e PFH in relazione all'architettura e documentazione definita nel progetto e delle caratteristiche della componentistica dei materiali, dei sottosistemi (Pannelli locali, sezionatori, ecc.).
4. Il calcolo del SIL della Funzione di comando dei sezionatori MAT dell'intera galleria da pulsante del QMAT (funzione a comando in eccitazione), dovrà essere eseguito per due differenti perimetrazioni: quella prevista in questo elaborato, che dovrà essere certificata SIL3 e quella che include anche i sezionatori di terra;
5. Emissione di un rapporto di commenti (eventuale) con le indicazioni (Fase di pre-verifica);
6. Emissione di Attestato di conformità (certificato) alle Norme CEI-EN 61508 Ed. 2 e CEI-EN 61511 Ed. 1, del livello di SIL delle 3 funzioni di sicurezza;
7. Informazioni su organizzazione manutenzione ed esercizio;
8. Indicazione di eventuali vincoli per le attività di verifica periodica e tempi di manutenzione programmata (ad esempio: possibilità e frequenza massima ammissibile di conduzione test di funzionalità anche parziale, procedure da eseguire in caso di fuori servizio parziale del sistema, attività di revisione delle apparecchiature);
9. Qualificazione degli Operatori dedicati alle attività di manutenzione routinaria e periodica.

9bis. Calcolo del livello SIL della funzione di comando dei sezionatori MAT dell'intero sistema galleria, da pulsante del QMAT includendo nella perimetrazione anche il sezionatore MAT.

10. Tutta la documentazione prodotta dall'ente certificatore indipendente e che verrà fornita ad Italferr dovrà essere conforme a quanto richiesto dalle CEI-EN 61508/61511; e dovrà inoltre includere oltre a quanto sopra evidenziato quanto segue:
11. Raccomandazioni per l'eventuale adeguamento delle specifiche tecniche alle revisioni condotte dall'ente stesso;
12. Documentazione per la gestione delle verifiche periodiche dei sistemi di sicurezza e per le modalità di esecuzione;
13. Aggiornamento dei Safety Manuals per i sistemi di sicurezza e il supporto per l'aggiornamento del Manuale della Gestione delle Emergenze;
14. Assunzioni utilizzate per la determinazione del SIL (PF Davg, PFH dangerous);
15. Assessment Specifiche dei requisiti di Sicurezza funzionale;
16. Assessment logiche di sicurezza applicative;

17. Assessment documentazione di progetto per le parti di revisione);
18. Informazioni per eventuali modifiche (procedure);

Si noti che nel corso della fase di certificazione da parte dell'ente certificatore indipendente verrà concordato un piano di prove intermedie e finali tutte già comprese e compensate in questo progetto. Nel corso della fase di collaudo del sistema di automazione in fabbrica verrà eseguita comunque una prova di funzionalità della logica del sistema con una composizione di apparecchiatura da ritenersi significativa a cura dell'ente certificatore.

12. DOCUMENTAZIONE E PROVE

Tutte le schede, apparecchiature e software saranno provvisti di documentazione di prova secondo le norme a riferimento, dei manuali utente e delle istruzioni operative del sistema realizzato.

Tutta la documentazione sarà in lingua italiana.