COMMITTENTE:

RFI RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE

PROGETTAZIONE:

ITALFERR
GRUPPO FERROVIE DELLO STATO ITALIANE

INFRASTRUTTURE FERROVIARIE STRATEGICHE DEFINITE DALLA LEGGE OBIETTIVO N. 443/01 e s.m.i

S.O. ENERGIA E TRAZIONE ELETTRICA

PROGETTO DEFINITIVO

NODO DI BARI

BARI NORD - VARIANTE SANTO SPIRITO PALESE

IMPIANTI STES

IMPIANTO STES GALLERIA GA04
Relazione Generale di Sistema comando e controllo, progettazione e certificazione funzioni di sicurezza

SCALA: -:-

COMMESSA	LOTTO	FASE	ENTE	TIPO DOC.	OPERA/DISCIPLINA	PROGR.	REV.
IADR	00	D	18	RO	SM0200	001	A

Rev.	Descrizione	Redatto	Data	Verificato	Data	Approvato	Data	Autorizzato Data
A	Emissione Esecutiva	L. Mutolo	09/2023	V. Vaccaro	09/2023	G. Dimaggio	09/2023	G. Guidi Buffarini 09/2023

ITALFERR S.p.A. U.O. Tecnologie Centro Ing. Guido Guidi Buffarini Ordine Ingegneri Provincia di Roma n° 15812

File: IADR00D18ROSM0200001A.dwg

INDICE

1. OGGETTO

Oggetto del presente elaborato è la descrizione del sistema di automazione dedicato al sezionamento e messa a terra di sicurezza del sistema di galleria *GA04* (3155 m).

In questo elaborato si vogliono descrivere, oltre alle 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 del sistema *Galleria* 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 al fine di espletare quanto previsto dalla norma CEI EN 50159;
- Possibilità di evitare lunghi e costosi cablaggi in galleria per i sezionatori MATS e le apparecchiature connesse al sistema di messa a terra di sicurezza;
- Sviluppo di un sistema innovativo, inserito nella specifica RFI DTC ST E SP IFS TE 150 A "S*istema per il sezionamento della linea di contatto e messa a terra di sicurezza per gallerie ferroviarie*", che prevede di realizzare sistemi di controllo remoto in sicurezza.

In particolare, si prevede che l'Appaltatore progetti e realizzi questo sistema inserendo le funzioni di sicurezza, da certificare SIL4, secondo le norme di cui al paragrafo 4 del presente elaborato.

E' previsto inoltre, sempre a carico dell'Appaltatore, che l'intero sistema locale di messa a terra (hardware, software, quadri e apparecchiature), venga, per le sue funzioni di sicurezza, certificato SIL 4 secondo le normative CEI EN 50126, CEI EN 50128 e CEI EN 50129 da ente indipendente.

Visti i contenuti specifici di questa attività, la società che eseguirà questo progetto di sicurezza dovrà documentare 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

- *MATS:* Messa A Terra di Sicurezza
- SIL: Livello di integrità di sicurezza
- BI: Funzione (bistabile) di bloccamento delle manovre dei DMBC
- ChE: Chiave elettromeccanica per l'ingresso in galleria
- DMBC: Dispositivo Motorizzato Bipolare di Cortocircuito per sistemi a 3 kV
- DOTE: Dirigente Operativo Trazione Elettrica – Gestore del posto centrale di telecomando/telecontrollo degli impianti di trazione elettrica di giurisdizione
- Fabbricato 1/2: Fabbricato Tecnologico di Imbocco 1/2
- iDOTE: Interfaccia verso il DOTE
- IMS: Interruttore di manovra-sezionatore (detto anche sezionatore longitudinale di linea)
- iSPVI: Interfaccia verso SPVI
- QCC: Quadro Controllo Continuità LdC a rotaia/terra
- QS: Quadro Squadre di Soccorso
- Sistema STES: Insieme di apparecchiature e relativi collegamenti per la realizzazione del sezionamento elettrico e alla messa a terra di sicurezza della la linea di contatto. (Nella presente relazione verranno utilizzati gli acronimi STES e MATS con identico significato)
- SPDT: Contatto in commutazione, libero da tensione, di un relè
- SPVI: Centro di supervisione dell'intero sistema di sicurezza di galleria, ubicato in prossimità di un imbocco
- UCP: Unità di Comando e Controllo Principale per Enti TE
- UCS: Unità di Comando e Controllo Secondaria per Ente, o gruppo di Enti TE
- UCS-DMBC: Unità di Comando e Controllo Secondaria per DMBC e QCC

- UCS-IMS: Unità di Comando e Controllo Secondaria per IMS
- UCS-QS: Unità di Comando e Controllo Secondaria per QS
- Rete Ethernet TLC: Rete Ethernet in fibra ottica monomodale realizzata a cura di altra specialistica.
- Switch TLC: Switch conforme alla specifica TT597 che realizza l'anello TLC principale della galleria
- 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 MATS" (IADR00D18RGSM0000001A), le apparecchiature di automazione dovranno essere conformi alle seguenti Norme e alle Norme e specifiche citate nei vari paragrafi di questo elaborato:

RFI DMA PS IFS 44 A del 07.02.2007 (Procedura Subdirezionale)
"Attività di "Verifica dei requisiti di affidabilità, manutenibilità e disponibilità nella fase di omologazione del prodotto."

RFI DTC ST E SP IFS TE 120
"Apparato per il controllo e monitoraggio della continuità della linea di contatto/feeder in corto circuito"

RFI DPRIM STF IFS TE 143
"Relè elettrici a tutto o niente per impianti di energia e trazione elettrica."

RFI DPRIM STF IFS TE 146
"Dispositivo motorizzato bipolare di cortocircuito per il sistema di trazione a 3 kVcc."

RFI DTC ST E SP IFS TE 150 A
"Sistema per il sezionamento della linea di contatto e messa a terra di sicurezza per gallerie ferroviarie."

RFI DTC DNS EE SP IFS 177
"Sezionamento della linea di contatto e messa a terra di sicurezza per gallerie ferroviarie (DM 28.10.2005)."

RFI DPRIM STF IFS TE 95
"Complessi a 3kVcc, per esterno e/o all'interno di quadri elettrici di protezione elettrica TE."

RFI DMA IM LA SP IFS 363
"Sistema di rilevazione voltmetrica (RV) per monitoraggio e protezione delle linee di trazione a 3kVcc."

DI TCSS ST IS 00 402
"Prove di Tipo e di Accettazione per le apparecchiature elettroniche ed elettromeccaniche destinate agli impianti di sicurezza e segnalamento."

RFI DMA IM LA LG IFS 500

"Sistema di governo per impianti di trasformazione e distribuzione energia elettrica."

RFI DTCSTSSSTB SR IS 20 039

"Sistema per la Trasmissione Dati in Sicurezza per impianti di Segnalamento (TDS)."

RFI DTC DNS SS RT IS05 021

"Protocollo Vitale Standard."

RFI TCTS ST TL 05 003 B

"Specifica tecnica impianti di telecomunicazione per la sicurezza nelle gallerie ferroviarie TT597."

C.G.A

"Condizioni Generali di Contratto per le forniture RFI approvate dal C.d.A.- Delibera 590/87" e successive modifiche e integrazioni."

RFI TC PR IS 00 009 A del 26/09/03

"Applicazione della Normativa CENELEC di Settore allo sviluppo e realizzazione di prodotti e sistemi elettronici ferroviari in sicurezza per il segnalamento ferroviario."

Disposizione n.32 del 12.11.2002 e sua modifica n.52 del 12.11.2007

"Applicazione della normativa CENELEC di settore allo sviluppo e realizzazione di prodotti elettronici in sicurezza per il segnalamento ferroviario."

CEI EN 50126

"Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane - La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS)."

CEI EN 50128

"Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane - Sistemi di telecomunicazione, segnalamento ed elaborazione - Software per sistemi ferroviari di comando e di protezione."

CEI EN 50129

"Applicazioni ferroviarie, tranviarie, filotramviarie e metropolitane: Sistemi di comunicazione, segnalamento ed elaborazione – Sistemi elettronici di sicurezza per il segnalamento."

CEI EN 50159

"Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane – Sistemi di telecomunicazione, segnalamento ed elaborazione – Comunicazioni di sicurezza in sistemi di trasmissione"

CEI EN 61508 serie

"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."

UNI EN ISO 9001

"Modello per l'assicurazione della qualità nella progettazione, sviluppo, fabbricazione, installazione ed assistenza."

CEI EN 61131-1 Serie

"Controllori programmabili"

CEI EN 61326 Serie

"Apparecchi elettrici di misura, controllo e laboratorio - Prescrizioni di compatibilità Elettromagnetica"

CEI EN 61000 Serie

"Compatibilità elettromagnetica (EMC)"

CEI EN 60870-5-104 ed. 7/2007

"Sistemi ed apparecchiature di telecontrollo"

5. DESCRIZIONE DEL SISTEMA

Il sistema è composto da:

- vari dispositivi motorizzati di cortocircuito (DMBC) per il collegamento di ciascuna sorgente di alimentazione alla rotaia. Ogni DMBC è corredato da un quadro di controllo continuità (QCC);
- un'unità di controllo secondaria (UCS-DMBC) in corrispondenza di ciascun sezionatore di terra (DMBC);
- due unita di controllo principale, denominate UCP, ciascuna posta all'interno dei fabbricati tecnologici presenti presso gli imbocchi principali della galleria. Una delle due UCP è collegata direttamente al DOTE;
- un'unità di controllo secondaria (UCS-QS) in corrispondenza di ogni imbocco e di ogni punto di accesso delle squadre di emergenza;
- un'ulteriore unità di controllo secondaria (UCS-QS) presso il DOTE di competenza;
- eventuali sezionatori di linea (IMS) per la disalimentazione della linea di contatto;
- un'eventuale unità di controllo secondaria (UCS-IMS) in corrispondenza di ciascun sezionatore di linea (IMS);
- il collegamento in fibra ottica fra tutte le unità di controllo sia primarie (UCP) che secondarie (UCS);
- il collegamento fra tutte le unità di controllo principali (UCP) attraverso la rete trasmissiva esterna RFI.

Le unità di controllo principali (UCP) saranno collegate, tramite la rete in F.O. prevista nell'ambito della specialistica TLC, alle varie unità secondarie (UCS), ubicate presso i sezionatori di messa e terra (UCS-DMBC), presso eventuali sezionatori di linea (UCS-IMS) e presso tutti accessi delle squadre di emergenza (UCS-QS).

Ad ogni UCS-DMBC dovranno essere riportati i segnali provenienti dai sezionatori di terra DMBC e dalle altre apparecchiature connesse al funzionamento del sistema di sezionamento e messa a terra di sicurezza della galleria (QCC).

Per questa funzione, ogni UCS-DMBC 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 DMBC dell'intero sistema galleria.

Ad ogni UCS-IMS dovranno essere riportati i segnali provenienti dai sezionatori di linea

IMS. Per questa funzione, ogni UCS-IMS dovrà essere provvisto di schede di acquisizione di segnali e di schede di uscita.

Il Sistema/Rete per la trasmissione dati del sistema STES deve essere conforme ai requisiti di base specificati nella norma CEI EN 50159.

Il sistema STES deve essere inoltre predisposto per comunicare con ulteriori sistemi esterni tramite il TDS e il protocollo vitale standard RFI definiti nei documenti rispettivamente RFI DTCSTSSSTB SR IS 20 039 e RFI DTC DNS SS RT IS05 021.

Il sistema di automazione che gestisce la supervisione e il controllo del sistema di messa a terra di sicurezza prevede una duplice architettura, indicata negli elaborati:

- IADR00D18DXSM0200002A “Architettura Comando e Controllo”

Il Sistema STES deve essere predisposto per l’interfacciamento con il DOTE tramite il protocollo IEC60870-5-104 o morsettiera “Z” in uso negli impianti di RFI (per quanto applicabile si faccia riferimento anche al documento RFI TC TE ST SSE DOTE 1 Ed. 2001).

Le informazioni minime da inviare al DOTE sono le seguenti:

- stato di aperto/chiuso di tutti i dispositivi IMS e DMBC;
- stato di messa a terra bloccata del Sistema STES con l’indicazione di tutti i relativi bloccamenti;
- stato di disalimentazione proveniente da ogni singolo RV;
- stato di alimentazione proveniente da ogni singolo RV;
- regime di telecomando Incluso/Escluso dall’UCP;
- Esclusi/Inclusi comandi remoti dalle singole UCS interessate;
- normalità chiavi ChE nei QS;
- stati chiave ChE e relativa ubicazione;
- mancanza alimentazione armadi/enti TE.

La messa a terra della galleria potrà avvenire anche per mezzo di comandi diretti sui quadri UCS-DMBC situati in corrispondenza dei sezionatori STES, modalità quest’ultima che può essere impiegata in condizioni di degrado del sistema, in mancato funzionamento del sistema di telecomando.

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 nei vari quadri;
- 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 dei quadri UCP;
- 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 SIL 4, 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 TLC e 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 4. 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 CPU del sistema ubicate nei quadri 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 4 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 dettagliata 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 SIL4;
- 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, a cura appaltatore/progettista, 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 UNITA' DI COMANDO E CONTROLLO PRINCIPALI (UCP)

L'Unità di Comando e Controllo Principale (UCP), ha la duplice funzione di:

- interfaccia di comando e controllo degli enti verso i sistemi di livello superiore (DOTE);
- piattaforma di configurazione e diagnostica del sistema in locale.

Pertanto, ogni quadro UCP avrà bordo delle schede PLC la cui configurazione di dettaglio evidenziata nell'elaborato:

- "Schema quadro UCP" (cod. IADR00D18DXSM0000001) di questo progetto.

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" sincronizzata dei vari eventi relativi a tutte le apparecchiature del sistema.

La generica UCP del Sistema STES si può trovare nei due seguenti stati:

- TIncl = Telecomando Incluso;
- TEscl = Telecomando Escluso.

Ciascuna Unità di Comando e Controllo Principale (UCP) del Sistema STES, in base a tale stato, può effettuare i seguenti comandi verso tutti gli enti TE gestiti:

- nello stato TIncl (stato di normale gestione dell'impianto) devono essere:
  - abilitati tutti i comandi verso gli enti TE gestiti dallo STES, compreso il macrocomando di messa in sicurezza della galleria ed il macrocomando di "Sbloccamento" (solo quando tutte le chiavi ChE risultano nella posizione 1), provenienti dal DOTE;
  - inibiti tutti i comandi di Chiusura/Apertura degli enti DMBC da qualunque Unità UCP del Sistema STES;
  - inibiti tutti i comandi di chiusura degli enti IMS da qualunque Unità UCP del Sistema STES;
  - abilitati tutti i comandi di Apertura degli enti IMS da qualunque Unità UCP del Sistema STES;
  - abilitata la richiesta verso il DOTE di entrata nello stato di Esclusione Telecomando (TEscl) da una qualunque Unità UCP del Sistema STES. A seguito dell'autorizzazione da parte del DOTE, l'UCP richiedente, e solo quella, viene configurata in TEscl. L'altra UCP, in questo caso, viene impossibilitata ad eseguire la medesima richiesta al DOTE;
  - predisposto ad accettare tutti i comandi o solo quelli configurati (in base alle disposizioni vigenti), verso gli enti TE del Sistema STES da parte del Sistema SPVI. Tali eventuali comandi per default devono essere tutti disattivati;

- inibito il macrocomando di messa in sicurezza della galleria ed il macrocomando di Sbloccamento, da qualunque Unità UCP del Sistema STES;
- abilitato il macrocomando di messa in sicurezza della galleria da qualunque quadro QS, a seguito della rotazione della relativa chiave ChE;
- visualizzazione dello stato di tutti gli enti TE gestiti dallo STES da tutte le UCP, dal DOTE e dal sistema SPVI.

- nello stato TEscl (tale stato può essere attivato, solo da personale autorizzato, su una determinata UCP alla volta tramite abilitazione dal DOTE) devono essere:
  - abilitati tutti i comandi verso gli enti TE gestiti dallo STES, compreso il macrocomando di messa in sicurezza della galleria ed il macrocomando di Sbloccamento (solo quando tutte le chiavi ChE risultano nella posizione 1), dalla relativa unità UCP che risulta essere abilitata dal DOTE;
  - inibiti tutti i comandi provenienti da DOTE;
  - inibiti tutti i comandi, se abilitati, provenienti da SPVI;
  - inibiti tutti i comandi provenienti dalle altre Unità UCP del Sistema TE;
  - inibita la gestione della richiesta di TEscl da un'altra UCP diversa da quella abilitata dal DOTE;
  - visualizzazione dello stato di tutti gli enti TE gestiti dallo STES da tutte le UCP, dal DOTE e dal sistema SPVI.

La richiesta di passaggio dallo stato TIncl a TEscl o viceversa, dovrà avvenire con metodo di richiesta e approvazione dal DOTE.

7.3 UNITA' DI CONTROLLO SECONDARIE (UCS)

Le funzioni principali di ogni UCS sono:

- interfaccia verso le UCP del Sistema STES;
- il controllo, comando e diagnostica, in particolare, di:
  - UCS-IMS;
  - UCS-DMBC e del QCC relativo;
  - UCS-QS.

L'insieme composto da ChE, UCS-QS, UCS-DMBC e dispositivo per la verifica della sicura messa in corto circuito/messa a terra della LdC (QCC), deve essere realizzato secondo i requisiti delle normative che esprimono i requisiti dei sistemi a SIL4 in ambito ferroviario richiamate nel par. II.6 della specifica RFI DTC ST E SP IFS TE 150 A.

Per quanto riguarda gli enti costituenti il sistema le realizzazioni devono essere modulari e facilmente manutenibili.

Per le UCS-QS e UCS-DMBC è richiesta una architettura del tipo 2oo3D o equivalente, tale da garantire il funzionamento e l'integrità SIL4 anche in modalità degradata, ovvero tolleranza al primo guasto di uno qualunque dei suoi moduli componenti: Alimentatore, CPU, Scheda I/O, Scheda di comunicazione, ecc.

Inoltre, nel Sistema STES è prevista la UCS-IMS, qualora tali IMS siano gestiti da tale sistema, che permette il comando e controllo dei sezionatori IMS di linea, sia da UCP che da remoto tramite DOTE.

Per tali UCS-IMS è richiesta una architettura del tipo 1oo2D o equivalente, tale da garantire il funzionamento anche in modalità degradata, ovvero tolleranza al primo guasto di uno qualunque dei suoi moduli componenti: Alimentatore, CPU, Scheda I/O, Scheda di comunicazione, ecc.

Ad ogni unità UCS-QS devono pervenire le seguenti informazioni:

- l'avvenuta messa in corto circuito/messa a terra della LdC da tutte le unità UCS-DMBC presenti;
- l'avvenuto bloccamento delle manovre dei DMBC da tutte le unità UCS-DMBC presenti.

Le azioni di sezionamento e messa in corto circuito della LdC, di bloccamento delle manovre dei DMBC devono avvenire a seguito della rotazione dell'elettrochiave ChE. L'UCS-QS acquisisce tale rotazione della chiave ChE e, mediante la rete dati interna alla galleria e/o a quella di richiusura esterna, la trasferisce a tutte le restanti unità UCS del Sistema STES (UCS-DMBC/IMS).

7.4 QCC

Il QCC deve essere in grado controllare in sicurezza la presenza e la corretta connessione dei cavi di collegamento dei DMBC alla rotaia e della presenza e corretta connessione dei cavi di collegamento dei DMBC alla linea di contatto attraverso la corretta chiusura delle lame dei DMBC stessi, verificando di fatto la continuità tra linea di contatto e rotaia una

volta che il DMBC è stato chiuso.
Il QCC dovrà essere realizzato in conformità alla specifica RFIDTCSTESPIFSTE120A.
Il costruttore deve garantire il corretto funzionamento di ogni singolo apparato dei QCC e la durata della loro vita attesa; si richiede quindi:

- MTBF del singolo apparato CC comprensivo dei Tx/Rx ..... : > 200000 ore;
- MTTR del singolo apparato (escluso i Tx/Rx) ..... : < 30 min;
- MTTR (restanti parti) ..... : < 60 min;
- MTBF del singolo Alimentatore ..... : > 200000 ore.

Il fornitore dovrà fornire una dettagliata dimostrazione del fatto che l'affidabilità, calcolata secondo quanto riportato sul documento MIL-HDBK-217F (o analogo), rispetti i precedenti valori definiti per una temperatura di 40°C e condizioni ambientali Ground Fixed elaborati con metodologia Part stress.

Il fornitore dovrà, inoltre, dimostrare che il comportamento dell'apparecchiatura è conforme a quanto previsto nelle EN 50126, EN 50128 e EN 50129, fornendo anche i report di prova.

Il QCC deve garantire il livello di integrità SIL 4 per le seguenti funzioni:

- Rilevazione cavo interrotto;
- Tempo per rilevazione cavo interrotto;
- Tensione massima del segnale di consenso assente;
- Indipendenza dei ricevitori di maglie diverse.

Tenuto conto del fatto che il QCC sarà inserito in un sistema di controllo in sicurezza con livello di integrità di sicurezza complessivo SIL 4, il Fornitore dovrà dimostrare, in conformità alle prescrizioni indicate nella norma EN 50129, che il livello di THR non sia superiore a 10^{-11} per ogni apparato di controllo (CC-) del QCC.

Si ribadisce che ciascun apparato di controllo della continuità (CC-) deve garantire singolarmente le funzioni e relativi livelli di integrità elencati nella tabella precedente, anche in caso della perdita della ridondanza 1oo2 prevista dalla specifica RFI DTC ST E SP IFS TE 120A.

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 presso i vari accessi della galleria. In questo modo, dalle UCP ubicate all'interno dei fabbricati tecnologici (e anche dalla postazione D.O.T.E.) dovrà essere possibile comandare, controllare e supervisionare tutte le apparecchiature del sistema di sezionamento e di messa a terra di sicurezza della Galleria;
- Visualizzazione, sui panel view delle UCP, e anche al DOTE, degli stati dei sezionatori MAT e delle apparecchiature a corredo del sistema (rilevatore RV, QCC, ecc.) di tutta la Galleria;
- Visualizzazione, sui panel view delle UCP, e anche al DOTE, 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 da 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 in 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 (DOTE), 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 panel view delle UCP 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, i PLC delle UCP dovranno essere in grado di ricevere la sincronizzazione oraria da un sistema esterno di riferimento.

Si noti che per tutte le funzioni di visualizzazione/interfaccia su tutti i panel view delle UCP, dovranno essere predisposte delle pagine video “attive” a colori per facilitare l’operatore; nel dettaglio, sui suddetti panel view, 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, QCC, RV) in cui saranno rappresentati allarmi e dati diagnostici. Su eventuali altri 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. LOGICHE DI FUNZIONAMENTO DEL SISTEMA STES

In caso di emergenza, per eseguire per la messa a terra della linea di contatto è necessario che un operatore si rechi in prossimità di uno dei quadri UCS-QS e ruoti la chiave ChE in senso orario, dalla posizione 1 alla posizione 2.

A tal punto il sistema di automazione:

1. Consente alle varie UCS e UCP di acquisire l’evento.
2. Effettua le manovre di apertura di tutti gli eventuali IMS esterni (sezionamento delle fonti di alimentazione).
3. Effettua le manovre di chiusura di tutti i dispositivi di messa a terra DMBC anche in caso di mancata apertura di uno o tutti gli IMS.

4. Controlla tramite i QCC che, in tutti i DMBC, la LdC sia sicuramente collegata alla Rotaia/Terra.

5. Opera il bloccamento nella posizione di chiuso di tutti i DMBC, inibendone qualsiasi manovra compreso quella manuale.

6. In caso di esito positivo delle operazioni descritte ai punti 4 e 5, aggiorna su tutti i quadri QS il nuovo stato di “Galleria a Terra Bloccata”; Attiva le segnalazioni luminose, indicanti che la galleria sia realmente a terra, su tutti i QS; Attiva la segnalazione acustica, indicante che la galleria sia realmente a terra, sul quadro QS dove sia avvenuta la rotazione della elettrochiave ChE (per indicare all’operatore che la chiave può essere estratta).

7. Alimenta l’elettromagnete di sblocco per la liberazione della chiave ChE.

8. Consente all’operatore di ruotare la chiave ChE, in senso orario, dalla posizione 2 alla posizione 3 e di estrarla.

9. A seguito dell’estrazione della chiave il sistema di automazione effettua la tacitazione della segnalazione acustica.

Qualora la messa in sicurezza della galleria (apertura degli IMS esterni e chiusura di tutti i DMBC) sia già stata comandata da DOTE/UCP1/2, l’operatore dovrà comunque ruotare la predetta elettrochiave ChE, presente sul quadro UCS-QS, per accedere alla galleria.
A seguito dell’estrazione di una o più elettrochiavi ChE, dopo aver espletato le operazioni del caso, il Sistema STES potrà essere ripristinato con la seguente procedura di esclusiva competenza di un operatore RFI dopo aver stabilito le condizioni per il ripristino:

1. Reinserzione di tutte le elettrochiavi ChE nelle rispettive sedi riportandole in posizione 1; Il Sistema STES acquisisce il nuovo stato delle ChE senza operare alcuna manovra.

2. Comando di Sbloccamento da UCP/DOTE. Tale comando opera la riabilitazione di tutte le manovre di tutti i DMBC del Sistema STES. Tale funzione di Sbloccamento non dovrà operare nessuna manovra degli enti.

Dopo aver operato la funzione di Sbloccamento suddetta gli enti TE ritornano ad essere gestibili normalmente da DOTE.

10. PROGETTAZIONE DEL SISTEMA E CERTIFICAZIONE DELLE FUNZIONI DI SICUREZZA

Le funzioni di sicurezza di cui si richiede la certificazione SIL 4 sono le seguenti:

a) Controllo LdC messa in corto circuito (per ogni singola UCS-DMBC)

Questa funzione comprenderà: selettore a chiave (ChE), sistema di automazione, quadro QCC, switch TLC e PLC, relè, contattori di uscita, alimentatori e alimentazioni, lampada gialla.

b) Manovra di riapertura DMBC Bloccata (Bloccamento) (per ogni singola UCS-DMBC)

Questa funzione comprenderà: selettore a chiave (ChE), sistema di automazione, quadro QCC, switch TLC e PLC, relè, contattori di uscita, alimentatori e alimentazioni, lampada verde.

c) Consenso all'Estrazione ChE (per ogni singola ChE)

Questa funzione comprenderà: selettore a chiave (ChE), sistema di automazione, switch TLC e PLC, relè, contattori di uscita, alimentatori e alimentazioni, lampada verde.

Si richiede, poi, che venga calcolato il PFH di intervento spurio di anche un solo sezionatore di terra, con messa a terra intempestiva della linea di contatto. Il valore del PFH [h^{-1}] risultante dovrà essere $\geq 10^{-9}$ 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.

Le apparecchiature coinvolte nelle funzioni da certificare SIL4, seppur diversamente indicato nei vari schemi dei quadri, dovranno essere opportunamente ridondate e impiegate in logiche idonee ad ottenere la certificazione SIL4 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.

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 SIL4 le 3 funzioni di sicurezza sopra definite secondo le norme 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 SIL4 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, al tipo di Switch TLC e alle modalità di collegamento dei PLC alla rete di riferimento. L'architettura della rete del sistema PLC è rappresentata negli elaborati IADR00D18DXSM0200002A (Architettura Comando e Controllo).

La realizzazione e il corretto funzionamento di funzioni safety (SIL4) 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, CEI EN 50128, CEI EN 50129, CEI EN 61508 e CEI EN 61511;
- 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 CEI EN 50126, CEI EN 50128, CEI EN 50129, e CEI EN 61508, CEI EN 61511, 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 suddette norme. Fermo restando l'obiettivo di certificare SIL 4 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 e la verifica e la validazione del calcolo del PFH dell'intervento spurio di messa a terra di un solo sezionatore.

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 Requirement Specification" – SRS), dei "Criteri globali di accettazione della sicurezza", dei "Requisiti funzionali della sicurezza" e della "Gestione della sicurezza". Riguardo al software, definizione delle specifiche delle funzioni standard e delle funzioni di sicurezza oggetto della certificazione SIL4 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 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 dovrà, a suo carico, 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 PFH in relazione all'architettura e documentazione definita nel progetto e delle caratteristiche della componentistica dei materiali, dei sottosistemi (Pannelli locali, sezionatori, ecc).

4. Emissione di un rapporto di commenti (eventuale) con le indicazioni (Fase di pre-verifica);
5. Emissione di Attestato di conformità (certificato) alle Norme CEI EN 50126, CEI EN 50128, CEI EN 50129, CEI EN 61508 e CEI EN 61511, del livello di SIL delle 3 funzioni di sicurezza;
6. Informazioni su organizzazione manutenzione ed esercizio;
7. 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);
8. Qualificazione degli Operatori dedicati alle attività di manutenzione routinaria e periodica.
9. Calcolo del livello del SIL della funzione di comando dei sezionatori MAT dell'intero sistema galleria a partire dal selettore ChE del quadro UCS-QS includendo nella perimetrazione anche il sezionatore MAT.

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:

1. Raccomandazioni per l'eventuale adeguamento delle specifiche tecniche alle revisioni condotte dall'ente stesso;
2. Documentazione per la gestione delle verifiche periodiche dei sistemi di sicurezza e per le modalità di esecuzione;
3. Aggiornamento dei Safety Manuals per i sistemi di sicurezza e il supporto per l'aggiornamento del Manuale della Gestione delle Emergenze;
4. Assunzioni utilizzate per la determinazione del SIL (PFHdangerous);
5. Assessment Specifiche dei requisiti di Sicurezza funzionale;
6. Assessment logiche di sicurezza applicative;
7. Assessment documentazione di progetto (per le parti di revisione);
8. 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.

11. DOCUMENTAZIONE E PROVE

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

Tutta la documentazione dovrà essere in lingua italiana.