CIRCOLARE D.G. N. 159/89— D.C. V N. 5/89

Prot. 1663 (56) 71.10

OGGETTO: Impianti funicolari aerei e terrestri. Sistemi a logica statica programmabile (a microprocessori) per la gestione ed il controllo dei dispositivi di comando, regolazione e sicurezza. Requisiti generali di sicurezza.

In relazione allo sviluppo che vanno assumendo i sistemi in oggetto indicati, anche nel settore dei pubblici servizi di trasporto effettuati con impianti funicolari aerei e terrestri, un apposito comitato di studio costituito in seno alla Commissione per le funicolari a. e t. ha elaborato un testo concernente i requisiti generali di sicurezza per gli anzidetti sistemi sul quale, nell'adunanza del 3 maggio u.s., si è favorevolmente espressa la stessa Commissione che ne ha altresì ritenuto, quanto meno in via provvisoria ed in attesa di una più completa normazione della materia, di dover fare riferimento a tali requisiti generali in sede di esame e parere su progetti comprendenti i sistemi di cui trattasi.

Per opportuna informazione degli Uffici in indirizzo, nonché delle Associazioni di categoria interessate, si trasmette quindi nell'allegata Nota Tecnica il surrichiamato testo, unitamente ad un preambolo inteso ad inquadrare il problema in un contesto più generale e con riferimento, per confronto, alle soluzioni tecniche più tradizionali sinora adottate per i dispositivi di comando, regolazione e sicurezza degli impianti funiviari.

Avuto riguardo peraltro alla notevole rilevanza assunta, agli effetti della sicurezza, dai sistemi in argomento, ma tenuto altresì conto della loro complessità, sotto il profilo concettuale, nonché della loro rapidissima evoluzione tecnologica, strettamente legata come è noto a quella dei settori dell'informatica applicata all'automazione, si ritiene opportuno far presente che è allo studio la possibilità di sostituire, almeno parzialmente, la documentazione tecnica illustrativa dei ripetuti sistemi, con una certificazione di rispondenza ai requisiti generali di sicurezza di cui all'acclusa Nota Tecnica, rilasciata da istituti specializzati di livello preferibilmente universitario, unitamente ai quali potranno eventualmente essere definite da questo Ministero ulteriori specifiche tecniche, verifiche e prove di accettazione e modalità di certificazione.

IL DIRETTORE GENERALE

ALLEGATO ALLA CIRCOLARE
D.G. n. 159/89 DEL 27.10.1989

NOTA TECNICA

Requisiti generali di sicurezza per i sistemi a logica statica programmabile (a microprocessori) per la gestione ed il controllo dei dispositivi di comando, regolazione e sicurezza degli impianti funicolari aerei e terrestri.

Come è noto, in diversi settori industriali si sono sviluppati negli ultimi anni dispositivi di controllo delle funzioni assolte dalle apparecchiature elettriche ed elettromeccaniche, proprie di ciascuno di tali settori, utilizzanti sistemi a logica statica programmabile e costituiti da insiemi di componenti elettronici (microprocessori, unità di memoria, unità di ingresso e di uscita, ecc.).

Tali sistemi sono di norma destinati ad elaborare determinati segnali elettrici in entrata, generalmente sotto forma digitale, coordinandoli mediante idonei programmi, eventualmente modificabili, e fornendo conseguenti segnali di risposta in uscita.

I richiamati sistemi sono così in grado di svolgere funzioni logiche prima assolte da complessi ed estesi circuiti cablati, comprendenti insiemi di componenti elettromeccanici (relè e schede elettroniche, queste ultime capaci di utilizzare segnali prevalentemente analogici), atti a compiere operazioni logiche e fra loro stabilmente collegati con cavetti, connessioni, ecc.

Tale tecnologia si va ora estendendo anche al settore degli impianti funicolari aerei e terrestri in servizio pubblico per il trasporto di persone, a cominciare da quelli monofune con veicoli a collegamento temporaneo che, notoriamente, risultano di maggiore complessità per i numerosi e delicati controlli di sicurezza prescritti durante il normale esercizio, in relazione anche alle elevate portate orarie richieste dagli esercenti.

Sistemi di gestione e controllo del tipo innanzi accennato sono stati ammessi da qualche anno a questa parte, su conforme parere della Commissione per le funicolari a. e t., ma sempre in via provvisoria data anche la difficoltà di disporre di una specifica normativa in proposito, al passo con il rapido e costante evolversi delle soluzioni tecnologiche immesse sul mercato.

L'esperienza sostanzialmente favorevole acquisita sulle singole realizzazioni ha peraltro indotto la Commissione anzidetta a fare studiare, nell'ambito di un proprio apposito comitato, la possibilità di individuare i principi generali di sicurezza ai quali dovrebbero rispondere, allo stato attuale, i sistemi di cui trattasi nonché i loro sottosistemi e componenti, al fine di consentirne in ogni caso il corretto funzionamento.

In proposito, appare necessario rammentare, innanzitutto, che ai sensi dell'art. 26, I° comma, del Regolamento Generale per le funicolari aeree approvato con D.P.R. 18.10.1957, n. 1367, i circuiti elettrici di sicurezza degli impianti in argomento devono essere realizzati in maniera da provocare l'arresto della marcia non soltanto per comando manuale diretto, ovvero per intervento dei dispositivi automatici di sicurezza e controllo, ma altresì nell'eventualità di avaria agli stessi circuiti tale da comprometterne il funzionamento.

La richiamata norma sancisce quindi il primo fondamentale principio di sicurezza per i sistemi di cui trattasi, ossia quello cosiddetto della "sicurezza intrinseca" (“fail safe”), postulando che qualunque disfunzione del sistema stesso debba determinare automaticamente l'arresto della marcia.

Nell'eventualità che il sistema, o comunque, uno o più dei suoi sottosistemi, ovvero uno dei componenti, non possa essere di per sé a sicurezza intrinseca (per ragioni costruttive, funzionali od altro), si deduce dal surrichiamato principio l'esigenza di realizzare sistemi ridondanti e, quindi, costituiti da sottosistemi e componenti duplicati, in costante sorveglianza reciproca per denunciare tempestivamente eventuali discordanze nello stato di due unità aventi la stessa funzione (“controllo di parità”), collegati in maniera da attuare il principio della “sicurezza intrinseca” attraverso l'arresto automatico della marcia in presenza di disparità.

Il rigoroso rispetto del principio della sicurezza intrinseca, come del resto è necessario, può tuttavia comportare problemi per la regolarità del servizio nel senso che la complessità dei moderni impianti funiviari, con un elevato quantitativo di dispositivi da gestire e controllare, comporta il rischio di arresti intempestivi, con conseguenti disservizi non determinati peraltro da reali pericoli per la sicurezza del servizio stesso.

A tali inconvenienti si è posto parzialmente rimedio, nei più moderni impianti nei quali il criterio della duplicazione è esteso a tutta la catena cablata connessa a dispositivi di sicurezza (doppio canale di sicurezza), introducendo un controllo permanente della corretta operatività del sistema (integrità operativa) tramite test periodici di efficienza e congruenza di stato tanto per i dispositivi medesimi, quanto per i relè finali delle due anzidette catene.

La logica dei suddescritti sistemi impone inoltre la condizione che, dopo ogni arresto, la ripresa del servizio risulta possibile solo previo test di efficienza dei dispositivi di sicurezza

duplicati e dei relè finali delle rispettive catene e comunque, in caso di accertata disfunzione di uno di tali dispositivi o relè, escludendo (parzializzazione) il dispositivo od il relè interessato, ma consentendo la marcia a velocità convenientemente ridotta (penalizzazione leggera di velocità); ciò, anche per tenere conto della possibilità che un eventuale ulteriore guasto renda inoperante l'intervento automatico del sistema ed il conseguente nuovo arresto dell'impianto.

Nel caso invece di accertata disfunzione dei corrispondenti disponitivi su ambedue i canali, ovvero dei rispettivi relè finali, la ripresa della marcia può risultare ancora possibile, comunque a velocità ridottissima (penalizzazione pesante di velocità) e solamente per consentire di far rientrare nelle stazioni i viaggiatori presenti in linea (svuotamento dell'impianto); ciò, naturalmente, sotto la diretta responsabilità dell'agente caposervizio il quale provvede ad escludere con le apposite chiavi ambedue i canali di sicurezza, ponendo in atto altresì le ulteriori cautele eventualmente necessarie.

In un moderno sistema per la gestione ad il controllo delle funzioni svolte dalle diverse apparecchiature costituenti l'impianto risulta peraltro conveniente, per una corretta individuazione dei compiti assolti, distinguere i seguenti tre insiemi:

a) insieme degli enti periferici, convenientemente alimentati ed in grado di emettere segnali digitali od analogici, normalmente costituito:

   a.1) da sensori, ossia dispositivi che individuano stati funzionali segnalandone ogni modifica (interruttori di fine corsa, interruttori di prossimità, interruttori a consenso, ecc.).

   a.2) da unità funzionali, ossia da dispositivi per rilevazione del corretto svolgimento di funzioni controllate, ovvero dell'insorgere di disfunzioni od anomalie in tale svolgimento (controlli di corrente, di velocità, di spazio, trasduttori, ecc.);

b) insieme delle linee di alimentazione e trasmissione dei segnali emessi dai sensori e dalle unità funzionali, ossia l'insieme dei cavi e delle connessioni che consentono di trasferire i segnali stessi alle unità centrali;

c) insieme delle unità di gestione, controllo e coordinamento centrali, normalmente costituito:

   c.1) da unità di controllo, ossia insieme di dispositivi opportunamente predisposto e programmato per ricevere ed analizzare i segnali digitali ed analogici provenienti dall'insieme degli enti periferici; per giudicare il corretto e coordinato valore dei segnali medesimi; per emettere, conseguentemente, determinati segnali finalizzati a consentire l'avviamento dell'impianto, la prosecuzione della sua marcia, ovvero il suo arresto, normale o rapido; tali unità devono essere altresì in grado di effettuare verifiche periodiche, o se del caso continue, del corretto funzionamento di unità funzionali periferiche e/o dell'integrità dei loro componenti, nonché ulteriori controlli (autodiagnostica);

c.2) da unità di visualizzazione ed interazione, ossia dispositivi che consentano di presentare all'operatore, in forma chiara e di immediata comprensione, lo stato generale dell'impianto e delle sue diverse apparecchiature, l'esito delle diagnosi, nonché eventuali suggerimenti per interventi da porre in essere; all'uopo tale unità deve essere in grado di dialogare con l'operatore e di interagire eventualmente con talune apparecchiature.

Naturalmente, agli effetti del richiamato art. 26, 1° comma del Regolamento Generale, ciascun insieme deve operare in sicurezza intrinseca, di per sé o ricorrendo a sottoinsiemi ridondanti; infatti, come prima accennato, ciò nei più recenti sistemi a logica cablata viene in concreto realizzato mediante due canali di sicurezza in sorveglianza reciproca; tuttavia tali sistemi, come del resto anche quelli a logica statica, hanno spesso i loro punti deboli negli enti periferici e, in particolare, negli organi sensori che non sempre possono essere effettivamente realizzati a sicurezza intrinseca, mentre la loro duplicazione - teoricamente realizzabile - può trovare ostacoli nella eccessiva complicazione dei circuiti con inconvenienti per la regolarità dell'esercizio.

Tutto ciò premesso per una più generale visione del problema in esame, si illustrano qui di seguito le conclusioni alle quali, pur tenendo conto della relativamente limitata esperienza acquisita nelle applicazioni, è pervenuto il comitato innanzi richiamato e sulle quali si è favorevolmente espressa la Commissione per le funicolari a. e t. nell'adunanza del 3 maggio u.s., per quanto riguarda sia i requisiti generali di sicurezza ai quali devono rispondere i sistemi di gestione, controllo e coordinamento delle protezioni negli impianti funicolari aerei e terrestri in servizio pubblico, sia la documentazione tecnica che, allo stato, appare necessaria per consentire il giudizio su tali sistemi:

1. - Ogni sistema di controllo delle funzioni legate all'attività di un impianto funicolare a. o t. deve comprendere due sottosistemi indipendenti a logica statica programmabile (canali A e B), affiancati da un terzo sottosistema di tipo tradizionale a logica cablata (canale C).

2. — I tre sottosistemi suddetti devono far capo ad un dispositivo (sottoinsieme individuato con c.2 in premessa) destinato ad assolvere solo funzioni di segnalazione; tale sottoinsieme deve consentire tanto una efficace e significativa visualizzazione in tempo reale dello stato di funzionamento dell'impianto, quanto la completa supervisione di tale funzionamento mediante sia colloquio con l'operatore, agli effetti anche della diagnostica, sia effettuazione di verifiche e prove in simulazione (TEST).

3. — I due sottosistemi a logica statica programmabile devono ricevere ai loro ingressi (INPUT) informazione sul funzionamento dell'impianto trasmesse, sotto forma di segnali logici, dall'insieme degli enti periferici e, in particolare, dai comandi manovrati dai macchinisti; devono individuare in base a tali informazioni, lo stato di funzionamento dello impianto, confrontandolo con lo stato comandato dal medesimo

macchinista; devono giudicare se lo stato di funzionamento individuato è conforme a quello richiesto e, in particolare, se esso è congruente con le prestabilite esigenze di sicurezza; devono conseguentemente comandare l'esecuzione delle opportune manovre per mezzo dei relè finali di uscita (OUTPUT) agenti sui dispositivi di comando dell'impianto (consenso alla partenza, arresto normale, arresto rapido, ecc.); devono infine informare il macchinista attraverso il sottoinsieme di segnalazione, sullo stato di funzionamento dell'impianto e, quando necessario mediante colloquio con l'operatore, fornire indicazioni sui provvedimenti da adottare.

4. — Il sottosistema a logica cablata deve comunque ricevere informazioni vitali ai fini della sicurezza del servizio; informazioni che, generate, trasmesse e rivelate con modalità distinte da quelle adottate per alimentare le corrispondenti entrate dei sistemi a logica statica, devono allo stato essere individuate nei segnali provenienti dai dispositivi di protezione seguenti:

4.1. - per tutte le categorie e classi di impianti:

4.1.1. — ultimo dispositivo elettrico di controllo della velocità (centrifugo elettrico o dinamo tachimetrica);

4.1.2. — dispositivi per il controllo della coppia erogata dal motore di trazione (principale o riserva);

4.1.3. — circuito di sicurezza di linea: si intendono comprese tanto le protezioni installate sui sostegni di linea, quanto quelle dei veicoli (apertura porte, freni dei carrelli, ecc.) e quelle per contatti indebiti fra funi (accavallamento);

4.1.4. — comandi di arresto ed interruttori di consenso a comando manuale;

4.1.5. — consensi del dispositivo di tensione dell'anello trattivo (o portante-traente), agli effetti del controllo che permangano le necessarie condizioni di aderenza;

4.1.6. — continuità della categna cinematica dell'argano: in azionamento principale o di riserva, in azionamento di recupero e/o di soccorso;

4.2. — per gli impianti aerei e terrestri a va e vieni:

4.2.1. — dispositivi per il controllo della velocità nelle zone soggette a limitazioni (dazi continui e discontinui);

4.2.2. — dispositivi elettrici di fine corsa delle vetture nelle stazioni;

4.3. — per gli impianti a moto continuo con veicoli a collegamento temporaneo:

4.3.1. — dispositivi di controllo geometrico del corretto accoppiamento delle morse, rispettivamente sulle rampe di partenza e su quelle di arrivo dei veicoli;

4.3.2. — dispositivi di controllo dell'efficienza o della tenuta delle morse (provamolle e/o provamorse);

4.3.3. — dispositivi anticollisione (sezioni di blocco) sia sulle rampe di partenza che su quelle di arrivo;

4.3.4. — controlli del corretto assetto delle pulegge motrici e/o di rinvio (se previsti);

4.4. — per gli impianti a moto continuo con veicoli a collegamento permanente (comprese le sciovie):

4.4.1. — controlli del corretto assetto delle pulegge motrice e/o di rinvio (se previsti);

4.4.2. — controlli del mancato sbarco dei viaggiatori o del loro mancato svincolo dai traini (se previsti).

5. — Fatto salvo quanto precisato al successivo punto 6, il sottosistema a logica cablata riceve e coordina i segnali provenienti dai dispositivi di protezione indicati al precedente punto 4., trasmessi alla catena di relè elettromeccanici costituente il sottosistema stesso (canale C) da sorgenti (enti periferici) che, qualora operanti nella logica della sicurezza intrinseca, possono presentare parti in comune con quelle utilizzate dai due sottosistemi a logica statica, ma la trasmissione di tali segnali deve essere completamente indipendente. I segnali provenienti da dispositivi di protezione duplicati devono pervenire separatamente da ambedue i dispositivi stessi; inoltre, qualora taluni segnali debbano essere elaborati all'interno dei sottosistemi a logica statica, il sottosistema a logica cablata deve essere provvisto di dispositivi in grado di svolgere funzioni analoghe.

6. — Nel caso che taluni dei dispositivi di protezione indicati al precedente punto 4. siano costituiti da unità funzionali autocontrollate, ossia realizzate mediante sottoinsiemi e/o componenti fra loro coordinati in modo tale da segnalare qualunque disfunzione intervenga nella prefissata sequenza logica delle funzioni assolte, può essere omesso di inserire i predetti dispositivi nella catena costituente il canale C, a condizione però che ogni segnalata disfunzione determini autonomamente l'arresto dell'impianto e che la ripresa del servizio venga successivamente consentita esclusivamente con le modalità indicate al successivo punto 11.2. (penalizzazione di velocità).

7. — In linea di principio, gli insiemi o le unità funzionali destinati ai comandi del funzionamento dell'impianto devono essere distinti da quelli destinati ai controlli; può essere consentito l'impiego di componenti comuni alle due categorie di insiemi sempreché ne risulti penalizzata, eventualmente, la regolarità dell'esercizio ma non mai la sicurezza.

8. — I due sottosistemi a logica statica, realizzati mediante tecnologia adeguatamente sperimentata (programmazione a contatti, in logica booleana, a stati macchina), devono utilizzare un "programma di base" connesso con un "programma applicativo"; il primo programma, non modificabile, caratterizza le modalità di funzionamento del sottosistema; il secondo, variabile da impianto ad impianto, comprende le regole decisionali impiegate dal sottosistema per consentire l'avviamento o la prosecuzione della marcia in relazione allo stato dei segnali d'ingresso. I due sottosistemi devono inoltre rispondere ai seguenti requisiti:

8.1. — i due sottosistemi devono essere completamente indipendenti e realizzati con dispositivi totalmente distinti, alimentati da due separate linee elettriche a 24 V. c.c. provenienti da due distinte batterie di accumulatori, ciascuna provvista del proprio gruppo di ricarica in tampone;

8.2. — i due sottosistemi devono essere completamente separati dagli altri circuiti elettrici dell'impianto e galvanicamente isolati dal campo; a tal fine, sia gli ingressi che le uscite dei segnali devono essere realizzati mediante interfaccia galvanicamente isolate (fotoaccoppiatori, trasformatori, relè, ecc.);

8.3. — gli enti periferici (sensori ed unità funzionali), anche se duplicati devono inviare i propri segnali, in parallelo, ad ambedue i sottosistemi;

8.4. — i dati ed i programmi memorizzati su componenti teoricamente soggetti a perdita di tali dati o programmi (EPROM) a causa della propria tecnologia costruttiva, devono essere sottoposti a test periodici con appositi programmi secondo quanto indicato ai successivi punti 9.1. e 9.3.; in ogni caso i risultati del test devono essere confrontati con i parametri memorizzati e visualizzati;

8.5. — tutte le funzioni e tutte le operazioni di ciascun sottosistema devono essere verificate in autodiagnosi mediante apposito programma ciclico (“ciclo di lavoro”), da sviluppare in un tempo non superiore a 40 ms (tale valore è minore del tempo minimo di rilascio di un relè elettromeccanico, sicché la durata del ciclo di lavoro garantisce prestazioni di rapidità di intervento almeno pari a quelle realizzabili con un sottosistema tradizionale a catena di relè);

8.6. — ad ogni ciclo di lavoro il sottosistema deve verificare la presenza di tutti i segnali di ingresso, ricavando da essi lo stato di funzionamento dell'impianto, e emettere i conseguenti segnali di uscita (consenso o arresto);

8.7. — la corretta e tempestiva ripetizione di ogni ciclo di lavoro deve essere verificata mediante dispositivo esterno al microprocessore del sottosistema (Watch-dog), atto ad intervenire nel caso che la durata del ciclo superi il valore prefissato; in tale eventualità tale dispositivo deve provocare l'arresto dell'impianto indipendentemente dall'eventuale intervento del microprocessore;

8.8. — le uscite dei due sottosistemi devono essere costituite da relè finali di consenso del tutto distinti fra loro ed agenti mediante contatti normalmente aperti; detti relè devono essere del tipo "dinamico", devono cioè eccitarsi in presenza di un segnale operativo avente prefissate caratteristiche di ampiezza e frequenza e generato "a programma" dal rispettivo sottosistema; segnali con caratteristiche diverse devono invece determinare la diseccitazione dei relè in questione e quindi l’arresto;

8.9. — i contatti dei relè finali di consenso dei sottosistemi a logica statica, così come quelli dei relè finali di consenso del sottosistema cablato, devono essere posti in serie nelle catene che comandano i diversi organi dell'impianto, in maniera che la diseccitazione anche di uno solo di tali relè determini l'arresto dell'impianto (o ne inibisca l'avviamento);

8.10. — ciascuno dei due sistemi a logica statica deve ricevere informazioni sullo stato dei relè finali di consenso, sia dell'altro analogo sottosistema, sia di quello a logica cablata, utilizzando all'uopo contatti degli stessi relè finali; tali informazioni devono essere utilizzate da ciascun sistema a logica statica per verificare la coerenza con lo stato dei propri relè finali di consenso, reiterando se del caso la richiesta di arrestare lo impianto; per assicurare la completa indipendenza dei due sottosistemi a logica statica, non deve esistere alcuna altra possibilità di scambio di informazioni ed il loro funzionamento deve essere asincrono;

8.11. — i componenti elettronici impiegati nei sottosistemi a logica statica devono essere garantiti per assicurare il corretto funzionamento degli stessi sottosistemi entro un campo di temperatura compreso fra 0 e +40° C; entro un campo di umidità relativa compreso fra il 20 ed il 90% e per una tensione di alimentazione compresa fra il –10% ed il +15% del valore nominale; qualora le condizioni locali non consentano il rispetto dei suindicati limiti, il costruttore dovrà fornire idonee istruzioni per assicurare l'efficienza in servizio dei componenti anzidetti nonché per garantirne la conservazioni fuori servizio;

9. — Negli impianti che utilizzano sottosistemi di controllo a logica statica programmabile devono essere realizzate le seguenti procedure di TEST:

9.1. — Test periodico (o di attivazione): effettuato ogni volta che il sottosistema viene posto sotto tensione, per verificare la "vitalità" dei microprocessori, il loro corretto funzionamento e la validità dei dati e programmi memorizzati su EPROM (v. precedente punto 8.4.);

9.2. — Test di avviamento: effettuato prima di ogni avviamento dell'impianto, tanto dopo un arresto normale quanto dopo arresti per intervento di protezioni; deve essere in questa occasione verificata la capacità del sottosistema di riconoscere ogni situazione che richiede un arresto; in particolare:

9.2.1. — tutti gli ingressi logici di tipo ON/OFF provenienti dai sensori e dalle unità funzionali periferiche devono essere sottoposti a test, mediante annullamento fisico conseguito con l'apertura dei relativi circuiti: si deve verificare se il sottosistema è in grado di riconoscere in sequenza l'annullamento di tutti gli ingressi e, conseguentemente, tutte le richieste di arresto;

9.2.2 — se il sottosistema riceve ed elabora segnali di tipo analogico, tali segnali devono essere automaticamente generati dalla procedura di test per verificare se il sottosistema medesimo è in grado di riconoscerli e di intervenire quando essi escono dal campo di validità prefissato (ad es. segnali di corrente e/o di velocità);

9.2.3. — se il sottosistema riceve segnali logici di tipo ON/OFF provenienti da unità funzionali periferiche (ad es. prova molle degli impianti a collegamento temporaneo), che elaborano in proprio grandezze analogiche o sviluppo di funzioni di controllo, la procedura di test delle medesime unità funzionali, se prevista, deve generare segnali dello stesso tipo per una verifica simile a quella illustrata al punto precedente;

9.3. — Test continuo (a scansione ciclica ripetitiva), ad ogni ciclo di lavoro (v. punto 8.5) devono essere effettuate le seguenti verifiche:

9.3.1. — verifica della durata del tempo del ciclo (v. punto 8.7) ;

9.3.2. — verifica di congruenza dei risultati, confrontando gli stati delle uscite sia dei due sottosistemi a logica programmabile che del sottosistema a logica statica (v. punto 8.6.);

9.3.3. — verifica delle memorie di lavoro (RAM), per accertare la capacità di corretto aggiornamento ed elaborazione dei dati in esse immagazzinati;

9.3.4. — verifica dei segnali di tipo "dinamico", ossia che si ripetono in forma simile ad ogni evento (v. punto 9.2.3.), verificando che tali segnali siano compresi nel campo di validità per essi prefissato.

10. — Le proposte per l’impiego, negli impianti funicolari a. e t., di sistemi di controllo a logica statica programmabile devono essere accompagnate da adeguata documentazione, atta a consentire di riconoscerne le peculiarità e di esprimere quindi un giudizio di ammissibilità. In particolare:

10.1. — il progetto da sottoporre all’approvazione dell'Amministrazione deve comprendere:

10.1.1. — schema a blocchi del sistema, scomposto nei suoi sottosistemi centrali e nei rispettivi insiemi periferici; di questi ultimi devono essere evidenziati, e contrassegnati per riferimento, quelli che possiedono le funzioni interessanti la sicurezza, individuate come vitali al precedente punto 4;

10.1.2. — descrizione dell'architettura dei sottosistemi e dei principi seguiti per garantire la sicurezza con riferimento ai requisiti generali innanzi illustrati;

10.1.3. — descrizione dettagliata, nelle forma di schema funzionale, delle funzioni di impianto controllate dai sottosistemi centrali e dalle relative uscite di consenso utilizzate nei circuiti di comando e segnalazione della marcia o dell'arresto, evidenziandone le interconnessioni con lo schema funzionale generale;

10.1.4. — descrizione, in forma di diagrammi di flusso ovvero di, schemi funzionali a contatti o equivalenti, del significato, provenienza o destinazione di ciascun segnale d'ingresso e di uscita, così da

consentire l'agevole individuazione delle funzioni ed in maniera da poterne desumere le conseguenze legate alla presenza, alla variazione od all'assenza del segnale medesimo;

10.1.5. — relazione illustrante, in particolare per le eventuali grandezze analogiche controllate dai sottoinsiemi, le modalità ed i valori di taratura, nonché le relative soglie ritenute ammissibili dal progettista del sistema d'intesa con il professionista che assume le funzioni di coordinatore generale per la progettazione dell'impianto; tale relazione deve altresì indicare le modalità di segnalazione di eventuali alterazioni operative dei singoli sottoinsiemi, nonché i condizionamenti che tali alterazioni determinano sulla prosecuzione del servizio eventualmente degradato (v. punto 11);

10.1.6. — dichiarazione del progettista del sistema, attestante che sia i limiti di impiego garantiti per l'apparecchiatura ai fini del sicuro funzionamento, e di cui al punto 8.11; sia le caratteristiche dei componenti impiegati sono compatibili con le condizioni locali di installazione, con le eventuali speciali istruzioni del caso (v. punto 8.11).

10.2. — Oltre al progetto suddescritto deve altresì essere depositata presso l'Amministrazione la seguente documentazione concernente i dettagli costruttivi:

10.2.1. — dimostrazione che ciascuno dei sottosistemi e degli insiemi e sottoinsiemi opera in sicurezza intrinseca, nel senso cioè che qualsiasi guasto od evento perturbatore deve porre il sottosistema, l'insieme od il sottoinsieme, nonché il livello gerarchicamente superiore, in uno stato funzionale compatibile con la sicurezza; a tal fine per ciascun sottosistema, insieme e sottoinsieme devono essere individuati:

a) la funzione o la sottofunzione nella quale opera;

b) lo stato funzionale per il quale viene esplicita la sicurezza intrinseca;

c) l'albero dei guasti e degli eventi perturbatori che ne possono compromettere l'operatività;

d) la verifica che gli eventi di cui alla lettera c) determinano le condizioni di stato cui alla lettera b);

10.2.2. — informazioni tanto sull'hardware quanto sul software dei sottosistemi e, più precisamente:

a) per i sottosistemi che utilizzano prodotti di normale reperimento in commercio (PLC, PC, ecc.), dovranno essere fornite, in merito ai programmi di base, le informazioni desumibili dai manuali operativi di tali prodotti, dimostrandone in ogni caso la compatibilità;

b) per i sottosistemi che utilizzano, invece, unità direttamente assemblate dal costruttore che provvede anche ad elaborare il programma di base, dovranno essere forniti gli schemi di principio, i diagrammi di flusso e tutte le informazioni atte a consentire un giudizio su tale programma;

c) per il programma applicativo, variabile da impianto ad impianto, dovranno essere fornite precise indicazioni circa le regole decisionali adottate per l'elaborazione dei segnali di consenso in uscita, in relazione allo stato dei segnali di entrata, completando tali indicazioni con ogni informazione atta a consentire un completo giudizio sulla validità del programma;

d) descrizione dei programmi di autodiagnosi del sottosistema di controllo centrale, sia per i test periodici (“ di attivazione”, v. punti 8.4, e 9.1.), sia per i test “di avviamento”(v. punto 9.2.) sia infine per i test compresi nel “ciclo di lavoro” (v. punti 8.5. e 9.2.), con dimostrazione della capacità per detti programmi di rilevare efficacemente i guasti del sottosistema medesimo;

e) i programmi software devono comunque essere documentati, sia in relazione al linguaggio utilizzato per la scrittura delle istruzioni di programma, che in relazione alle strutture dei programmi, sia, infine, fornendo l’insieme delle istruzioni costituenti i vari programmi (di base, applicativi e diagnostici).

11. — Nell'eventualità di guasto o disfunzione di uno dei due sottosistemi a logica statica, ovvero di quello a logica cablata, tali da impedirne il corretto e completo funzionamento, il sistema di gestione e controllo deve consentire le seguenti modalità di prosecuzione dell'esercizio:

11.1. — nell'ipotesi di guasto, anche parziale, ad uno dei due sottosistemi a logica statica, il sistema deve opportunamente segnalare il guasto e la sua causa; l'esclusione del sottosistema in avaria, ossia del relativi relè finali ovvero, se realizzabile, di quella sua parte interessata dal guasto (parzializzazione), è consentita solo all'agente, caposervizio (mediante apposita chiave a lui in consegna), previa decisione dello stesso sulla possibilità di proseguire l’esercizio e sulle eventuali speciali cautele da adottare (ove possibile da indicare nel regolamento d'esercizio); la ripresa della marcia può essere comunque consentita ad una velocità non superiore ai 3/4 di quella massima autorizzata (penalizzazione leggera di velocità) e, in ogni caso, con presenziamento continuo del banco di manovra tale riduzione deve essere automaticamente imposta dal sistema e inoltre, negli impianti del tipo a va e vieni, detta ripresa deve essere attuata esclusivamente mediante comando manuale, con esclusione automatica dell'eventuale marcia a programma;

11.2. — nell’ipotesi che il guasto interessi ambedue i sottosistemi a logica statica, ovvero un sottosistema a logica statica e quello a logica cablata, ovvero infine solo quest'ultimo sottosistema, previo intervento dell'agente caposervizio (che anche in questo caso decide circa l'eventuale ripresa della marcia e circa le

eventuali speciali cautele da adottare), la prosecuzione del servizio può essere consentita esclusivamente per la ultimazione della corsa (negli impianti a va e vieni) o per lo svuotamento della linea (negli impianti a moto continuo), ma comunque a velocità non superiore a 1/3 di quella massima autorizzata (penalizzazione pesante) e, in ogni caso, con presenziamento continuo del banco di manovra; tale riduzione deve essere automaticamente imposta dal sistema e inoltre, negli impianti a va e vieni, la ripresa della marcia deve essere attuata esclusivamente mediante comando manuale, con esclusione automatica della marcia a programma.

IL DIRETTORE DELLA DIVISIONE

(Dr. Ing. Salvatore Perciabosco)

Roma, ottobre 1989