Sviluppo e varianti della tecnica dell'albero dei guasti nell'applicazione delle Norme CENELEC in analisi RAM di sistemi ed impianti attinenti diversi settori industriali.

Autori: ing. M. Buldrini[1], ing. L. Ceraulo[1], ing. P. Vestrucci[1,2], ing. G. Zappellini[1]

1: NIER Ingegneria s.r.l. via Altabella, 3 Bologna

2: DIENCA Facoltà di Ingegneria di Bologna

Sommario

La tecnica dell'albero dei guasti è forse fra le più utilizzate nell'ambito di analisi RAMS (Reliability, Availability, Maintainability and Safety) con una più lunga esperienza applicativa. Proprio per tali caratteristiche, si sono integrati nel tempo, varianti applicative introdotte da situazioni particolari o complesse realizzate nei sistemi di controllo e protezione. La memoria in oggetto riprende gli aggiornamenti di maggior utilizzo, applicando, per completezza, la metodologia CENELEC a valutazioni di disponibilità riferite sia a sistemi in fase di esercizio, sia a sistemi in fase di risposta su chiamata. L'analisi del primo tipo è condotta mediante esemplificazioni ricavate dall'applicazione delle Norme Cenelec a sistemi inerenti il trasporto ferroviario altamente automatizzato. L'analisi del secondo tipo è condotta mediante esemplificazioni riferite ai Sistemi Antincendio di tipo ormai classico, nelle diverse tipologie di richieste.

Entrambi gli studi sono accompagnati dalle valutazioni di manutenibilità: programmi di ispezioni, test, manutenzione preventiva nonché dagli interventi di manutenzione correttiva. Tali valutazioni sono messe in relazione con le caratteristiche di disponibilità, quali valutate nella parte precedentemente descritta. L'analisi è sviluppata, per ciascuna ipotesi, sia mediante valutazioni analitiche che attraverso l'uso di programmi di calcolo applicati sia allo sviluppo degli alberi di guasto che alla capacità di risposta delle sezioni e dei componenti il sistema antincendio, chiamati ad intervenire. Una parte finale della memoria riassume in forma tabellare i risultati relativi alle diverse casistiche analizzate e ne evidenzia le conclusioni di maggior interesse.

Premessa ed obbiettivi

Nel presente rapporto si intende proporre l'utilizzo della tecnica dell'albero dei guasti, insieme con metodi affini (master logic diagramme, ecc.) nell'ambito della più vasta analisi RAM (reliability, availability, maintenabilty) applicata a sistemi di controllo ed impianti industriali. In particolare si intende presentare e porpore, sia pure in termini molto sintetici, l'applicazione delle norme CENELEC, riferite al sistema ferroviario, per un più esteso utilizzo, stante la completezza di trattamento contenuto. L'obbiettivo sopra enunciato viene perseguito, almeno tentativamente, presentando in una prima parte una applicazione più propria delle CENELEC e cioè riferita ad un sistema di controllo automatico in ambito ferroviario. In una seconda parte viene applicata un'estrapolazione ad un'analisi del tutto diversa e riferita alla valutazione di una sistema idrico antincendio, per il quale, tra l'altro, viene sviluppato un confronto della disponibilità rispetto a due diverse soluzioni impostate con diverso grado di affidabilità.

PARTE PRIMA

1. Descrizione del sistema

1.1 Architettura generale e funzioni dell'ASCV

L'apparato ASCV è un complesso di apparecchiature appositamente progettate per il governo e il controllo di piazzali ferroviari. Gestisce in sicurezza gli enti della "stazione", cioè invia ai dispositivi presenti sul piazzale e sulla linea comandi tali da non creare situazioni di esercizio che possano essere pericolose per gli impianti stessi, gli utenti o il pubblico che fruisce del servizio, anche in presenza di anormalità sugli impianti comandati o di guasti al suo interno.

L'architettura del ASCV è quella della macchina elettronica monocalcolatore che elabora in sicurezza i comandi verso gli enti di piazzale e le informazioni da essi provenienti. Sostituisce pienamente gli impianti a relè, mantenendo la stessa logica di sicurezza e fornendo nel contempo nuove funzionalità; sostituisce, infatti, le tradizionali reti logiche realizzate mediante tecnologia elettromeccanica, con un sistema elettronico di tipo fail-safe in grado di elaborare, in modo sicuro, le medesime reti logiche espresse sotto forma di equazioni booleane.

L'apparato ASCV svolge le seguenti funzioni:

- Acquisizione dello stato degli enti d'ingresso vitali e non vitali[1] siano essi direttamente controllati attraverso interfacce fail-safe oppure acquisiti attraverso una comunicazione.
- Determinazione dello stato richiesto sugli enti d'uscita direttamente controllati oppure dello stato richiesto da enti sotto il controllo di attuatori in funzione dello stato corrente degli enti d'ingresso.
- Comando dello stato richiesto sugli enti d'uscita vitali direttamente controllati e controllo di consistenza tra volontà di comando e stato diagnosticato per ciascun ente d'uscita vitale. Gli enti d'uscita non vitali non vengono controllati.
- Comando dello stato richiesto per ciascun ente remoto comunicando la volontà calcolata alla Unità Periferica di gestione degli enti di piazzale.
- Acquisizione dei comandi da parte degli operatori sia localmente che da posto centrale
- Visualizzazione dello stato degli enti periferici

L'apparato è dotato di un Sistema di Diagnostica e Manutenzione (SDM) che ha il compito di raccogliere ed elaborare le informazioni di stato e di diagnostica delle apparecchiature, allo scopo di fornire una diagnosi completa sui guasti rilevati e di supportare la funzione di manutenzione riducendo i tempi di riparazione

L'apparato ASCV prevede la completa ridondanza delle funzioni di input/output, delle funzioni di elaborazione e di quelle di comando degli enti periferici. Le uniche funzioni non ridondate sono quelle di interfaccia operatore locale.

1.2 Struttura fisica dell'ASCV

L'ASCV è fisicamente così costituito:

- SLE (Sottosistema Logico di Elaborazione)
- SSW (Sottosistema di Switch)
- MMI (Man Machine Interface)
- PA (Pannello di Alimentazione)
- SD (Sottosistema di Diagnostica)

L'SLE costituisce la parte del sottosistema deputata all'acquisizione ed elaborazione dati e alla gestione degli output. Tale gruppo è scomponibile come segue:

[1] Con il termine "vitale" si intende qui una funzione o una apparecchiatura realizzata in sicurezza.

- ULE (Unità Logica di Elaborazione)
- UVIO (Unità Input/Output Vitali)
- Cestello ventilazione

L'SSW è composto dall'hardware dedicato alla generazione della potenza vitale per l'alimentazione dei carichi in uscita, alla verifica della non contemporanea presenza di alimentazione dei carichi da parte dei due equipaggiamenti ridondati ed alla gestione della commutazione tra un SLE e l'altro.

Il Pannello di Alimentazione (PA) contiene i trasformatori con relativi interruttori di protezione per la generazione delle tensione necessarie al funzionamento di tutto l'apparato.

L'MMI costituisce il gruppo deputato alla gestione dell'interfaccia uomo - macchina oltre ad alcune funzioni accessorie.

Il Sottosistema di Diagnostica (SD) è scomponibile come segue:

- IDE
- SDM

L'Interfaccia Diagnostica Elementare (IDE) contiene i dispositivi di diagnostica/interfaccia tra gli SLE e l'MMI.

Il Sistema di Diagnostica e Manutenzione (SDM) centralizza le informazioni di diagnostica generate dai vari sottosistemi e le rende disponibili all'operatore in forma alfanumerica e grafica.

1.3 Struttura gerarchica

Nella tabella seguente viene rappresentata la struttura gerarchica dell'ASCV (livello 0) in cui sono presenti i seguenti Sottosistemi (livello 1), Unità (livello 2), Moduli (livello 3) e Schede (livello 4).

LIVELLO				SIMBOLO	DESCRIZIONE	Q.TÀ
Sottosistema				SLE	Sottosistema Logica di Elaborazione	2
	Unità			ULE	Unità Logica Elaborazione	1
		Modulo		MAIN	Acquisizione ingressi vitali ed elaborazione vitale	1
			Scheda	EIONT MAIN	Interfaccia tra ULE e modulo ingressi vitali	1
			Scheda	ECPU2 MAIN	Gestione ingressi ed elaborazione vitali	1
		Modulo		RCHK	Attuazione uscite vitali e elaborazione di controllo	1
			Scheda	EIOINT RECHECK	Interfaccia tra ULE e modulo uscite vitali	1
			Scheda	ECPU2 RECHECK	Attuazione comandi, gestione rilettura di uscite vitali ed elaborazione di controllo	1
		Modulo		VCOM	Gestione comunicazioni con rete FSFB	1
			Scheda	EHICOM FSFB	Interfaccia di comunicazione verso rete FSFB	1
			Scheda	EHICOM N/R	Interfaccia di comunicazione verso altra ULE	1
		Modulo		NVIO	Gestione ingressi e uscite non vitali e comunicazioni a bassa velocità	1
			Scheda	ELICOM	Interfaccia di comunicazione verso le unità logiche dei posti periferici fissi adiacenti	1
			Scheda	ECPU1	Gestione funzioni non vitali/diagnostica	1
			Scheda	E32INP	Ingressi non vitali	2
			Scheda	E32OUT	Uscite non vitali	1
		Modulo		EVPD	Vital Power Driver, pilotaggio energia vitale	1
			Scheda	EVPD		1
		Modulo		PSLO	Modulo di alimentazione SLE	1
			Scheda	ALIM. SLE	Alimentatore SLE	1
		Modulo		MOTHER BOARD ULE		1
			Scheda	MOTHER	Scheda madre per l'ULE	

LIVELLO				SIMBOLO	DESCRIZIONE	Q.TÀ
				BOARD ULE		
	Unità			UVIO	Unità Ingressi e Uscite Vitali	1
		Modulo		VINP	Modulo Ingressi Vitali	1
			Scheda	EIOBUF INPUT	Interfaccia tra ingressi e modulo MAIN	1
			Scheda	EVIN16	Ingressi vitali	Var.
		Modulo		VOUT	Modulo Uscite Vitali	1
			Scheda	EOVCM	Connessione AOVD	1
			Scheda	EIOBUF OUTPUT	Interfaccia tra uscite e modulo RCHK	1
			Scheda	EDBO16	Uscite vitali	Var.
		Modulo		MOTHER BOARD UVIO		1
			Scheda	MOTHER BOARD UVIO	Scheda madre per l'UVIO	1
Sottosistema				SSW	Sottosistema Swicth	1
	Unità			UCS	Interfaccia MUX, Commutazione	1
		Modulo		LSW	Modulo commutazione linee	1
			Scheda	ELH	Commutatore linee di comunicazione	2
		Modulo		MRD	Modulo modem Ripetitori Diramatori	1
			Scheda	MRD	Modem Ripetitori Diramatori	2
		Modulo		SUP_AL5	Modulo di alimentazione dell'unità interfaccia MUX, Commutazione	1
			Scheda	SUP_AL5	Alimentatore unità interfaccia MUX, Commutazione	1
	Unità			UVPS	Unità Modulo di Arbitraggio	1
		Modulo		VP N/R	Generatore di energia vitale e lettura stato uscite VP Normale o Riserva	1
			Scheda	VP	Generatore di energia vitale	Var.
			Scheda	AOVD	Lettura stato uscite VP	Var.
			Scheda	ALIM. VP12	Alimentatore VP	2
		Modulo		AFM	Modulo commutazione tra sottosistema normale e sottosistema di riserva	1
			Scheda	AFM	Commutazione tra sottosistema normale e sottosistema di riserva	1
		Modulo		MOTHER BOARD UVPS		1
			Scheda	MOTHER BOARD UVPS	Scheda madre per l'UVPS	1
Sottosistema				MMI	Interfaccia operatore	1
		Modulo		ACM	Governo video e pulsantiera	1
			Scheda	CPU-5D	Gestione ed elaborazione dati	1
			Scheda	SGC	Controllo in sicurezza delle elaborazioni MMI	1
			Scheda	VPC	Controllo in sicurezza della visualizzazione	1
		Modulo		PSMMI	Modulo alimentazione MMI	1
			Scheda	ALIM. MMI	Alimentatore MMI	1
		Modulo		PLS	Pulsantiera	1
			Scheda	SEKBGP	Decodifica tasti premuti e comunicazione con ACM	1
			Scheda	MT108	Pulsanti e gestione pulsanti	1
			Scheda	LCD	Display di servizio	1
		Modulo		MOTHER BOARD MMI		1
			Scheda	MOTHER BOARD MMI	Scheda madre MMI	1
		Modulo		FS_CRT	Monitor per visualizzazione sinottica e eco pulsantiera	1
Sottosistema				SD	Sottosistema di Diagnostica	1
	Unità			IDE	Interfaccia di Diagnostica Elementare	1
		Modulo		IDE		1

LIVELLO				SIMBOLO	DESCRIZIONE	Q.TÀ
	Unità			SDM	Sistema di Diagnostica e Manutenzione	1
		Modulo		SDM		1

La numerosità di alcuni gruppi funzionali di livello 4 (scheda) non è stata specificata poiché il sottosistema ASCV è di tipo modulare e quindi la sua configurazione dipende dal contesto in cui sarà inserito.

2. Profilo di missione

2.1 Condizioni ambientali

L'ASCV costituisce un'apparecchiatura di cabina facente parte, insieme ad altre apparecchiature di terra, del sistema di segnalamento e automazione.

Le apparecchiature di cabina sono caratterizzate dal fatto di essere concentrate ed installate all'interno dei cosiddetti edifici tecnologici dotati di sistema di controllo delle condizioni ambientali.

Le condizioni ambientali cui sono soggette tali apparecchiature sono quelle ottimali in cui si hanno valori di temperatura ed umidità controllati ed assenza di sollecitazioni meccaniche (vibrazioni ed urti). Queste condizioni sono quelle designate con il termine "Ground Benign" in MIL-HBK 217F Notice 2 e sono caratterizzate da "immobilità, controllo di umidità e temperatura ed immediata accessibilità per operazioni di manutenzione".

Per quanto riguarda queste condizioni ambientali si utilizzerà una temperatura di riferimento di 35 °C. Tale valore è ottenuto considerando una temperatura ambiente di 20 °C (costante essendo l'ambiente condizionato) ed un salto medio di temperatura fra ambiente e l'interno dell'armadio pari a 15 °C; l'apparato di stazione oggetto del presente rapporto attiene interamente a questa tipologia.

2.2 Profilo di missione

La missione associata al sottosistema prevede che almeno un SLE sia in grado di svolgere tutte le elaborazioni logiche correttamente, di comandare lo stato delle uscite vitali e di abilitare la scheda VP a generare la tensione vitale destinata ad alimentare gli output vitali.

È inoltre necessario che la funzione di selezione e controllo svolta dall'unità Modulo Arbitraggio (UVPS) sia disponibile. Per quanto riguarda questa unità, al fine di garantire la continuità del servizio, è infatti necessario distinguere, dal punto di vista concettuale, due differenti modi di guasto. La suddivisione discende direttamente dalla funzione di tipo switch svolta da tale unità.

Il primo modo di guasto è relativo alla funzionalità di selezione di uno dei due SLE (normale o riserva) in condizioni "statiche", quando cioè non è richiesta la commutazione da un sottosistema elementare all'altro. Se per un qualsiasi motivo il Modulo di Arbitraggio subisce un guasto che comporti la indeterminazione della scelta del sottosistema di elaborazione (né normale né riserva), **l'ASCV è posto fuori servizio (shut down)**.

Il secondo modo di guasto del Modulo di Arbitraggio è legato alla funzione di commutazione da un SLE all'altro. Tipico modo di guasto dei "commutatori", in senso lato, è quello di "bloccato in una posizione" in caso di richiesta di commutazione.

Questo modo di guasto non pregiudica da solo il funzionamento dell'ASCV poiché la selezione di uno dei due equipaggiamenti è garantita in ogni caso. Nel caso però di richiesta di commutazione, da un SLE all'altro, il dispositivo di commutazione rimane bloccato sul sottosistema elementare selezionato al momento della richiesta. Questo modo di guasto del modulo di arbitraggio comporta quindi il fuori servizio dell'apparato di stazione solo nel momento in cui **si verifica un guasto al Sottosistema Logico di Elaborazione (SLE) attivo** con conseguente impossibilità da parte dell'ASCV di attivare l'SLE di riserva.

3. Affidabilità

3.1 Affidabilità di base

L'affidabilità di base è stata calcolata prendendo in considerazione tutti i componenti (schede) collegati in serie. Due o più elementi sono collegati in serie se per il funzionamento corretto del sistema è necessario che tutti gli elementi che lo costituiscono funzionino correttamente.

Quindi l'affidabilità di base avrà la forma:

$$R_s = \prod_{i=1}^{n} R_i = R_1 \cdot R_2 \cdot ..... \cdot R_n$$

dove

R_S = affidabilità di base del sistema,

R_i = affidabilità del singolo componente,

n = numero di elementi che costituiscono il sistema.

Poiché l'affidabilità di ogni elemento può essere espressa in funzione del rateo di guasto secondo l'equazione:

$$R(t) = e^{-\frac{t}{MTBF}} = e^{-\lambda t}$$

dove

MTBF= tempo medio fra i guasti del singolo componente

λ = rateo di guasto del singolo componente

se ne deduce che l'affidabilità di base del sistema, in termini di "failure rate", è data dalla sommatoria dei ratei di guasto dei componenti.

Per il calcolo dell'affidabilità di base si è seguito il metodo della "Stress Analisys" indicata in MIL HNBK 217F Notice 2 utilizzando i parametri relativi alle condizioni "Ground Benign" con componenti di tipo commerciale. Come temperatura ambiente è stato utilizzato il valore di 35°C.

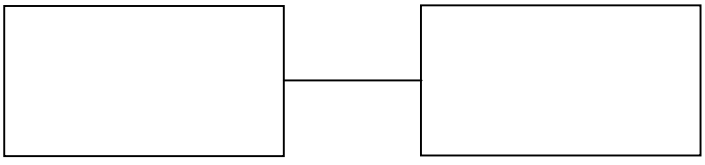
I sottosistemi elementari per i quali sono stati calcolati i valori di tasso di guasto sono i seguenti:

- Sottosistema Logica di Elaborazione (SLE)
- Sottosistema Switch (SSW)
- Sottosistema Man Machine Interface (MMI)
- Sottosistema di Diagnostica (SD)

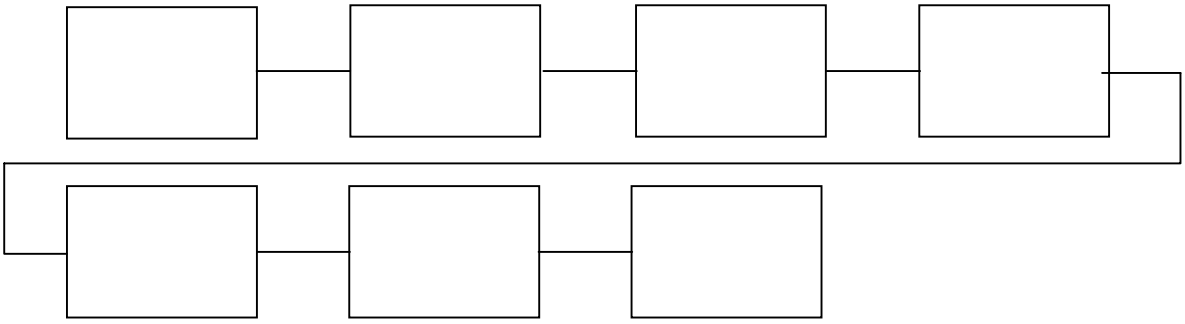
In base alla descrizione dell'ASCV, data nei paragrafi precedenti, il diagramma di affidabilità di base è rappresentato nel diagramma seguente:

ASCV:

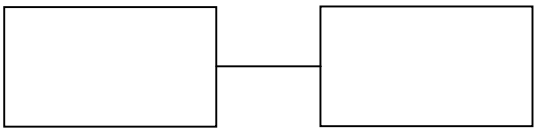
SLE:



ULE:



MAIN:



A titolo esemplificativo, in questa sede, vengono riportati, unitamente al diagramma dell'ASCV, solo i diagrammi relativi all'affidabilità di base di un sottosistema elementare, una unità ed un modulo. Nella tabella seguente sono riassunti i risultati ottenuti.

Sottosistema	**MTBF(h)**	**λ 10^{-6} (h^{-1})**	**Quantità**	**λ Tot 10^{-6} (h^{-1})**
SLE	2616.02	382,26	2	764.52
SSW	7568.3	132,13	1	132.13
MMI	4798.93	208,38	1	208.38
SD	9900.99	101	1	101
TOTALE	**829.17**	**_**	**_**	**1206.03**

3.2 Affidabilità di missione

Per lo studio dell'affidabilità di missione si è considerato, come top event dell'albero dei guasti lo shut down dell'ASCV inteso come perdita totale delle funzionalità del sottosistema o comunque come impossibilità di comandare l'accensione delle uscite vitali (funzionamento fortemente degradato).

L'ASCV è provvisto di completa ridondanza delle funzioni legate alle SLE. La ridondanza è di tipo stand by con il sottosistema di riserva che è però sempre caldo ed allineato con quello normale, allo scopo di garantire la disponibilità dell'apparato anche in caso di guasto su un SLE.

Allo scopo di rilevare i guasti latenti del SLE di riserva, sono previsti dei test di commutazione periodici con frequenza giornaliera (24 h).

Nella presente analisi si è tenuto conto sia dell'esecuzione periodica dei test necessari per l'individuazione dei guasti latenti sia del tempo di riparazione del singolo SLE reso indisponibile dal verificarsi del primo guasto (stimato in 72 h).

Si noti, come sarà chiarito nel seguito, che per i sottosistemi in esame sono distinguibili **due MTTR**: uno (MTTR1) assunto pari ad 72 ore è il tempo di riparazione del primo guasto (che porta all'entrata in servizio di SLE in stand by e di fatto non ha effetti sulla circolazione ferroviaria), l'altro (MTTR2), è di gran lunga inferiore in quanto è riferito al guasto che porta allo shut down dell'ASCV.

I livelli superiori dell'albero evidenziano gli effetti di guasto osservabili a livello di sottosistemi elementari ed originati dalle singole modalità di guasto delle schede.

Come già indicato il top event è rappresentato dallo shut down dell'ASCV al quale si può giungere attraverso:

- indisponibilità di entrambi i sottosistemi SLE in servizio ed SLE in stand by
- guasto dell'SLE in servizio e mancata commutazione, a causa di un guasto sull'UVPS, che impedisce all'SLE in stand by di entrare in servizio
- malfunzionamento UVPS che porta entrambi i VP ad erogare contemporaneamente potenza al carico senza che la scheda AFM sia in grado di intervenire
- guasto all'UCS, che non consente all'ASCV di comunicare con la rete FSFB, e quindi, non disponendo di informazioni vitali, di comandare l'accensione delle uscite vitali (funzionamento fortemente degradato

Nella costruzione dell'albero dei guasti, si è partiti dalle modalità di guasto, suddivise per blocchi funzionali, così come individuate nell'analisi FMECA, considerando solo le modalità di guasto che singolarmente, o in combinazione con altre, portano all'indisponibilità dell'SLE in cui si verificano.

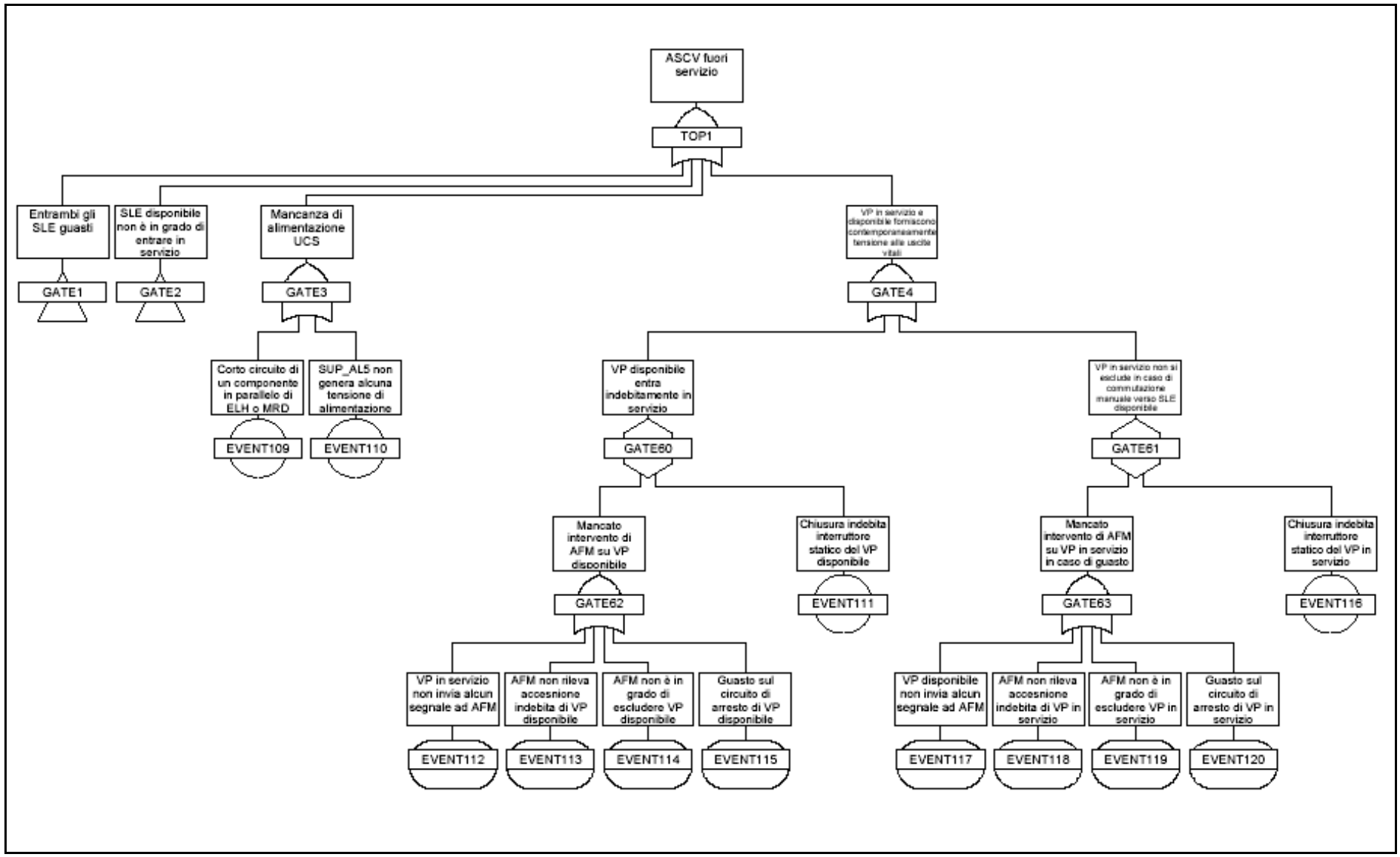
Per quanto riguarda l'analisi quantitativa del fault tree, necessaria per il calcolo della probabilità di accadimento del top event, si sono fatte le seguenti assunzioni:

- guasto su SLE in servizio: guasto rilevabile e rateo di guasto costante;
- guasto su SLE in stand by: guasto rilevabile e rateo di guasto costante;
- guasto su SLE in servizio durante il tempo di riparazione del altro SLE: guasto rilevabile, rateo di guasto costante, MTTR1;
- Mancata commutazione: guasto latente rilevabile su test (t=24 h) e rateo di guasto costante;
- Mancanza di alimentazione UCS: guasto rilevabile e rateo di guasto costante;

Per quanto concerne gli eventi sottesi al gate "VP in servizio e disponibile forniscono contemporaneamente tensione alle uscite vitali", si fa notare come entrambi le situazioni che la possono generare, derivano dal verificarsi di due eventi: un guasto latente (mancato intervento di AFM su VP) non rilevabile nemmeno su test ed un guasto (chiusura indebita interruttore statico VP) rilevabile. Perché, quindi, si arrivi al top event, è necessario che in un primo tempo si verifichi il guasto su AFM (latente) e che in seguito avvenga il guasto su VP. La situazione è ben descritta utilizzando un gate di tipo inhibit dove l'evento relativo all'AFM è l'evento condizionante. Si noti come la failure frequency relativa a questo ramo dell'albero è fortemente dipendente dal tempo di vita del sistema adottato.

Allo scopo di tenere conto, almeno in modo generale, delle possibili cause comuni di guasto, si è utilizzato, conservativamente, il "beta factor model" con beta pari a 0.02 ed un rateo di guasto pari al rateo di guasto dell'SLE in sevizio.

Nella figura seguente viene riportato la parte superiore dell'albero dei guasti realizzato.


ASCV fuori servizio
TOP1
Entrambi gli SLE guasti
SLE disponibile non è in grado di entrare in servizio
Mancanza di alimentazione UCS
VP in servizio e disponibile formacono contemporaneamente tensione alle uscite vitali
GATE1
GATE2
GATE3
GATE4
Corto circuito di un componente in parallelo di ELH o MRD
SUP_AL5 non genera alcuna tensione di alimentazione
VP disponibile entra indebitamente in servizio
VP in servizio non si esclude in caso di commutazione manuale verso SLE disponibile
EVENT109
EVENT110
GATE60
GATE61
Mancato intervento di AFM su VP disponibile
Chiusura indebita interruttore statico del VP disponibile
Mancato intervento di AFM su VP in servizio in caso di guasto
Chiusura indebita interruttore statico del VP in servizio
GATE62
EVENT111
GATE63
EVENT116
VP in servizio non invia alcun segnale ad AFM
AFM non rileva accesnione indebita di VP disponibile
AFM non è in grado di escludere VP disponibile
Guasto sul circuito di arresto di VP disponibile
VP disponibile non invia alcun segnale ad AFM
AFM non rileva accesnione indebita di VP in servizio
AFM non è in grado di escludere VP in servizio
Guasto sul circuito di arresto di VP in servizio
EVENT112
EVENT113
EVENT114
EVENT115
EVENT117
EVENT118
EVENT119
EVENT120

4. Manutenibilità

Il parametro considerato più significativo per descrivere lo stato di manutenibilità del sistema è il Mean Time To Repair (tempo medio alla riparazione) che in seguito indicheremo con MTTR.

Questo parametro indica la sola parte attiva del tempo di riparazione, non vengono quindi considerati i ritardi logistici.

La definizione formale del MTTR è la seguente:

$$MTTR = \frac{\sum_i Et_i \cdot \lambda_i}{\sum_i \lambda_i}$$

dove:

Et = Elapsed Time: è il tempo necessario all'effettuazione dell'azione manutentiva supponendo che gli elementi di supporto (strumentazione, ecc.) siano tutti disponibili;

λ = rateo di guasto.

I tempi costituenti l'Elapsed Time derivano dalle seguenti azioni manutentive elementari:

1. Diagnosi
2. Accesso
3. Rimozione del dispositivo che necessita manutenzione
4. Installazione del nuovo componente
5. Richiusura
6. Test.

Tutte queste operazioni verranno analizzate di seguito per le varie unità presenti.

4.1 Manutenzione preventiva

La manutenzione preventiva prevista per il sottosistema ASCV è costituita essenzialmente da: sostituzione periodica dei filtri, ispezione periodica ed eventuale sostituzione delle ventole, sostituzione periodica del monitor (Fs_CRT).

Il monitor è l'unico equipaggiamento elettronico soggetto a fenomeni di invecchiamento ed usura.

4.2 Manutenzione correttiva

Per quanto riguarda questo argomento faremo riferimento alle Line Replaceable Units (LRU) che sono rappresentate, per il sottosistema ASCV dalle singole schede. Unica eccezione è il modulo FS_CRT che, essendo costituito unicamente da un monitor di tipo commerciale, è da considerarsi nel suo insieme una singola LRU.

Primo scopo dell'analisi di manutenibilità, sarà quello dell'identificazione dei dati di input per l'analisi. Tali dati sono rappresentati dalle liste delle LRU definite per ogni sottosistema.

In base a queste considerazioni andiamo ad analizzare i contributi temporali delle varie voci che intervengono nel calcolo dell'Elapsed time, parametro utilizzato per determinare il MTTR e quindi la disponibilità dell'impianto.

Di seguito sono riportate a titolo esemplificativo alcune tabelle con indicati i tempi di intervento stimati per le LRU.

Si noti che i tempi di accesso sono tutti pari a 2 minuti in quanto il tempo impiegato per l'apertura dell'armadio e l'accesso alle singole LRU è lo stesso per tutte. Analoga considerazione va fatta anche per le altre fasi ovvero: rimozione, installazione, richiusura e test.

ULE

Modulo	Scheda	Quantità	Diagnosi (min)	Accesso (min)	Rimozione (min)	Installazione (min)	Richiusura (min)	Test (min)	Totale (min)	Elapsed time (h)	Tasso totale di guasto del sistema	MTTR (h)
MAIN	EIOINT MAIN	1	20	2	5	5	2	5	39	0,65	8,010E-06	
	ECPU2 MAIN	1	20	2	5	5	2	5	39	0,65	1,072E-05	
RCHK	EIOINT RCHK	1	40	2	5	5	2	5	59	0,98	8,010E-06	
	ECPU2 RCHK	1	40	2	5	5	2	5	59	0,98	1,072E-05	
VCOM	EHICOM FSFB	1	20	2	5	5	2	5	39	0,65	1,189E-05	
	EHICOM N/R	1	20	2	5	5	2	5	39	0,65	1,189E-05	
NVIO	ELICOM	1	10	2	5	5	2	5	29	0,48	1,172E-05	
	ECPU1	1	30	2	5	5	2	5	49	0,82	1,316E-05	
	E32INP	2	10	2	5	5	2	5	29	0,48	2,848E-05	
	E32OUT	1	10	2	5	5	2	5	29	0,48	2,980E-05	
EVPD	EVPD	1	20	2	5	5	2	5	39	0,65	1,146E-05	
PSLO	ALIM. SLE	1	50	2	180	180	2	5	419	6,98	1,870E-06	
MOTHER BOARD ULE	MOTHER BOARD ULE	1	5	2	5	5	2	5	24	0,40	1,667E-05	
											2,029E-04	**0,65**

Calcolo del MTTR per l'unità ULE

ASCV

Sottosistema elementare	Unità	Quantità	Elapsed time (h)	Tasso totale di guasto	MTTR (h)
SLE N	ULE	1	0,65	2,029E-04	
	UVIO	1	0,54	1,794E-04	
SLE R	ULE	1	0,65	2,029E-04	
	UVIO	1	0,54	1,794E-04	
SSW	UVPS	1	0,63	3,631E-05	
	UCS	1	0,47	9,582E-05	
MMI	MMI	1	0,56	2,084E-04	
SD	SDM	1	0,67	1,000E-04	
	IDE	1	0,58	1,000E-06	
				1,206E-03	**0,59**

Calcolo del MTTR per il sottosistema ASCV

Il risultato ottenuto mostra che il tempo medio di riparazione (MTTR) a fronte di un guasto qualsiasi è pari a circa 0,59 h.

5. Disponibilità

Il calcolo della disponibilità asintotica (A) del sottosistema è stata effettuata considerando l'MTBF relativo all'affidabilità di missione.

Il calcolo è condotto mediante la seguente formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$

dove:

- MTBF (Mean Time Between Failure) è il tempo medio fra guasti (= λp-1); il valore assunto in questa sede è riferito all'affidabilità di missione del sottosistema
- MTTR (Mean Time To Repair) è il tempo medio di riparazione dei suddetti guasti

Nel caso in cui si utilizzi il MTTR che comprende il solo tempo attivo di manutenzione, si ottiene la disponibilità intrinseca del sottosistema che tiene conto solo delle caratteristiche di affidabilità (MTBF) e manutenibilità (MTTR) del sistema.

Se, invece, si includono nel MTTR anche i ritardi logistici si ottiene la disponibilità operativa del sottosistema che tiene conto anche dell'organizzazione delle risorse e dei mezzi necessari alla manutenzione dell'impianto.

Considerando l'affidabilità di missione, la disponibilità asintotica riferita all'MTTR, che comprende il solo tempo attivo di manutenzione del sottosistema ASCV, è pari a:

$$A = 0,99994$$

Nella tabella seguente sono riportati i valori di disponibilità calcolati assumendo valori di MTTR compresi tra il valore minimo calcolato per il sistema (MTTR attivo) ed un valore massimo di 10 h. Oltre alla disponibilità espressa come numero puro (percentuale), l'indisponibilità (U) espressa in minuti annui di fuori servizio ottenuta moltiplicando per i minuti di un anno il complemento ad 1 della disponibilità.

MTBF (h)	MTTR (h)	A	U (MIN/ANNO)
10000	0,59	0,99994	31
10000	1	0,99990	53
10000	2	0,99980	105
10000	3	0,99970	158
10000	4	0,99960	210
10000	5	0,99950	263
10000	6	0,99940	315
10000	7	0,99930	368
10000	8	0,99920	420
10000	9	0,99910	473
10000	10	0,99900	525

6. Conclusioni

6.1 Affidabilità di Base

Il tasso di guasto relativo al verificarsi di un qualsiasi guasto nell'ASCV (Affidabilità di base), è pari a 1,206 x 10-3 h-1, si ha cioè un tempo medio tra guasti del sottosistema pari a circa 8,29 x 102 h.

6.2 Affidabilità di Missione

Il tasso di guasto relativo al fallimento della missione individuata per l'ASCV (Affidabilità di missione), è pari a 9.99 x 10-5 h-1, si ha cioè un tempo medio tra guasti che comportano lo shut down del sottosistema pari a circa 1 x 104 h.

6.3 Manutenibilità

Il tempo medio di riparazione (MTTR) a fronte di un guasto qualsiasi per il sottosistema in esame è pari a circa 0,59 h.

6.4 Disponibilità

Considerando l'affidabilità di missione, la disponibilità asintotica riferita all'MTTR, che comprende il solo tempo attivo di manutenzione del sottosistema ASCV, è pari a 0,99994 corrispondente ad una indisponibilità di 31 min. all'anno.

PARTE SECONDA

Analisi di disponibilità di Impianto idrico antincendio

1. Impostazione

L'analisi di disponibilità sviluppata in questa sede è applicata ad un impianto esistente per il quale sono sviluppate due ipotesi di progetto per l'impianto idrico antincendio: una con alimentazioni di "tipo ordinario" ed uno con alimentazioni di "tipo superiore", quali definiti di requisiti UNI 9490.

2. Tipologia dell'impianto considerato e specifiche antincendio richieste

Stante gli obiettivi riportati, l'impianto industriale considerato è soltanto di riferimento e scelto per le sue caratteristiche di semplicità. Esso è costituito da:

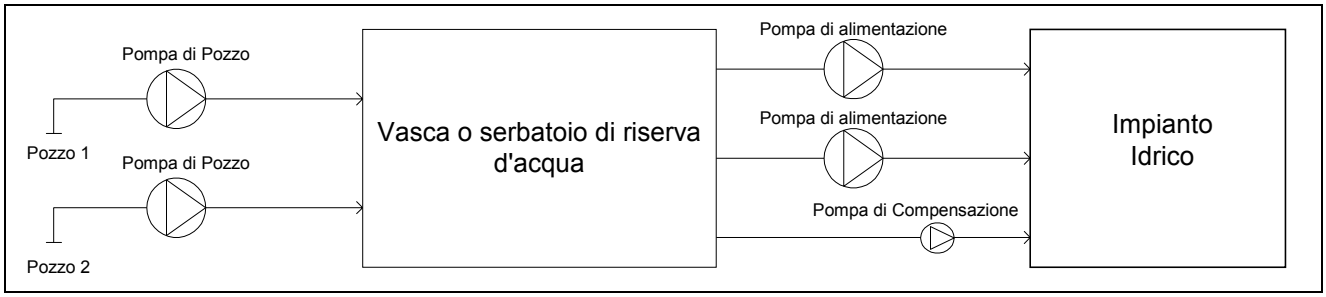
- un impianto di frazionamento aria con produzione di Ossigeno, Azoto, Argon;
- uno stoccaggio di gas criogenici sopra indicati, con le seguenti caratteristiche:
  - O_2 liquido (Lox) in serbatoio cilindrico verticale da 1000 m^3 (d ≈15m);
  - N_2 liquido in n.2 serbatoi orizzontali per circa 1500 t ciascuno;
  - Argon liquido in n.2 serbatoi di stoccaggio per circa 35 t ciascuno;
- n.4 rampe di carico delle sostanze criogeniche su ATB e di cui:
  - n.2 rampe di carico per Lox;
  - n.1 rampa di carico per Azoto liquido;
  - n.1 rampa di carico per Argon liquido.

L'area di impianto (impianto di frazionamento + stoccaggio) ha una superficie occupata di S=4500 m2.

3. Soluzioni di rete antincendio con tipologia ordinaria (A) e con tipologia superiore (B) per le alimentazioni

Lo schema generale e la tipologia delle fonti idriche utilizzabili nel caso specifico presentato sono le stesse, nelle due sezioni. Diverse sono le scelte e le dimensioni di alcuni componenti base, le funzioni svolte e pertanto lo schema funzionale d'impianto, considerando le unità ausiliare di rincalzo, di reintegro, di controllo e segnalazione, nonché le caratteristiche di allacciamento delle alimentazioni elettriche.

Schema generale delle alimentazioni



Schema generale dell'impianto idrico

- Maglia rettangolare di lato 53 m·85 m
- Idranti soprasuolo: n.4 DN70 ai vertici della maglia; n.4 DN45 ai punti medi di ciascun lato.

Soluzione A

- Riserva d'acqua: vasca interrata da 50 m3, pertanto con necessità di rincalzo entro un'ora di funzionamento (UNI 9490-4.8.2.1).
- n.2 pompe tipo Grundfos innescanti in 2 pozzi separati: alimentazioni con funzioni di rincalzo in funzionamento e di reintegro ad impianto fermo, se necessario; ciascuna pompa ha prestazioni sufficienti per tali funzioni: portata di 22 m3/h con prevalenza di 60 m e 56 m3/h con prevalenza di 25 m.
- n.2 pompe di alimentazione impianto tipo DAB-K50-800T: entrambe le pompe richiedono un'installazione ed un impianto per alimentazione soprabattente (vedi schema in fig.1), con portata di 45 m3/h con prevalenza di 35 m e 35 m3/h con prevalenza di 40 m (per sopperire alla richiesta massima sono necessarie entrambe le pompe in funzionamento).
- n.1 pompa di compensazione, al fine di assicurare sempre sull'impianto idrico (sempre pieno d'acqua) una pressione adeguata; l'installazione è del tipo soprabattente; portata di 7.5 m3/h, con avviamento automatico comandato da presso stato (90% Pst).

<u>Collegamento dell'alimentazione elettrica</u>

L'alimentazione elettrica è fornita da n.2 linee distinte e separate:

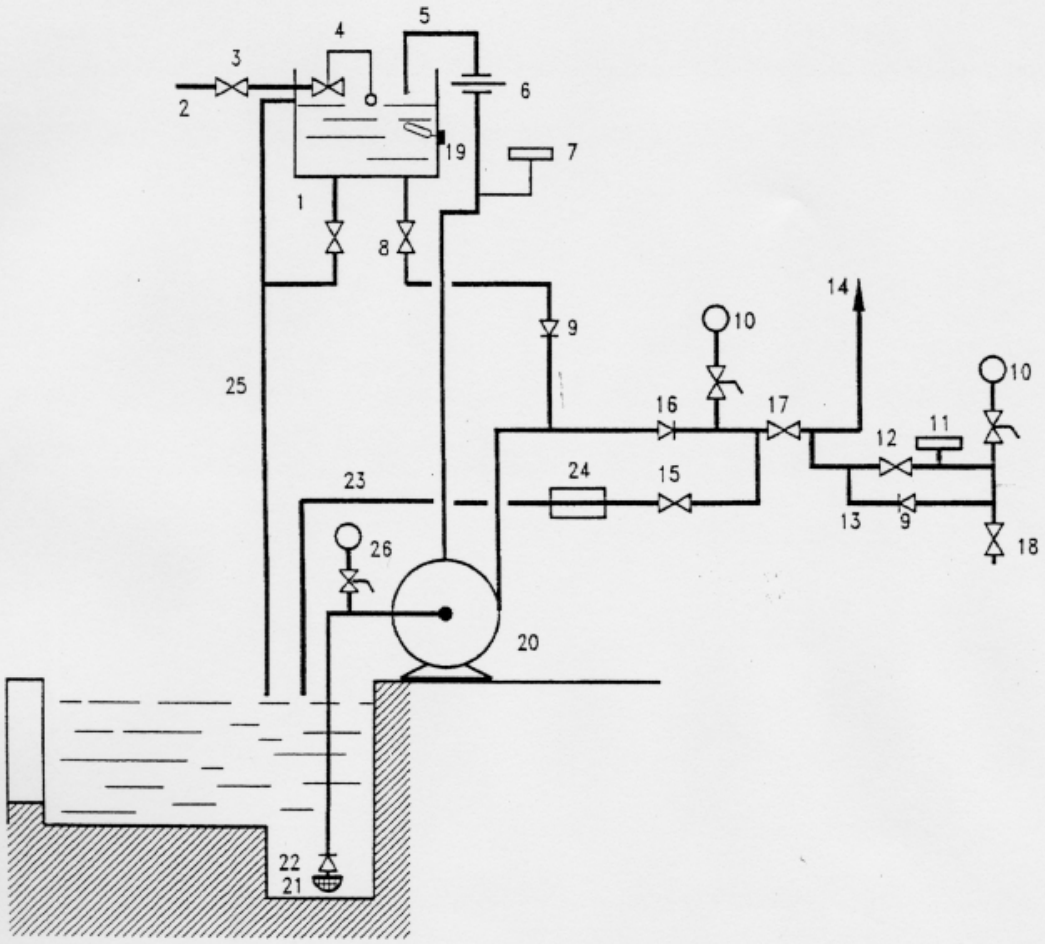
- linea A: linea ENEL di normale distribuzione;
- linea B: linea ENEL preferenziale.

Ciascuna linea è in grado di fornire la potenza sufficiente alle alimentazioni (principali più ausiliare e rincalzi); il collegamento è eseguito con allacciamento separato di una singola linea, su un singolo gruppo di alimentazione.

<u>Caratteristiche della soluzione A</u>

Essa, benché soddisfi ai requisiti di "tipo ordinario" riportati al punto 4.9.9 di UNI 9490, risponde alla massima richiesta d'acqua con le seguenti limitazioni:

- dispone di una riserva d'acqua insufficiente per la prevista durata globale di incendio di 69 minuti e richiede, pertanto, un rincalzo (sia pur previsto dalla normativa); tale riserva è realizzata con vasca interrata;
- il rincalzo è fornito da pozzi, sia pur ridondati (n.2, ciascuno con pompa sufficiente al rincalzo ed al ripristino);
- essendo la vasca interrata, l'installazione della pompa di alimentazione dell'impianto deve essere soprabattente, soluzione accettata ma mai consigliata non fosse altro che per la necessità di installazione di un serbatoio d'innesco e relativo collegamento, sempre riempito d'acqua, con pompa e condotta pescante.



1 Serbatoio di adescamento
2 Alimentazione serbatoio di adescamento
3 Valvola di intercettazione
4 Valvola a galleggiante
5 Ricircolo e sfogo d'aria
6 Diaframma ricircolo acqua
7 Pressostato pompa in moto
8 Valvola intercettazione adescamento
9 Valvola di non ritorno
10 Manometro
11 Pressostato d'avviamento
12 Valvola intercettazione pressostato
13 Collegamento al pressostato d'avviamento
14 Collegamento all'impianto
15 Valvola prova pompa
16 Valvola di non ritorno in mandata
17 Saracinesca mandata
18 Valvola di scarico
19 Regolatore di livello elettrico
20 Pompa
21 Filtri
22 Valvola di fondo
23 Tubazione prova portata pompa
24 Misuratore di portata
25 Scarico di troppo pieno
26 Manovuotometro

Fig.1 - Schema di installazione di una pompa di alimentazione soprabattente

Soluzione B

- Riserva d'acqua: costituita da un serbatoio a gravità da 100 m3 pertanto adeguato alla richiesta d'acqua senza bisogno di rincalzo.
- n.2 pompe tipo Grundfos innescanti in 2 pozzi separati, con funzione di puro reintegro; portate da 22 m3/h con prevalenza di 60 m e 56 m3/h con prevalenza di 25 m.
- n.2 pompe di alimentazione impianto tipo DAB-K50-800T: installazione di ciascuna pompa per alimentazione sottobattente (vedi schema in fig.3); portata di 45 m3/h con prevalenza di 35 m e 35 m3/h con prevalenza di 40 m.
- pompa di compensazione: atta ad assicurare nella rete immessa la pressione di esercizio, con portata di 35 m3/h ed installazione per alimentazione sottobattente.

Collegamento dell'alimentazione elettrica

L'alimentazione elettrica è fornita da n.2 linee distinte (vedi soluzione A), ma con potenza sufficiente ad alimentare tutti i gruppi di alimentazione idrica. Lo schema di collegamento è realizzato come riportato in fig.4 che permette l'utilizzo "in riserva" di una delle 2 linee.

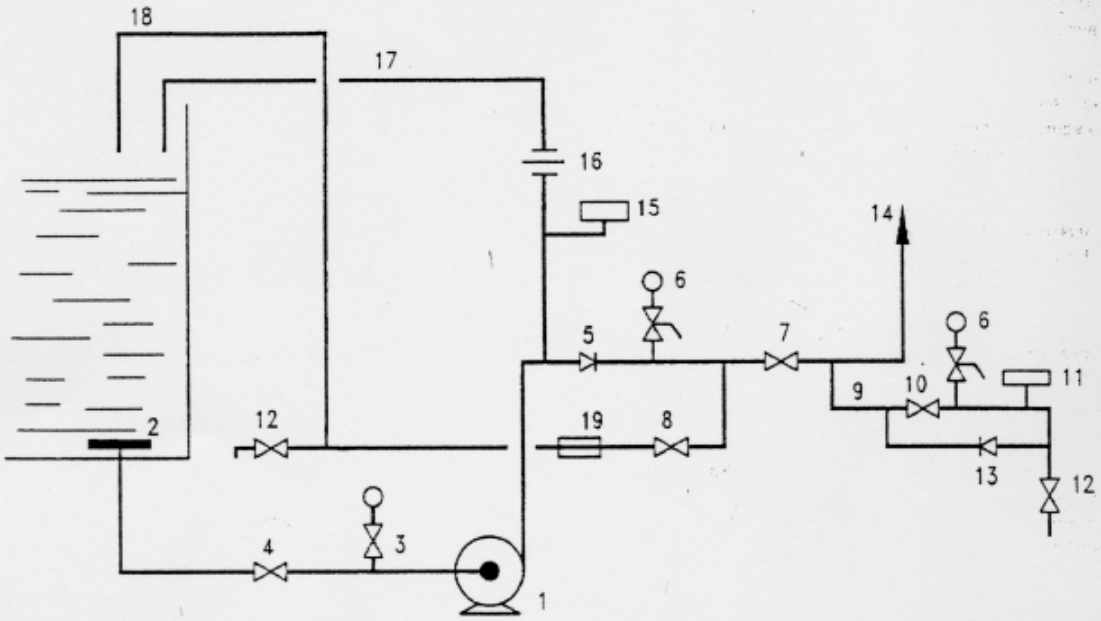
Caratteristiche della soluzione B

Essa soddisfa ai requisiti per alimentazione "di tipo superiore" UNI 9490, pag.499, 4.11.1.

Dispone di una riserva d'acqua in serbatoio a gravità, di capacità adeguata alla richiesta.

Il reintegro è fornito con raddoppio e l'alimentazione principale di impianto è realizzata con installazione sottobattente.

Le linee elettriche di alimentazione sono collegate in reciproca ridondanza.



1 Pompa
2 Antivortice (eventuale)
3 Manovuotometro
4 Saracinesca aspirazione
5 Valvola di non ritorno in mandata
6 Manometro
7 Saracinesca in mandata
8 Valvola prova pompa
9 Collegamento al pressostato d'avviamento
10 Valvola intercettazione pressostato
11 Pressostato d'avviamento
12 Valvola di scarico
13 Valvola di non ritorno
14 Collegamento all'impianto
15 Pressostato pompa in moto
16 Diaframma ricircolo acqua
17 Ricircolo e sfogo d'aria
18 Tubazione prova portata pompa
19 Misuratore di portata

Fig.3 - Schema di installazione di una pompa di alimentazione sottobbattente

4. Analisi di disponibilità

Conformemente agli obiettivi posti in premessa l'analisi di disponibilità del sistema di alimentazione dell'impianto idrico antincendio, nelle due soluzioni descritte in Cap.3 è sviluppata secondo metodologia CENELEC riferita ad una analisi RAM, seguendone i passi procedurali.

Occorre considerare che la presente applicazione è del tutto particolare in quanto l'analisi deve qualificare la capacità di risposta di un sistema normalmente in stand-by richiamato solo da un evento di probabilità estremamente bassa o da un test di determinata frequenza. Convenzionalmente in questa sede si adotta il criterio di far riferimento per la valutazione di disponibilità alla richiesta di funzionamento dell'impianto quale imposta da un test che viene ripetuto con un intervallo pari a 4380 ore (due test l'anno).

4.1. Profilo di missione

La metodologia individua le funzioni principali svolte dal sistema in esame che nel caso in oggetto possono essere individuate come segue:

1. fornitura pronta su chiamata della portata d'acqua prevista in specifica per un tempo minimo quale previsto pure in specifica;

2. mantenimento del sistema in condizioni idonee alla fornitura richiesta, durante tutto il tempo di stand-by.

Da tali funzioni viene individuata per il sistema una unica missione definibile come segue.

Missione del sistema: disponibilità alle due funzioni indicate.

In questa sede vengono indicate le condizioni ambientali nelle quali è richiesta la missione del sistema. Tali condizioni sono ovviamente quelle relative ad un sistema fisso in luogo aperto e definito, per l'individuazione dell'affidabilità dei suoi componenti con il termine Ground Fixed.

4.2. Strutture gerarchica del sistema

Il sistema, per comodità d'analisi è suddiviso normalmente in sottosistemi e questi in unità intermedie, se nel caso, e componenti. Per il sistema in oggetto si sono individuati i seguenti sottosistemi:

- Sottosistema di alimentazione principale dell'impianto idrico (SAP)
- Sottosistema di riserva d'acqua (SR)
- Sottosistema di alimentazione ausiliaria (rincalzo/ripristino della riserva d'acqua) (SAA)
- Sottosistema di alimentazione elettrica (SAE)

La struttura di tali sottosistemi sono in parte descritti in fig.1, fig.2, fig.3, fig.4; non si vede la necessità di introdurre unità intermedie ma si attribuirà a ciascun sottosistema i componenti principali che lo costituiscono.

In riferimento agli obbiettivi dell'attuale rapporto, non si ritiene pertinente una individuazione completa di tutti i componenti (vitali o ausiliari) presenti nel sistema. Verranno indicati pertanto soltanto i componenti "vitali" o indirettamente influenti perché venga assolta la missione indicata.

Tale ripartizione è riportata nelle tabelle che seguono, compilate in riferimento alla soluzione A e alla soluzione B di cui al Cap.3.

Soluzione A				
Livello		**Simbolo**	**Descrizione**	**Quantità**
Sottosistema di alimentazione principale dell'impianto idrico		SAP	Gruppo pompe di alimentazione del impianto idrico	
	Componente	SAP1	Pompa tipo DAB-K50-800T	2
	Componente	SAP2	Saracinesca di mandata	1
	Componente	SAP3	Pressostato di avviamento	1
	Componente	SAP4	Valvola prova pompa	1
	Componente	SAP5	Serbatoio di addescamento	1
	Componente	SAP6	Valvola di intercettazione adescamento	1
	Componente	SAP7	Misuratore di livello addescamento	1
	Componente	SAP8	Valvola di alimentazione addescamento	11
	Componente	SAP9	Valvola di fondo	1
Sottosistema di riserva d'acqua		SR	Vasca interrata 50 m^3	1
	Componente	SR1	Misuratore di livello in vasca	1
	Componente	SR2	Allarme di basso livello	1
	Componente	SR3	Scarico di troppo pieno	1
Sottosistema di alimentazione ausiliaria		SAA	Sottosistema di rincalzo/ripristino della riserva d'acqua)	
	Componente	SAA1	Pompa tipo Grundfos	2
	Componente	SAA2	Valvola di fondo	2
	Componente	SAA3	Attuatore avviamento pompa	2
Sottosistema di alimentazione elettrica		SAE	Alimentazione elettrica	1
	Componente	SAE1	Linea 1 (ordinaria)	1
	Componente	SAE2	Interruttore linea 1 su una pompa di alimentazione	1
	Componente	SAE3	Interruttore linea 1 su una pompa di pozzo (e/o pompa di compensazione)[2]	1
	Componente	SAE4	Linea 2 (preferenziale)	1
	Componente	SAE5	Interruttore linea 2 su una pompa di alimentazione	1
	Componente	SAE6	Interruttore linea 2 su una pompa di pozzo (e/o pompa di compensazione)	1

Soluzione B				
Livello		**Simbolo**	**Descrizione**	**Quantità**
Sottosistema di alimentazione principale dell'impianto idrico		SAP	Gruppo pompe di alimentazione del impianto idrico	
	Componente	SAP1	Pompa tipo DAB-K50-800T	2
	Componente	SAP2	Saracinesca di mandata	1
	Componente	SAP3	Pressostato di avviamento	1
	Componente	SAP4	Valvola prova pompa	1
	Componente	SAP5	Saracinesca aspirazione	1
Sottosistema di riserva d'acqua		SR	Serbatoio a gravità 100 m^3	1
	Componente	SR1	Misuratore di livello in vasca	1
	Componente	SR2	Allarme di basso livello	1
	Componente	SR3	Scarico di troppo pieno	1

[2] La pompa di compensazione serve per mantenere la pressione richiesta in condizioni di stand-by. Il suo cattivo funzionamento, o perdite ingenti delle linee, determinano l'avviamento delle pompe principali, segnalando la condizione anomala.

Soluzione B				
Livello		**Simbolo**	**Descrizione**	**Quantità**
Sottosistema di alimentazione ausiliaria		SAA	Sottosistema di rincalzo/ripristino della riserva d'acqua)	
	Componente	SAA1	Pompa tipo Grundfos	2
	Componente	SAA2	Valvola di fondo	2
	Componente	SAA3	Attuatore avviamento pompa	2
Sottosistema di alimentazione elettrica		SAE	Alimentazione elettrica	1
	Componente	SAE1	Linea 1 (ordinaria)	1
	Componente	SAE2	Interruttore linea 1 su una pompa di pozzo (e/o pompa di compensazione)	1
	Componente	SAE3	Linea 2 (preferenziale)	1
	Componente	SAE4	Interruttore linea 2 su una pompa di pozzo (e/o pompa di compensazione)	1
	Componente	SAE5	Interruttore e deviatore di linea[3]	1

4.3. Affidabilità del sistema

La normativa CENELEC individua due modelli di affidabilità: Affidabilità di base ed Affidabilità di missione.

L'Affidabilità di base è definita come la probabilità del sistema di operare senza alcun guasto. Essa è pertanto indipendente dall'influenza che il guasto di un qualunque componente può avere sulla missione.

L'Affidabilità di missione viene definita come la probabilità del sistema a soddisfare la missione assegnatali.

4.3.1. Affidabilità di base del sistema

Nel calcolo dell'affidabilità di base, al fine di elaborare i guasti dei singoli componenti con algoritmi omogenei, essi sono espressi in termini di Rateo di guasto λ (eventi/h). Ove fosse disponibile e significativa la sola probabilità di risposta su chiamata (P), il λ corrispondente può essere ricavato dall'espressione λ= n P dove n è il numero di chiamate (test) nel tempo di riferimento (un'ora). In generale nella presente valutazione viene seguita la periodicità di test richiesta dalla norma UNI 9490 e pari a 2 test l'anno.

Soluzione A		
Sottosistema	Componenti	Λ (h^{-1})
Sottosistema di alimentazione principale dell'impianto idrico	Pompa tipo DAB-K50-800T	$2 \cdot 1/4380 \cdot 10^{-3} = 0.457 \cdot 10^{-6}$
	Saracinesca di mandata	$1/4380 \cdot 10^{-4} = 0.228 \cdot 10^{-7}$
	Pressostato di avviamento	10^{-6}
	Valvola prova pompa	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Serbatoio di addescamento	10^{-7} (leakage)
	Valvola di intercettazione adescamento	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Misuratore di livello addescamento	10^{-6}
	Valvola di alimentazione addescamento	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Valvola di fondo	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	TOTALE	$\mathbf{4.778 \cdot 10^{-6}}$

[3] Ciascuna linea tramite i deviatori po' fornire tensione ad entrambe le pompe di alimentazione (vedi fig.4)

Soluzione A		
Sottosistema	Componenti	Λ (h^{-1})
Sottosistema di riserva d'acqua	Vasca interrata 50 m^3	10^{-6} (leakage)
	Misuratore di livello in vasca	10^{-6}
	Allarme di basso livello	10^{-6}
	Scarico di troppo pieno	10^{-7} (ostruzione)
	TOTALE	$\mathbf{3.1 \cdot 10^{-6}}$
Sottosistema di alimentazione ausiliaria	Pompa tipo Grundfos	$2 \cdot 1/4380 \cdot (3 \cdot 10^{-3}) = 0.457 \cdot 10^{-6}$
	Valvola di fondo	$2 \cdot 1/4380 \cdot 10^{-3} = 0.457 \cdot 10^{-6}$
	Attuatore avviamento pompa	$2 \cdot 1/4380 \cdot (3 \cdot 10^{-3}) = 1.36 \cdot 10^{-6}$
	TOTALE	$\mathbf{2.3 \cdot 10^{-6}}$
Sottosistema di alimentazione elettrica	Linea 1 (ordinaria)	$1/4380 \cdot (3 \cdot 10^{-4}) = 0.68 \cdot 10^{-7}$
	Interruttore linea 1 su una pompa di alimentazione	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Interruttore linea 1 su una pompa di pozzo (e/o pompa di compensazione)[4]	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Linea 2 (preferenziale)	$1/4380 \cdot (3 \cdot 10^{-4}) = 0.68 \cdot 10^{-7}$
	Interruttore linea 2 su una pompa di alimentazione	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Interruttore linea 2 su una pompa di pozzo (e/o pompa di compensazione)	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	TOTALE	$\mathbf{1.05 \cdot 10^{-6}}$
Sistema complessivo soluzione A		$\mathbf{\underline{1.13 \cdot 10^{-5}}}$

Soluzione B		
Sottosistema	Componenti	Λ (h^{-1})
Sottosistema di alimentazione principale dell'impianto idrico	Pompa tipo DAB-K50-800T	$2 \cdot 1/4380 \cdot 10^{-3} = 0.457 \cdot 10^{-6}$
	Saracinesca di mandata	$1/4380 \cdot 10^{-4} = 0.228 \cdot 10^{-7}$
	Pressostato di avviamento	10^{-6}
	Valvola prova pompa	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Valvola di fondo	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	TOTALE	$\mathbf{1.9 \cdot 10^{-6}}$
Sottosistema di riserva d'acqua	Vasca interrata 50 m^3	10^{-6} (leakage)
	Misuratore di livello in vasca	10^{-6}
	Allarme di basso livello	10^{-6}
	Scarico di troppo pieno	10^{-7} (ostruzione)
	TOTALE	$\mathbf{3.1 \cdot 10^{-6}}$

[4] La pompa di compensazione serve per mantenere la pressione richiesta in condizioni di stand-by. Il suo cattivo funzionamento, o perdite ingenti delle linee, determinano l'avviamento delle pompe principali, segnalando la condizione anomala.

Soluzione B		
Sottosistema	Componenti	Λ (h^{-1})
Sottosistema di alimentazione ausiliaria	Pompa tipo Grundfos	$2 \cdot 1/4380 \cdot (3 \cdot 10^{-3}) = 0.457 \cdot 10^{-6}$
	Valvola di fondo	$2 \cdot 1/4380 \cdot 10^{-3} = 0.457 \cdot 10^{-6}$
	Attuatore avviamento pompa	$2 \cdot 1/4380 \cdot (3 \cdot 10^{-3}) = 1.36 \cdot 10^{-6}$
	TOTALE	$\mathbf{2.3 \cdot 10^{-6}}$
Sottosistema di alimentazione elettrica	Linea 1 (ordinaria)	$1/4380 \cdot (3 \cdot 10^{-4}) = 0.68 \cdot 10^{-7}$
	Interruttore linea 1 su una pompa di pozzo (e/o pompa di compensazione)[5]	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Linea 2 (preferenziale)	$1/4380 \cdot (3 \cdot 10^{-4}) = 0.68 \cdot 10^{-7}$
	Interruttore linea 2 su una pompa di pozzo (e/o pompa di compensazione)	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	Interruttore e deviatore di linea	$1/4380 \cdot 10^{-3} = 0.2285 \cdot 10^{-6}$
	TOTALE	$\mathbf{0.82 \cdot 10^{-6}}$
Sistema complessivo soluzione B		$\mathbf{0.82 \cdot 10^{-5}}$

4.3.2. Manutenibilità

L'analisi viene condotta facendo riferimento al parametro considerato più significativo, per descrivere lo stato di manutenibilità del sistema, ovvero l'MTTR (mean time to repaire).

Al fine dell'analisi, è necessario procedere come nel caso precedente all'individuazione, per il sistema in oggetto, delle singole LRU (line replaceable unit), ovvero delle unità che in caso di guasto vengono sostituite o riparate. In pratica, quindi, si considera che in caso di guasto, non è necessariamente il singolo componente ad essere riparato o sostituito, ma che l'azione manutentiva possa riguardare un unità di livello superiore (un insieme di componenti che comprenda anche quello guasto).

Nel caso in esame, vista la semplicità del sistema e le caratteristiche dei componenti si è ritenuto corretto individuare ogni singolo componente come singola LRU.

I tempi costituenti l'Elapsed Time in questo caso derivano dalle seguenti azioni manutentive elementari:

1. Diagnosi
2. Accesso
3. Rimozione o Riparazione
4. Richiusura
5. Test.

Per tutte queste operazioni, su ogni singola LRU, sono indicati di seguito i rispettivi tempi di svolgimento.

[5] La pompa di compensazione serve per mantenere la pressione richiesta in condizioni di stand-by. Il suo cattivo funzionamento, o perdite ingenti delle linee, determinano l'avviamento delle pompe principali, segnalando la condizione anomala.

Soluzione A

LRU	Quantità	Diagnosi (min)	Accesso (min)	Rimozione/ Riparazione (min)	Richiusura (min)	Test (min)	Totale (min)	Elapsed time (h)	Tasso totale di guasto del sistema	MTTR (h)
SAP1	2	15	5	120	5	15	160	2.67	4.57E-07	
SAP2	1	5	5	60	5	5	80	1.33	2.28E-08	
SAP3	1	5	5	15	5	15	45	0.75	1.00E-06	
SAP4	1	5	5	20	5	5	40	0.67	2.29E-07	
SAP5	1	5	60	60	10	5	140	2.33	1.00E-07	
SAP6	1	5	5	20	5	5	40	0.67	2.29E-07	
SAP7	1	10	5	15	5	15	50	0.83	1.00E-06	
SAP8	1	5	5	20	5	5	40	0.67	2.29E-07	
SAP9	1	5	5	20	5	5	40	0.67	2.29E-07	
SR1	1	5	5	15	5	15	45	0.75	1.00E-06	
SR2	1	5	5	15	5	15	45	0.75	1.00E-06	
SR3	1	5	10	20	10	20	65	1.08	1.00E-07	
SR4	1	120	60	120	60	60	420	7.00	1.00E-06	
SAA1	2	15	5	120	5	15	160	2.67	4.57E-07	
SAA2	2	5	5	20	5	5	40	0.67	4.57E-07	
SAA3	2	5	5	15	5	15	45	0.75	1.36E-06	
SAE1	1	5	5	30	5	10	55	0.92	6.80E-08	
SAE2	1	5	5	20	5	5	40	0.67	2.29E-07	
SAE3	1	5	5	20	5	5	40	0.67	2.29E-07	
SAE4	1	5	5	30	5	10	55	0.92	6.80E-08	
SAE5	1	5	5	20	5	5	40	0.67	2.29E-07	
SAE6	1	5	5	20	5	5	40	0.67	2.29E-07	
									9.9E-06	**1.57**

Soluzione B

LRU	Quantità	Diagnosi (min)	Accesso (min)	Rimozione/ Riparazione (min)	Richiusura (min)	Test (min)	Totale (min)	Elapsed time (h)	Tasso totale di guasto del sistema	MTTR (h)
SAP1	2	15	5	120	5	15	160	2.67	4.57E-07	
SAP2	1	5	5	60	5	5	80	1.33	2.28E-08	
SAP3	1	5	5	15	5	15	45	0.75	1.00E-06	
SAP4	1	5	5	20	5	5	40	0.67	2.29E-07	
SAP5	1	5	5	20	5	5	40	0.67	2.29E-07	
SR1	1	5	5	15	5	15	45	0.75	1.00E-06	
SR2	1	5	5	15	5	15	45	0.75	1.00E-06	
SR3	1	5	10	20	10	20	65	1.08	1.00E-07	
SR4	1	5	60	60	10	10	145	2.42	1.00E-06	
SAA1	2	15	5	120	5	15	160	2.67	4.57E-07	
SAA2	2	5	5	20	5	5	40	0.67	4.57E-07	
SAA3	2	5	5	15	5	15	45	0.75	1.36E-06	
SAE1	1	5	5	30	5	10	55	0.92	6.80E-08	
SAE2	1	5	5	20	5	5	40	0.67	2.29E-07	
SAE3	1	5	5	30	5	10	55	0.92	6.80E-08	
SAE4	1	5	5	20	5	5	40	0.67	2.29E-07	
SAE5	1	5	5	20	5	5	40	0.67	2.29E-07	
									8.2E-06	**1.16**

4.3.3. Affidabilità di missione e disponibilità del sistema

Per chiarezza metodologica si richiama l'apporccio normalmente seguito (vedi parte prima) se la missione è costituita da uno o più funzionamenti continuativi del sistema.

In tal caso l'Affidabilità di missione viene valutata dalle probabilità di guasto dei soli componenti vitali per la missione nella combinazione logica richiesta dalla missione stessa (vedi parte prima albero dei guasti).

Se ne ricava il corrispondente MTBF e la disponibilità del sistema viene definita come "disponibilità asintotica" espressa dalla relazione:

$$A=MTBF/(MTBF+MTTR)$$

Nel caso in esame, in cui la missione è rivolta ad un sistema normalmente in “stand by” al quale viene chiesto di fornire un funzionamento con determinate prestazioni per un certo tempo, **si propone** di rappresentare la disponibilità del sistema direttamente con la sua affidabilità di missione.

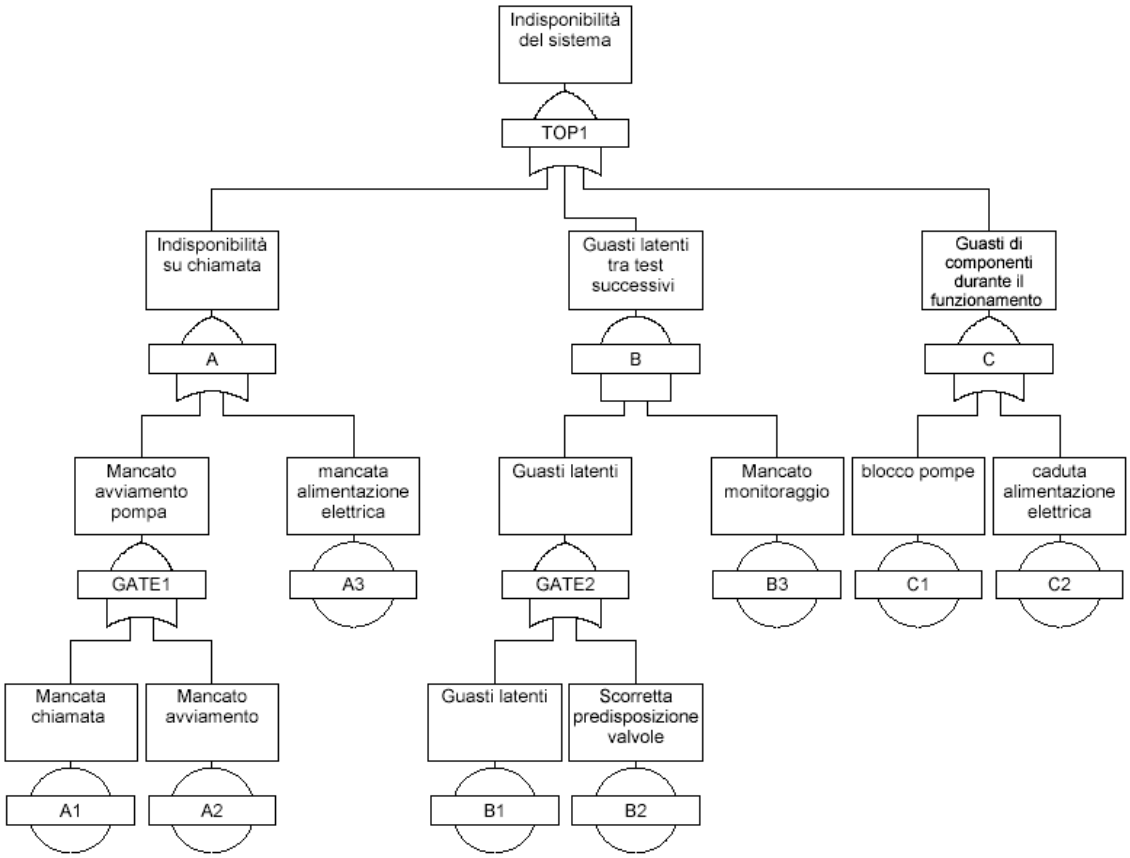
Quest’ultima viene poi ricavata come complemento ad uno della combinazione logica delle probabilità di insuccesso relative a diverse modalità di guasto dei suoi componenti vitali (vedi master logic diagramme delle indisponibilità).

Sono state identificate tre diverse modalità di guasto per il sistema in esame:

a. mancata risposta diretta su chiamata di componenti vitali (gruppo pompe di alimentazione, alimentazione elettrica);
b. indisponibilità delle alimentazioni ausiliarie, della riserva d’acqua e delle predisposizioni del sistema, a causa di guasti verificatisi durante il tempo tra due test consecutivi (4380 h) e non monitorati (guasti latenti);
c. indisponibilità di componenti vitali per guasti che possono intervenire durante il tempo di funzionamento richiesto (1 h).

Vengono considerati nella valutazione in oggetto solo i componenti essenziali e viene trascurata la possibilità di successivi interventi operativi.

I dati affidabilistici di mancata risposta su chiamata e di guasto in funzionamento sono stati desunti dal “Fermi Lab ES&H Manual” per completezza ed omogeneità degli stessi.



Master logic diagramme

Soluzione A

Simbolo	Tipo di guasto	Correlazioni logiche	Probabilità
A1	Mancata richiesta pressostati	OR sulle due pompe	2×10^{-4}
A2	Mancato avviamento pompe (pompa + motore)	OR sulle due pompe	2.6 x 10-3
A3	Mancata tensione sulle linee (per 1h di interruzione)	OR delle due linee	6 x 10-4
A1+A2+A3			**3.4 x 10-3**
B1	Mancanza d'acqua nel serbatoio di adescamento senza reintegro	OR sulle due pompe	4.4 x 10-3
B2/a	Mancata apertura valvola di intercettamento / adescamento	OR sulle due pompe	6 x 10-3
B2/b	Mancata apertura della saracinesca di mandata	OR sulle due pompe	2 x 10-3
B3	Mancato monitoraggio	OR sulle due pompe	6 x 10-2
(B1+B2/a+B2/b) x B3			**0.74 x 10-3**
C1/a	Inadeguata riserva d'acqua senza rincalzo (in 4380 h)	OR sulle due pompe	6 x 10-3
C1/b	Blocco pompa in funzionamento (1 h)	OR sulle due pompe	10-4
C2	Caduta alimentazione elettrica	OR sulle due linee	10-4
C1/a + C1/b + C2			**6.2 x 10-3**
Totale soluzione A			**10.3 x 10-3**
Disponibilità soluzione A = 1 - 10.3 x 10-3			**98.97%**

Si palesa la forte penalizzazione apportata dalla vasca interrata con capacità inadeguata e dal sistema di alimentazione sopra battente.

Soluzione B

Simbolo	Tipo di guasto	Correlazioni logiche	Probabilità
A1	Mancata richiesta pressostati	OR sulle due pompe	2×10^{-4}
A2	Mancato avviamento pompe (pompa + motore)	OR sulle due pompe	2.6×10^{-3}
A3	Mancata tensione sulle linee (per 1h di interruzione)	AND delle due linee	10^{-7}
A1+A2+A3			**2.8×10^{-3}**
B1	Non più pertinente	-	-
B2/a	Non più pertinente	-	-
B2/b	Mancata apertura della saracinesca di mandata	OR sulle due pompe	2×10^{-3}
B3	Mancato monitoraggio	OR sulle due pompe	6×10^{-2}
B2/b x B3			**1.2×10^{-4}**
C1/a	Non più pertinente	-	-
C1/b	Blocco pompa in funzionamento (1 h)	OR sulle due pompe	10^{-4}
C2	Caduta alimentazione elettrica	AND delle due linee	10^{-7}
C1/b + C2			**10^{-4}**
Totale soluzione B			**3×10^{-3}**
Disponibilità soluzione A = 1 - 3×10^{-3}			**99.7%**

La presente valutazione è da considerare naturalmente indicativa.

CONCLUSIONI

L’applicazione della metodologia CENELEC è certamente consigliabile per **sistemi complessi con mansioni a funzionamento continuativo variamente articolato**.

Per valutazioni di disponibilità essa incoraggia un più attento esame dei guasti latenti e si presta ad una più completa analisi del sistema e studio delle varianti.