Analisi del rischio: un esempio applicativo al settore farmaceutico della Fault Tree Analysis

Attraverso l'analisi dell'albero dei guasti è possibile indicare quelle combinazioni di eventi che portano ad un certo evento critico (siano essi imputabili a guasti delle apparecchiature che ad errori umani) in modo da poter individuare le misure preventive atte a ridurre la probabilità dell'incidente. In questa prima parte ci si focalizzerà sul come si costruisce un albero dei guasti, mentre nella seconda parte si analizzerà un caso pratico

Parole chiave: Analisi del rischio • Evento critico • Classificazione dei guasti • Ripartizioni sterili • Eventi intermedi

L. Sabatini
Lesatec Srl – Opera – Milano

Introduzione

L' albero dei guasti, noto generalmente come Fault Tree Analysis, è una metodologia di analisi del rischio che tramite visualizzazione grafica consente di individuare le cause iniziatrici di incidenti che sono frutto di una complessa combinazione di eventi. Il risultato dell'analisi è un diagramma logico, mutuato dalla teoria delle decisioni che, in definitiva, risponde a questa domanda: *"Che cosa deve succedere perché si abbia un determinato guasto?"*.
È una tecnica induttiva che parte dagli eventi finali, detti Eventi Top o Eventi Critici, (scoppio, incendio, rilascio di materiale tossico, contaminazione al di fuori dei limiti, etc.) e risale ai guasti od agli errori iniziali (Fault). Un albero dei guasti è un diagramma costruito con l'utilizzo di porte logiche *and/or* che illustra le relazioni tra le cause iniziatrici e l'evento finale indesiderato mostrando al contempo il contributo di ogni fattore.

> …è una procedura completa attraverso la quale possono essere trovate tutte le combinazioni di eventi che conducono all'evento critico…

Operativamente occorre per prima cosa individuare i sistemi coinvolti nell'Evento Critico e procedere quindi nella catena di sistemi, sottosistemi, apparati, ecc., fino ad arrivare a valutare l'impatto dei guasti dei singoli componenti per i quali si devono conoscere i valori della probabilità di guasto da utilizzare nella valutazione (eventualmente facendo ricorso a banche dati). La combinazione di questi dati attraverso le operazioni logiche and/or riportate sul diagramma, permetterà di determinare la probabilità (P) dell'Evento Critico. Conoscendo la severità (X) connessa a tale evento è poi possibile calcolare il relativo rischio con la nota relazione:

$$R = P * X$$

L'analisi dell'albero dei guasti consente di trattare anche il contributo al rischio derivante da errori umani, così come di individuare le cause di guasto comuni a più sottosistemi. È quindi una procedura completa attraverso la quale possono essere trovate tutte le combinazioni di eventi che conducono all'evento critico, siano essi guasti di apparecchiature che errori umani permettendo di focalizzare l'attenzione sulle misure preventive per ridurre la probabilità dell'incidente. Essa può guadagnare in semplicità operando la suddivisione dei sistemi complessi in combinazioni logiche di sottosistemi (alberi), più semplici da analizzare. In questo caso un approccio di gruppo può essere preferibile in quanto ciascun membro potrebbe concentrarsi principalmente su un albero: l'interazione fra i membri del gruppo e di questi con personale esperto garantirebbe all'analisi completezza ed esaustività.
È chiaramente possibile utilizzare questa tecnica anche per una valutazione qualitativa del rischio. I limiti di questa tecnica sono dettati non dalla procedura ma dalla competenza o accuratezza di chi la usa.
Di seguito sintetizziamo le caratteristiche del metodo.

Obiettivo

Identificazione delle combinazioni di guasto di componenti ed errori umani che sono all'origine di un incidente.

Campo di applicazione

- In fase di progetto: può essere usato per identificare modi di guasto non usuali, con riduzione del rischio.
- In fase operativa: è uno strumento utile per valutare la probabilità di modi di guasto di tipo comune, inclusi gli interventi dell'operatore, sia autonomi che per l'inosservanza delle procedure.
- In generale: può essere usato quando si vuole determinare la probabilità di verificarsi di determinati incidenti e/o scenari.

Tipo e natura dei risultati

Con sufficienti dati di base, la procedura può dare risultati sia qualitativi che quantitativi. In ogni caso consente di individuare le combinazioni di guasto ed errore umano che originano specifici Eventi Critici (elenco degli eventi elementari concomitanti che possono provocare il danno) nonché la relativa importanza come contributo al rischio (influenza dei vari eventi elementari nel determinare il danno).

Requisiti

La preparazione di un albero dei guasti presuppone l'esatta conoscenza sia del funzionamento del sistema e dei suoi componenti in situazione di normale attività sia dei suoi modi di guasto e dei relativi effetti, dati questi ricavabili, ad esempio, da un precedente studio HAZOP, FMEA o FMECA.
Ogni albero deve essere predisposto da un singolo analista, con la collaborazione di operatori ed altro personale con esperienza nel funzionamento dei componenti e dei sistemi inclusi nell'analisi, in modo da avere le informazioni sui guasti che contribuiscono all'incidente.

Costruzione dell'Albero dei Guasti

L'albero dei guasti viene costruito per mezzo di grafi che uniscono gli eventi alle cause con simboli specifici rappresentanti funzioni logiche (vedi Fig. 1).
Il punto di partenza del grafo è l'Evento Critico da cui si risale alla/e possibile/i causa/e che lo possono produrre.

Esempio applicativo del metodo FTA

Consideriamo il caso di una cleanroom in esercizio nella quale si esegua la ripartizione asettica di un farmaco in fiale aperte.
Il locale riempimento sarà, quindi, caratterizzato da una classe "A" nella zona considerata critica (zona di riempimento ed eventuali depositi e percorsi sterili), e da una classe "B" (zona ad essa adiacente). Per simili locali è praticamente obbligatorio eseguire campionamenti

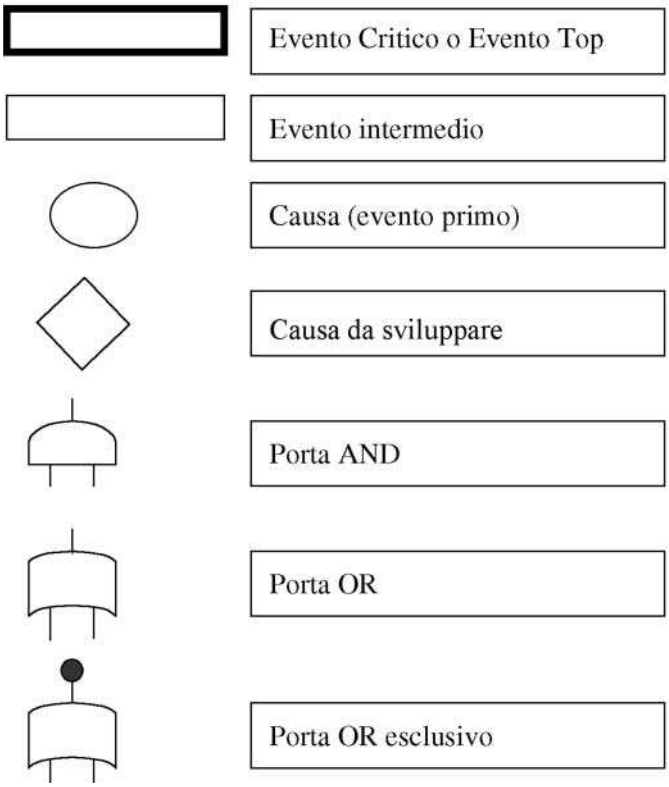


Fig. 1 Simbologia per la costruzione dell'albero dei guasti

continui, in condizioni operative, della concentrazione di particelle in aria sia nelle zone critiche che in almeno in un punto della zona "B" rappresentativo dell'impatto della contaminazione sulla qualità del prodotto finale. La posizione di questo punto, che nella figura 2 è indicato con "P", può essere definita, ad esempio, con l'ausilio della metodologia HACCP.
Consideriamo come Evento Critico il superamento non sistematico in "P" del limite della classe ISO 7 in condizioni operative e poniamoci l'obbiettivo di individuare le eventuali cause che lo possono determinare.

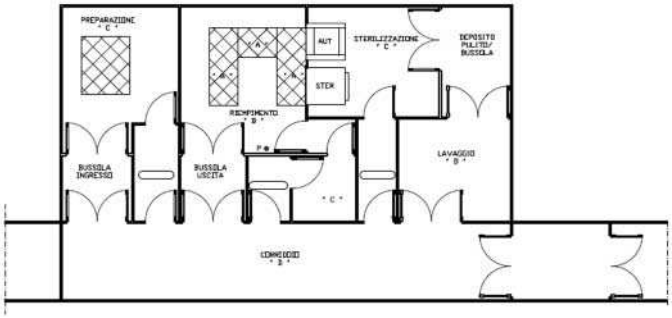


Fig. 2 Pianta reparto

Per eseguire una analisi FTA occorre inizialmente descrivere correttamente il sistema ed il suo funzionamento, e quindi valutare i guasti che possono averlo causato.

Descrizione del reparto di ripartizione sterile

Il reparto è basato su un locale di ripartizione al quale l'operatore accede per mezzo di uno spogliatoio in tre stadi di collegamento con il corridoio classificato "D". Le fiale riempite escono per mezzo di una bussola con porte interbloccate di collegamento con il corridoio "D". Le fiale sterili da riempire entrano tramite la porta sterile di una sterilizzatrice depirogenatrice e gli altri materiali tramite la porta sterile di un'autoclave. I principali locali ancillari (vedi Fig. 2) quindi sono i seguenti:
- Locale sterilizzazione in classe "C" con sterilizzatrice ed autoclave.
- Locale preparazione soluzione in classe "C" con dissolutore e sistema di filtrazione della soluzione.
- Locale lavaggio in classe "D" con lava fiale.

La ripartizione vera propria è fatta da una ripartitrice dotata di sezione di saldatura alla quale occorre addurre manualmente le fiale vuote con apposito cestello di carico e dalla quale occorre asportare i cestelli riempiti. Come dotazione pertinente alla produzione ipotizziamo la presenza di un carrello di servizio per i cestelli riempiti. La soluzione viene direttamente portata alla riempitrice con un sistema di pressurizzazione e di filtrazione sterile.
All'interno del locale di ripartizione lavora solo un operatore, "Operatore 1", mentre all'esterno lavora uno o più operatori che indicheremo genericamente con "Operatore 2".

Descrizione delle operazioni svolte dall'operatore 1:

- Ingresso operatore nel locale ripartizione e controllo della documentazione di produzione.
- Prelievo dei dispositivi e dei filtri finali dall'autoclave.
- Montaggio dei dispositivi e dei filtri.
- Controllo funzionale della riempitrice e delle sue impostazioni.
- Prelievo di tutti i carrelli dei contenitori primari dalla sterilizzatrice e loro posizionamento nel deposito sterile con chiusura della porta della sterilizzatrice.
- Caricamento dei contenitori primari sulla riempitrice.
- Inizio produzione con caricamento dei cestelli riempiti nel carrello di servizio.
- Spostamento del carrello riempito nella bussola di uscita e proseguo della produzione con i cestelli di un altro carrello.
- Ripetizione del ciclo per il numero di volte previsto per l'esaurimento del lotto.

Descrizione delle operazioni svolte dall'operatore 2:

- Prelievo del carrello riempito dalla bussola da parte dell'operatore 2, suo svuotamento ed adduzione del carrello al locale lavaggio per la sua pulizia e caricamento con altri cestelli di fiale lavate.
- Inserimento dei carrelli riempiti con fiale lavate nel locale sterilizzazione.
- Riempimento della sterilizzatrice dal locale sterilizzazione con i carrelli addoti dal locale lavaggio ed avvio nuovo ciclo di sterilizzazione.
- Ripetizione del ciclo per il numero di volte previsto per l'esaurimento del lotto.

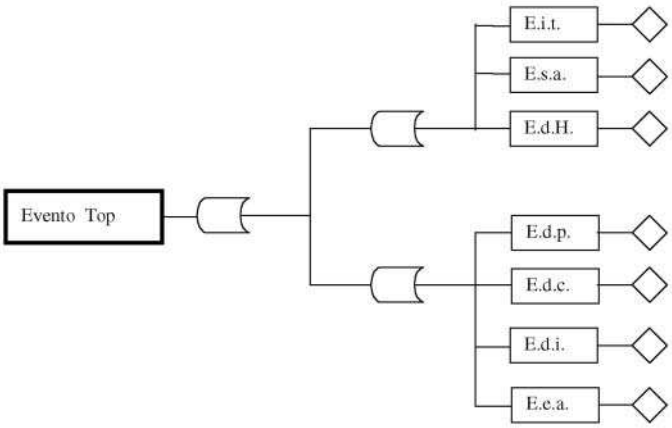
Valutazione dei guasti o malfunzionamenti che possono avere causato l'Evento Critico

Si può iniziare cercando di rispondere alla domanda: "cosa deve succedere per avere il guasto ipotizzato?".
Fra le cause possiamo porre:
- diminuzione di portata di aria;
- variazione della temperatura di ingresso dell'aria che altera i percorsi aerodinamici all'interno del locale riempimento;
- variazione della portata di estrazione dei gas di combustione delle fiamme che a sua volta induce variazioni dei percorsi aerodinamici;
- guasto non rilevato al sistema di controllo della pressione ambientale con aumento delle infiltrazioni;
- danneggiamento grave di uno o più filtri terminali;
- guasto al sistema di interblocco della bussola uscita materiali che ne permette l'apertura prima dello scadere del relativo recovery time;
- operatore che agisce non in conformità alla procedura qualificata per la produzione, per esempio muove i carrelli troppo velocemente;
- procedura qualificata di produzione non sufficientemente precisa per cui la ripetibilità dei dati dipende dalla bravura dell'operatore;
- procedura qualificata di produzione precisa ma non sufficientemente controllata nell'applicazione;
- procedura qualificata di produzione precisa ma operatore non correttamente addestrato;
- non corretta applicazione procedura di pulizia di fine lavoro;
- non corretto controllo applicazione procedura di pulizia;
- caduta di un cestello con fiale piene o vuote od altro evento di natura accidentale svincolato dai punti precedenti.

Tali eventi ipotetici possono essere suddivisi in categorie distinte per semplificare la costruzione dell'albero. Per stabilire quali eventi entrano in una categoria e quali no può essere scelto il criterio della connessione degli eventi che le compongono. In questo modo, se ciò è possibile, si individuano delle sequenze incidentali che possono essere analizzate indipendentemente. Queste sequenze, la cui corretta scelta dovrà però essere comprovata a posteriori, possono a loro volta essere suddivise in fasi distinte separatamente analizzate. Nel nostro caso possiamo fare le seguenti suddivisioni:

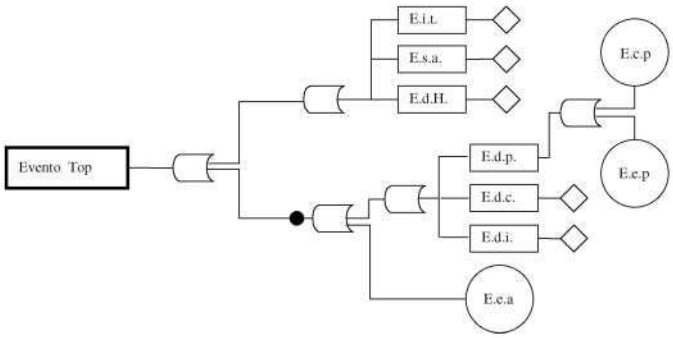
- Eventi connessi con impianto di trattamento aria (E.i.t.)
- Eventi connessi con sistemi ausiliari (interblocco bussola) (E.s.a.)
- Eventi connessi con danneggiamenti filtri HEPA terminali (E.d.H.)
- Eventi connessi con difetti procedurali (E.d.p.)
- Eventi connessi con difetto di controllo d'applicazione delle procedure (E.d.c.)
- Eventi connessi con difetto d'istruzione del personale (E.d.i)
- Eventi connessi con errori umani accidentali (E.e.a.)

Alla luce di quanto detto è possibile rappresentare il nostro albero dei guasti in questo modo:



Grafo 1

Tutti gli eventi intermedi segnati possono essere ulteriormente sviluppati.
Prima di procedere, è utile fare alcune riflessioni in merito all'errore accidentale.
Se le procedure sono corrette e correttamente applicate da operatori istruiti e controllati, gli eventi E.d.p, E.d.c., E.d.i. avranno probabilità assimilabile a "0" mentre l'evento E.e.a., pur avendo probabilità in questo caso molto bassa, sarà preponderante. Se invece uno degli altri eventi può accadere, l'influenza di E.e.a. sarà praticamente ininfluente. Questo stato di cose può essere reso bene dall'inserimento di una porta "OR ESCLUSIVO".
Si ricorda che tale operatore logico assume valore "1" (vero), quando gli ingressi sono diversi, assumendo il valore "0" (falso), quando gli ingressi sono uguali. Con questa ipotesi di lavoro l'evento E.e.a. può essere considerato come evento "causa" non ulteriormente sviluppabile.
In altri termini si esclude a priori la concomitanza dell'evento E.e.a con gli altri tre.



Grafo 2

L'evento E.d.p. può essere ulteriormente approfondito (vedi il Grafo 2). Considerando non realistica un'errata procedura dovuta all'imperizia dello staff che l'ha redatta, si possono ipotizzare due possibili cause prime:
- Non completa conoscenza della problematica di produzione (E.c.p.)
- Non rispondenza ergonomica del diagramma di produzione alla procedura (E.e.p.)

Gli eventi Edi e Edc possono anch'essi essere ulteriormente sviluppati oppure considerati come cause prime.

Summary *Fault tree analysis (FTA) is a risk analysis technique that visually models how logical relationships between equipment failures, human errors, and external events can combine to cause specific accidents. Thanks to this analysis is possible identify preventive measures to reduce accident probability*

Per ulteriori informazioni segnare sull'apposito tagliando il n. 1

Analisi del Rischio: un esempio applicativo al settore farmaceutico della Fault Tree Analysis

Dopo aver visto nella parte prima cos'è e come si costruisce un albero dei guasti, in questa parte inizieremo a sviluppare gli eventi intermedi individuati

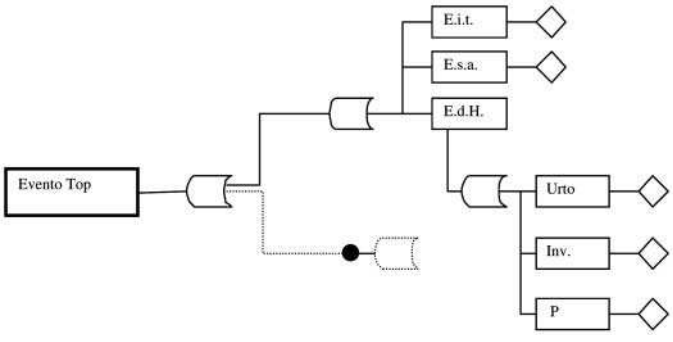
Parole chiave: Filtri HEPA • Danneggiamenti filtri • Sistemi ausiliari • Recovery Time

L. Sabatini
Lesatec Srl – Opera – MI

Eventi connessi con danneggiamenti filtri HEPA terminali (E.d.H.)

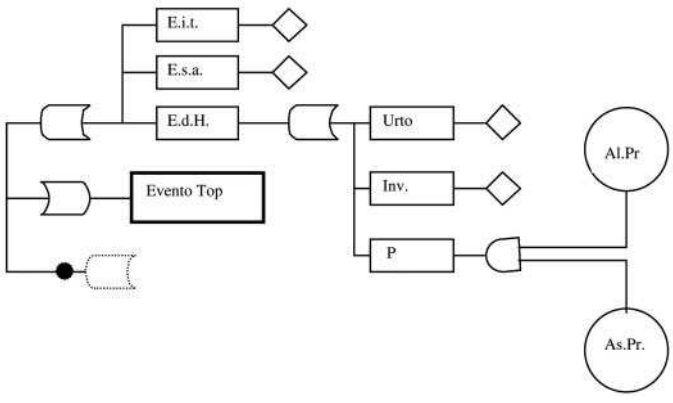
Consideriamo l'insieme di guasti che possono portare all'evento Top per problemi connessi alla rottura dei filtri HEPA.
Da un punto di vista concettuale un filtro HEPA più si intasa meglio filtra fino a quando non intervengono:
- problematiche legate all'invecchiamento (*Inv.*), che provocano un lento decadimento dell'efficienza di filtrazione;
- problemi di rottura innescati da salti di pressione troppo elevati (ΔP) che provocano la rottura meccanica delle fibre del filtro e quindi diminuzione rapida dell'efficienza di filtrazione;
- eventi traumatici accidentali quali danneggiamenti dovuti ad urti (*Urto*).

Le tre ipotesi di guasto possono essere inserite nell'albero per mezzo di una porta OR (vedi Grafo 3).
L'evento ΔP può essere sviluppato ulteriormente sulla base delle seguenti considerazioni:
- il ventilatore ha una prevalenza massima superiore alla pressione di rottura dei filtri HEPA (*Al.P*);
- è assente una procedura di controllo manuale od automatica delle perdite di carico di detti filtri (*As. P*).



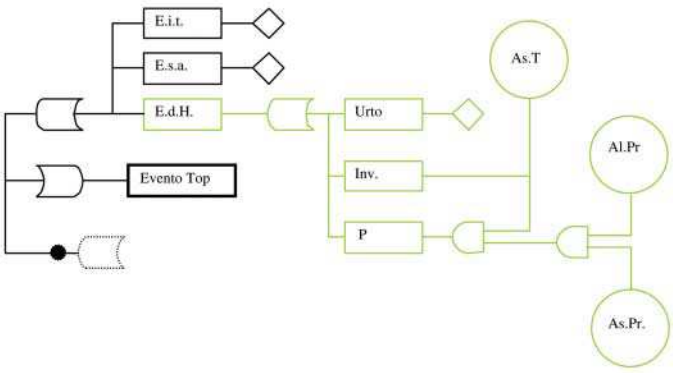
Grafo 3

Questi due eventi sono connessi attraverso una porta AND perché entrambi devono essere "veri" per avere l'evento ΔP "vero" e possono essere considerate cause iniziatrici (vedi Grafo 4).
Nella realtà il deterioramento conseguente all'evento ΔP, per la tipologia e l'uso continuo degli impianti considerati, assume un andamento non impulsivo ma di lento decremento dell'efficienza per cui una procedura di controllo basata sull'utilizzo pianificato del DPC leak test, che non peggiora le condizioni di intasamento dei filtri, o del Recovery Time può evidenziare tale degrado prima che insorgano seri problemi.
Altro tipo di fenomenologia da considerare in relazione a questo evento sono le rotture per stress meccanico connesse ai cicli di accensione. Anche questi deterioramenti da "fatica" possono essere evidenziati o imponendo un numero massimo di cicli di accensione oppure eseguendo i test prima elencati ad ogni riavvio; cosa oggettivamente assai semplice con il Recovery Time. L'esecuzione di tali test può però evidenziare anche l'in-



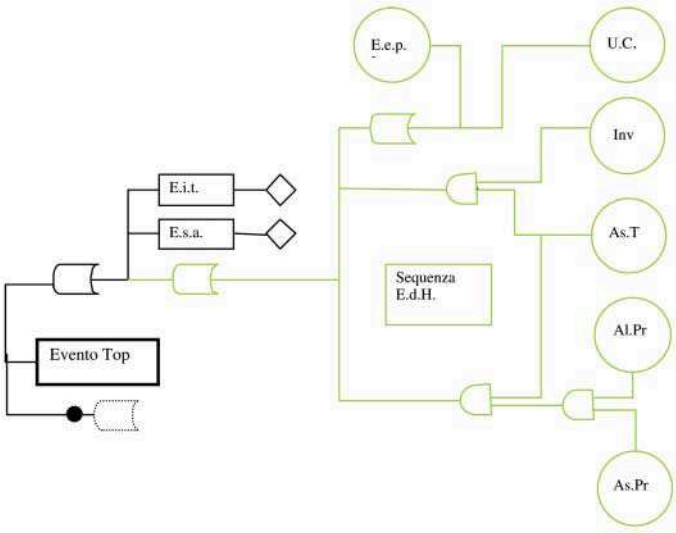
Grafo 4

sorgere di problemi connessi con l'invecchiamento.
Con queste ulteriori considerazioni, introducendo la causa prima "assenza di test" (*As. T*) il nostro albero si modifica come riportato nel Grafo 5.



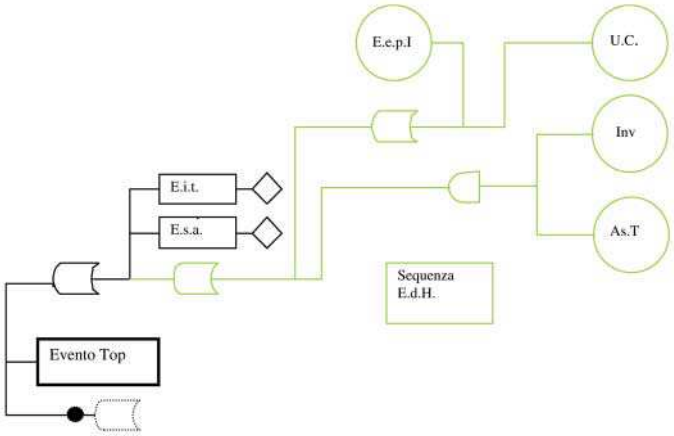
Grafo 5

Nella stesura dell'albero fino ad adesso abbiamo continuato a riportare per chiarezza esplicativa gli eventi intermedi che definivano la catena incidentale. Nella realtà una volta giunti alle rispettive cause iniziali ciò non è più necessario, anzi potrebbe indurre ad errori in fase di valutazione delle probabilità connesse con ogni singola sequenza. Nel Grafo 6 è applicato quanto sopra detto alla sequenza E.d.H. che, ricordiamo, rappresenta la sequenza di eventi che danno come risultato finale una diminuzione della efficienza di filtrazione dei filtri finali.

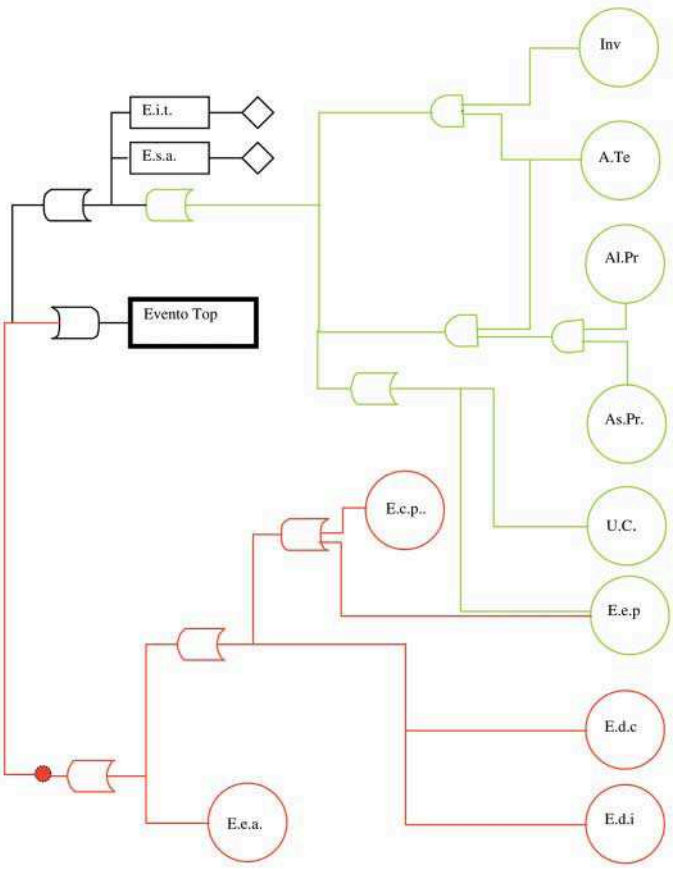


Grafo 6

Per completezza facciamo alcune considerazioni in merito ai danneggiamenti dovuti agli urti meccanici.
Se le procedure di installazione e la I.Q. dell'impianto di ventilazione sono state correttamente eseguite,non sono da prendere in considerazione i danneggiamenti causati da materiali lanciati sui filtri dal sistema di ventilazione stesso. Rimangono, quindi, le cause che insorgono all'interno della camera bianca quali gli eventi catastrofici, urti causali (U.C) (rottura di una macchina di processo con "lancio" di mezzi contundenti, "esplosione" di un flacone durante il riempimento, errore procedurale grave dell'operatore, errore procedurale grave della squadra di pulizia ecc.) che sono, comunque, eventi a bassissima frequenza, e gli eventi riconducibili ad azioni sistematiche causate dalla non corrispondenza ergonomica delle procedure di produzione con il diagramma di produzione (E.e.p.) già in precedenza introdotte. Tenendo comunque in conto che l'invecchiamento è a tutti gli effetti una causa prima, il diagramma risulta modificato come riportato nel grafo 6.
Occorre fare una osservazione dettata dall'esperienza. Nelle camere bianche in classe ISO7 ed ISO8 l'intasamento dei filtri finali è estremamente lento. In media occorrono più di 3-4 anni per pervenire a perdite di carico di 400-450 Pa. contro perdite di carico massime sopportabili dai filtri terminali superiori ai 1000 Pa. Ciò comporta una netta prevalenza dei guasti causati dall'invecchiamento rispetto a quelli causabili dallo sforzo meccanico. Nella pratica, anche per problematiche legate al rumore ed ai consumi energetici, è prassi comune sostituire i filtri terminali prima del quarto anno di funzionamento. Ciò comporta la non necessità di disporre di ventilatori di notevole potenza in grado di scaricare sui filtri terminali salti di pressione paragonabili a quelli di rottura. Se il dimensionamento del sistema di ventilazione è stato eseguito tenendo in conto questo dato di fatto vengono eliminati i danneggiamenti dovuti alla alta pressione. La sequenza E.d.H. si modifica come sotto riportato (grafo 6a). Come si vede ciò, indipendentemente dalle considerazioni che verranno svolte, comporta comunque una buona semplificazione e mostra l'inutilità del controllo della caduta di pressione, e relativa procedura, sui filtri HEPA terminali in quanto l'evento primo da cui dipendeva è eliminato.



Grafo 6a



Grafo 7

Possiamo in modo analogo rappresentare l'insieme delle sequenze connesse con errori procedurali o omissioni di controllo come da Grafo 7.

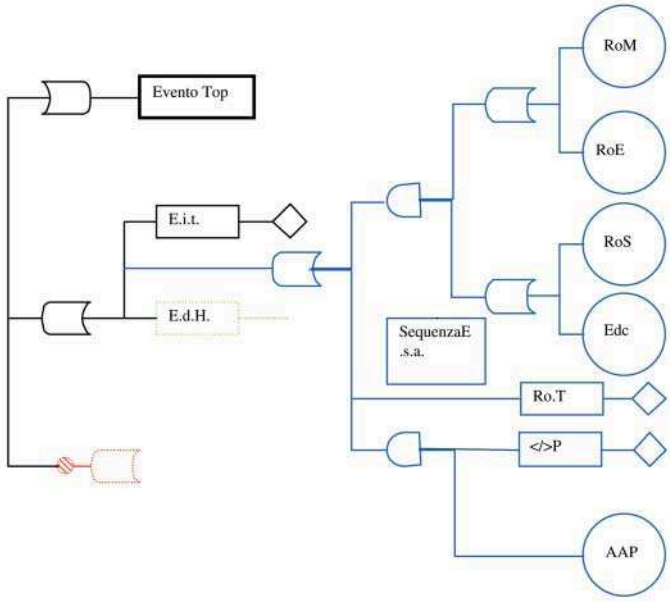
Eventi connessi con sistemi ausiliari (interblocco bussola) (E.s.a.)

Analizziamo adesso le problematiche connesse con i guasti o il non corretto utilizzo dei sistemi ausiliari quali la bussola di uscita del prodotto (E.s.a.).
Normalmente tali sistemi sono così concepiti:
- bussola ventilata con pressione intermedia tra i locali che pone in comunicazione
- interblocco temporizzato tra le due porte
- segnalazioni ottiche sullo stato delle porte

Per quanto riguarda la ventilazione possiamo avere due soluzioni: a) la bussola può essere ventilata indipendentemente; b) la bussola è ventilata attraverso un sistema comune anche ai locali connessi.
Dal punto di vista dei malfunzionamenti non è rilevante né il "valore" di portata immessa né il "valore" della pressione relativa. Essi influenzano la classe di contaminazione, il recovery time ed il grado di contenimento ma se sono stati considerati idonei per l'applicazione in oggetto e certificati, non possono essere considerati fonte di eventi dannosi.

Sono, invece, eventi dannosi le variazioni dei valori di tali parametri. Se l'impianto di ventilazione è unico dovremo sviluppare questi eventi nella catena incidentale connessa con l'impianto di trattamento aria (*E.i.t.*), altrimenti nella catena (*E.s.a*).
In relazione all'Evento Top i guasti che hanno importanza sono:
- apertura porta interna prima che sia trascorso il Recovery time dalla chiusura della porta esterna;
- aumento della pressione nella bussola a valori superiori di quella del locale riempimento;
- diminuzione della pressione nella bussola al di sotto di quella del corridoio "D".

Nel primo caso se l'Operatore 1 apre la porta interna prima che sia trascorso un recovery time da che è stata chiusa la porta esterna, il locale riempimento verrà in contatto diretto con un'area più contaminata. Questo evento può verificarsi sia per una rottura meccanica (*Ro.M.*) che elettrica (*Ro.E.*) delle serrature accompagnata da un contemporaneo guasto alle spie di segnalazione (*Ro.S.*). Altra possibile causa potrebbe essere un guasto al temporizzatore (*Ro.T*).
Nel secondo caso, (>P), quando l'Operatore 2, uscendo, chiude la porta esterna, l'aria interna alla bussola, più contaminata, entrerà nel locale di riempimento, per via delle infiltrazioni, per tutta la durata del recovery time della bussola. Nel caso di suo ingresso a tale periodo occorrerà aggiungere il tempo della sua permanenza all'interno.
Nel terzo caso,(<P) le infiltrazioni di aria più contaminata dal corridoio possono fare sì che le condizioni di pulizia idonee per l'apertura della porta interna non vengano mai raggiunte.
Nel Grafo 8 sono riportate le considerazioni sopra espresse.



Grafo 8

Gli eventi rottura temporizzatore e alta/bassa pressione sono eventi da sviluppare ulteriormente. Se la bussola è dotata di sistema di allarme per bassa/alta pressione, l'osservanza di questo allarme evita le conseguenze sull'evento Top, anche se il suo intervento impedisce l'uso in sicurezza della bussola medesima. Introduciamo quindi la causa prima "assenza allarme pressione nella bussola" AAP.
Si sono introdotti, tra le cause prime, gli eventi connessi con il difetto di controllo d'applicazione delle procedure (*E.d.c.*), in quanto, data per scontata l'esistenza di idonea procedura, l'inosservanza delle spie di segnalazione può solo essere causata da un difetto nel controllo dell'applicazione delle procedure.

Summary *After examinating in the firts part how a fault tree is designed, in this second part we analyze the graphical representation of undesired evets caused by intermediated events*

Per ulteriori informazioni segnare sull'apposito tagliando il n. 1

Analisi del Rischio: un esempio applicativo al settore farmaceutico della Fault Tree Analysis

In questa ultima parte vengono sviluppate le sequenze relative ai malfunzionamenti degli impianti di ventilazione e trattamento aria. L'esempio è infine completato dalla metodologia di valutazione del rischio

Parole chiave: Criteri impiantistici • Portata del sistema • Controllo della temperatura • Controllo dell'umidità • Valutazione del rischio

L. Sabatini
Lesatec Srl – Opera - Milano

Eventi connessi con l'impianto di trattamento aria (E.i.t.)

Rimane da esaminare l'evento intermedio (***E.i.t.***) dipendente dai guasti o malfunzionamenti degli impianti di ventilazione e trattamento aria. Le catene incidentali che determinano questo evento dipendono fortemente da come l'impianto è stato progettato, realizzato e qualificato. Per procedere nella sua analisi occorre pertanto descriverlo con sufficiente precisione.
Supponiamo che esso sia stato progettato e realizzato tenendo in conto i seguenti criteri:

- *Distribuzione dell'aria negli ambienti del reparto effettuata per mezzo di filtri HEPA terminali*;
- *Equi portata specifica dei filtri terminali*: questo significa che in tutti i filtri terminali la velocità di attraversamento del mezzo filtrante è la stessa, ovvero che la portata di aria per unità di superficie filtrante è costante;
- *Costanza delle caratteristiche tecniche dei media filtranti dei filtri terminali*: ossia, le caratteristiche tecniche dei media filtranti, quali efficienza di filtrazione, diametro di massima penetrazione, perdita di carico in funzione della velocità di attraversamento e sua variazione in funzione dell'omogeneo intasamento sono le stesse;
- *Costanza delle caratteristiche geometriche dei filtri terminali*: ovvero, le pieghettature del mezzo filtrante hanno tutte la stessa profondità e spaziatura. Con il soddisfacimento contemporaneo dei precedenti requisiti, ciò si traduce nella uguaglianza delle perdite di carico di tutti i filtri del reparto a parità di velocità frontale di emissione;
- *Equi intasamento del sistema filtrante finale*: supponiamo che il sistema di ventilazione sia dotato dei tre classici sistemi di filtrazione. Il primo di bassa efficienza (G4), il secondo costituito da filtri ad alta efficienza (F8) ed il terzo sistema, sul quale transita ovviamente tutta l'aria, costituito dagli HEPA terminali di efficienza H14 con ventilatore di mandata posto tra sistema secondario e terminale (vedi Fig. 3). Questo tipo di schema di ventilazione garantisce che su tutti i filtri terminali la contaminazione media dell'aria in arrivo sia la stessa in quanto tutta l'aria in circolo subisce lo stesso tipo di prefiltrazione e passa per il medesimo ventilatore. Questo tipo di geometria, unito al soddisfacimento delle caratteristiche precedenti, fa sì che le variazioni di perdita di carico dei filtri con il proseguire dell'intasamento siano uguali per tutti;
- *Condizione di stabilità aerodinamica*: è noto che i percorsi aerodinamici all'interno delle clean room a flusso misto, dipendono, una volta fissata la geometria dei dispositivi di immissione e ripresa, dalle velocità di immissione e dalla differenza tra la temperatura di immissione e la temperatura media ambientale. Con il diminuire di tale differenza di temperatura e della velocità di immissione può generarsi il fenomeno della inversione aerodinamica. Nel caso specifico supponiamo che la velocità di immissione, che è costante per tutti i filtri, e quindi le portate siano state definite in modo da garantire il funzionamento stabile in tutte le condizioni;
- *Criteri di determinazione della portata di aria immessa*: la portata minima da immettere in ogni ambiente è definita prioritariamente per garantire le classi di contaminazione previste in condizioni operative e l'alimentazione dei flussi unidirezionali a protezione delle zone critiche. Tale valore di portata normalmente è superiore, a parità di grado di sottoraffredda-

mento, a quella necessaria per il mantenimento delle condizioni termiche medie. Occorre però verificare che tale portata renda accettabili le variazioni spaziali dei parametri termoigrometrici, rispetto ai valori medi, in funzione dei carichi per rendere trascurabile il diverso impatto della sudorazione degli operatori;

- ***Invarianza del sistema di ventilazione***: questo significa che essendo i parametri fondamentali ambientali (temperatura, classe di contaminazione, recovery time) garantiti dalle portate di aria immessa negli ambienti, che a sua volta dipendono dalle perdite di carico di tutto il circuito, il sistema di distribuzione dell'aria è progettato per rimanere meccanicamente invariante. Ovvero che una volta effettuata in fase di avvio la ripartizione delle portate e dei gradienti di pressione con le serrande manuali all'uopo predisposte, esse rimangono fisse durante la vita dell'impianto. Unica eccezione l'organo di regolazione della potenza del ventilatore che deve sopperire all'incremento delle perdite di carico del sistema filtrante al fine di mantenere costante la portata di aria in ciclo.

Con il tipo di presupposti sopra riportati abbiamo che nei tratti di circuito compresi tra i filtri terminali, e quindi gli ambienti, e la zona del condizionatore a monte dei filtri G4, le pressioni rimangono sempre costanti se la portata rimane costante. Nel tratto compreso tra il valle dei filtri G4 ed il monte dei filtri H14 invece le pressioni dovranno variare per mantenere costante la portata per via dell'intasamento progressivo. Ogni variazione di portata si ripercuoterà in modo quadratico, ma con stessa legge parabolica, sulle pressioni del tratto 1 del circuito. Ciò garantirà comunque il mantenimento di differenze di pressione relative tra i vari tratti del circuito, ivi comprese le differenze di pressione ambientali. Tali differenze aumenteranno o diminuiranno con l'aumentare o il diminuire della portata annullandosi solo con l'annullamento della medesima senza mai invertirsi.

Appare evidente che il soddisfacimento dei criteri enunciati implica che un parametro da tenere sicuramente sotto controllo e la cui costanza è da garantire attraverso una idonea gestione è la portata del sistema. Esso può essere considerato, per il tipo di impianto prospettato, un vero e proprio parametro critico di controllo. La sua costanza, ripetiamo, garantisce:

a) mantenimento delle classi di contaminazione prefissate;
b) mantenimento, a porte chiuse, delle pressioni ambiente e, quindi, del contenimento per pressione previsto;
c) mantenimento, con idonea posizione geometrica dei filtri terminali, della distribuzione delle temperature previste negli ambienti;
d) costanza del recovery time.

…un parametro da tenere sicuramente sotto controllo e la cui costanza è da garantire attraverso una idonea gestione è la portata del sistema…

Altri parametri conseguenti da misurare e gestire sono le temperature e le umidità per il loro impatto sul benessere e la sudorazione degli operatori.

Supponiamo che nel nostro caso il controllo delle condizioni termoigrometriche sia effettuato per mezzo di una batteria centralizzata di deumidificazione e raffreddamento posta nella macchina di trattamento aria, da batterie di zona di post riscaldamento ed un umidificatore anche esso centralizzato. Le variabili misurate nel caso specifico risultano:

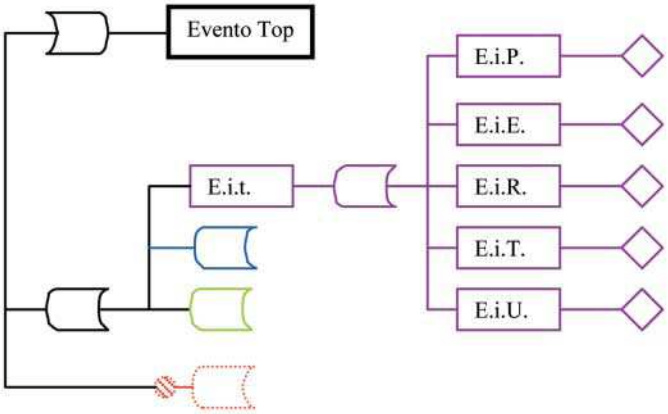
- temperature ed umidità medie dell'aria ricircolata al condizionatore per mezzo di trasmettitori inseriti nel canale di ripresa. Tali valori serviranno per il controllo della batteria e dell'umidificatore centralizzato;
- temperatura degli ambienti pilota delle varie zone termiche per mezzo di trasmettitori posti nelle canalizzazioni di ripresa da tali ambienti. Tali valori serviranno per il controllo delle batterie di post riscaldamento di zona.

Il soddisfacimento dei criteri impiantistici e delle condizioni di benessere impone però alcuni ulteriori vincoli che è bene evidenziare. Uno di questi è il grado di sottoraffreddamento massimo che può avere l'aria immessa. Data la tipologia della distribuzione non è salutare per gli operatori che esso superi i 4 °C quando le velocità di immissione sono quelle tipiche previste dalle pratiche di buona fabbricazione dei farmaci (0,45 m/s). Altro vincolo è rappresentato dalla necessità di garantire la corretta ossigenazione degli ambienti imponendo un sufficiente tasso di rinnovo dell'aria in circolo.

Occorrerà perciò dotare l'impianto di idonei sistemi di presa aria esterna ed espulsione che possano supplire alla bisogna e che, contemporaneamente, non alterino l'invarianza del circuito di ventilazione. Nel nostro caso ciò è stato ottenuto per mezzo di un espulsore che preleva parte dell'aria ricircolata al condizionatore e con l'immissione di aria esterna direttamente alla sezione di presa del condizionatore stesso.

Con riferimento al nostro Evento critico le sequenze incidentali pertinenti possono essere ridotte alle seguenti:

- malfunzionamento del sistema di controllo della portata totale di aria in ciclo con riduzione della medesima (***E.i.P***);
- depressurizzazione degli ambienti causata da un aumento della portata di aria di espulsione (***E.i.E***);
- depressurizzazione degli ambienti causata da una rottura di un componente del sistema di distribuzione dell'aria (***E.i.R***);
- malfunzionamento del sistema di controllo della temperatura (***E.i.T***);
- malfunzionamento del sistema di controllo della umidità (***E.i.U***).



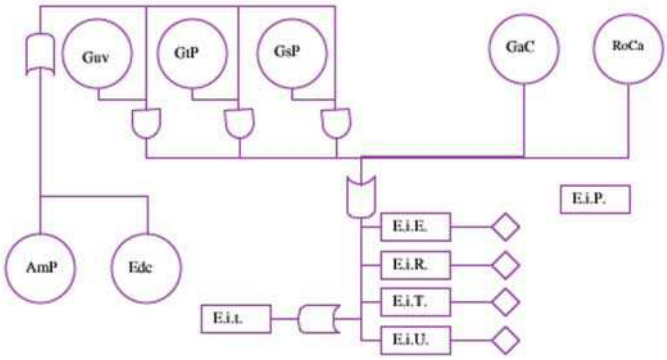
Grafo 9

Possiamo a questo punto riportare in forma grafica i nuovi eventi intermedi individuati per la sequenza ***E.i.t.*** (vedi grafo 9) ed iniziare le analisi per le sequenze individuate.
Occorre però fare una importante precisazione. Parlando di apparati meccanici od elettronici possiamo suddividere tali guasti in due categorie principali: quelli riducibili a livelli accettabili o eliminabili per mezzo di una manutenzione ben programmata e quelli di natura prettamente stocastica connessa con l'affidabilità della componentistica utilizzata. Al primo tipo sono chiaramente riconducibili i malfunzionamenti delle trasmissioni, dei cuscinetti, ecc. mentre al secondo tipo quelli tipici dei controller, PLC o trasmettitori di segnale.
Oltre a questi occorre ipotizzare eventi catastrofici connessi con eventi non prevedibili quali tranciature di cavi, cadute di gravi su componenti, ecc.

Malfunzionamento del sistema di controllo della portata totale di aria in ciclo con riduzione della medesima (*E.i.P*)

Con le precisazioni sopra fatte, per l'evento intermedio ***E.i.P*** possiamo suddividere nel seguente modo i possibili malfunzionamenti:
- Guasti dovuti a carente o assente manutenzione:
  a) guasto alla trasmissione del ventilatore (***GuV***);
  b) guasto per sporcamento o ossidazione del sensore/trasduttore di portata (***GtP***);
  c) guasto per "baco" al software del PLC (***GsP***)
- Guasti dovuti alla affidabilità dei componenti (***GaC***) quali:
  a) guasti elettronici dei controller/PLC;
  b) guasti elettronici dei trasmettitori di segnale;
  c) guasti elettrici dei motori;
  d) guasti degli inverter
- Guasti dovuti ad eventi catastrofici (***Ro.Ca***) quali:
  a) tranciature cavi trasmissione dati o potenza;
  b) rotture per eventi catastrofici dei componenti

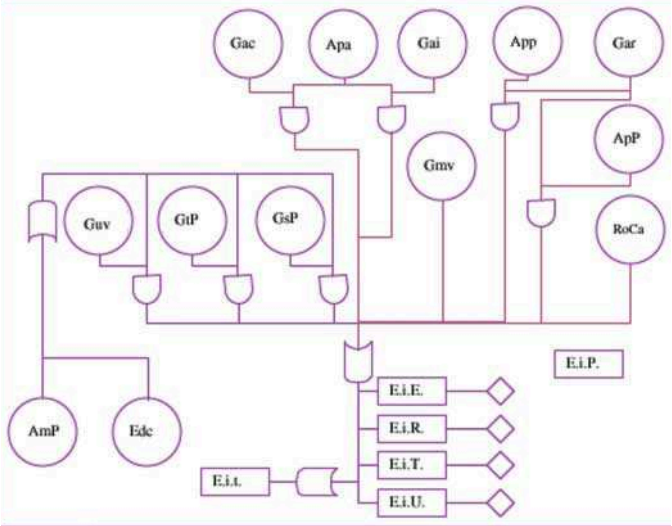
La lista dei guasti proposta, sicuramente non esaustiva, è prettamente dipendente dalla tipologia di impianto prospettata e, quindi, non generalmente valida.



Grafo 10

Data la tipologia degli eventi considerati e la scarsa influenza della manutenzione programmata su alcuni di essi è opportuno prevedere azioni parallele sia per prevenire, attraverso le ridondanze dei componenti meno affidabili, che per mitigare o contenere le conseguenze delle sequenze incidentali a più bassa probabilità di accadimento.
Nel grafo 10 sono stati riportati gli eventi primi già individuati con l'aggiunta della assenza della manutenzione preventiva (***AmP***). Si è provveduto anche ad inserire l'evento Edc in quanto se non vi è controllo dell'applicazione della procedura di manutenzione non c'è la sicurezza che venga effettuata.
Il diagramma ottenuto si presta ad alcune ottimizzazioni che, limitatamente al nostro Evento Top, possono permettere, per un non trascurabile numero di guasti causati dall'affidabilità (***GaC***), di attenuarne gli effetti senza ricorrere estesamente alle ridondanze di impianto per i componenti di notevole costo e buona affidabilità.
Diremo subito che con quanto proporremo non è possibile coprire i guasti stocastici dovuti al motore del ventilatore (***Gmv***).
Nell'ipotesi che il ventilatore di mandata sia stato dimensionato conformemente a quanto sopra descritto, molti dei guasti ***GaC*** che comportano una diminuzione di portata, con l'esclusione della rottura del motore del ventilatore, potrebbero essere mitigati nelle loro conseguenze imponendo che le variabili controllate vadano al loro valore massimo attraverso il distacco dell'organo controllato. Per esempio al guasto per sovra assorbimento o eccessiva dispersione dell'inverter (***Gai***) potrebbe corrispondere l'immediato passaggio all'alimentazione diretta del motore. Analogamente all'azzeramento del segnale di portata (***Gac***), o sua diminuzione al disotto di una soglia prefissata, un relè potrebbe alimentare l'organo regolante con un segnale prossimo al valore massimo. Se in fase di qualificazione della installazione è stato provato che il passaggio dalle condizioni normali a queste condizioni di guasto "attenuato" non comporta un superamento dei limiti per l'evento critico in questione, allora gli operatori potrebbero avere il tempo di esaurire il prodotto in linea senza la necessità di eli-

minarlo. Chiaramente il ciclo di lavoro dovrà essere interrotto per permettere la riparazione del guasto. Altri tipi di guasto potrebbero essere quelli che comportano un blocco delle capacità di regolazione (*Gar*). Questi ultimi, comunque causati, possono non essere immediatamente percepiti. È quindi necessario che opportune segnalazioni indichino il degrado del sistema di controllo. Per fare questo occorre che le variabili controllate, in questo caso la portata, vengano misurate anche da un sistema ausiliario ad elevata affidabilità di facile o immediata manutenzione (ridondanza). Nel caso della portata questo potrebbe essere un manometro a liquido o meccanico collegato ad un tubo di venturi o ad una flangia tarata.
Impostando su tale manometro, in parallelo con il sistema di controllo automatico, il valore della portata nominale e l'intervallo accettabile in diminuzione (livelli di allerta/azione), il variare del valore misurato entro detto intervallo potrebbe essere utilizzato come indicatore delle condizioni di guasto e permettere di esaurire in sicurezza il prodotto in linea. Possiamo quindi introdurre nel nostro grafo le due condizioni sopra dette, ovvero l'evento "Assenza progettazione autosicura" (*Apa*) e "Assenza preallarme portata" (*App*). Nel nostro schema di condizionamento la pressione dipende essenzialmente dalla portata in quanto la quantità di aria esterna aumenta/diminuisce con l'aumentare/diminuire della portata in ciclo mentre l'espulsione tende a rimane costante se i relativi sistemi sono ben funzionanti. Oltre a ciò le pressioni ambientali dipendono dal quadrato della portata e così pure le variazioni. Pertanto la diminuzione di pressione può essere evidenziata in tempi assai più rapidi della diminuzione della portata. Per tener conto di ciò introduciamo l'evento "Assenza preallarme pressione" (*ApP*).
Nel grafo 11 queste considerazioni sono state introdotte previa la suddivisione degli eventi *GaC* nelle tre categorie ipotizzate che, nella pratica, ne esauriscono le ipotesi di guasto con l'aggiunta del guasto al motore.



Grafo 11

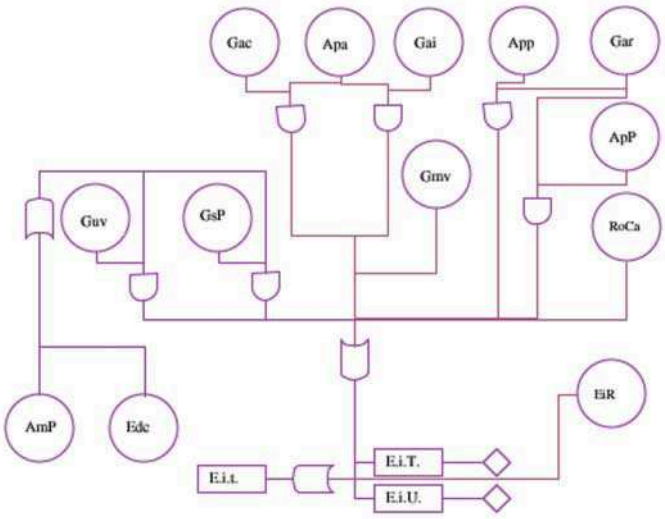
Possiamo fare una ulteriore considerazione in merito alla causa prima *GtP*, ovvero il non corretto funzionamento del sensore a causa della carente manutenzione. È evidente che le conseguenze di questo evento vengono mitigate dalla presenza delle cause prime *Apa*, *ApP* e *App*. Pertanto tale evento può non avere influenza sulla contaminazione del prodotto in lavorazione anche se riduce l'affidabilità produttiva del sistema. Avendo finalizzato l'analisi non alla produttività con garanzia di qualità ma alla valutazione del rischio connesso con il superamento occasionale dei limiti di contaminazione particellare nel punto di controllo della Classe B, riteniamo che per questo fine esso possa essere eliminato.

Depressurizzazione degli ambienti causata da un aumento della portata di aria di espulsione (E.i.E)

Nella definizione prima data lo abbiamo limitato alle ipotesi di guasto che determinano un aumento della portata di espulsione in quanto tale aumento comporta una diminuzione di pressione negli ambienti e quindi un aumento delle infiltrazioni con ricaduta nell'evento critico considerato. Viceversa una diminuzione della portata di espulsione causa un aumento della pressione negli ambienti che non ha effetto pratico ai nostri fini anche se ciò può comportare inconvenienti ai controsoffitti ed agli infissi.
Nel nostro esempio la portata di espulsione è controllata per mezzo di una serranda dotata di servomotore con posizionamento manuale. Tale serranda è a taratura fissa quindi tale servomotore può essere eliminato inserendo una serranda con blocco meccanico da tarare e fissare in sede di collaudo. Per l'esclusione ad impianto fermo può essere introdotta una ulteriore serranda dotata di servomotore ON/OFF con ritorno a molla.
Con questa aggiunta di "progettazione auto-sicura" l'evento E.i.E cessa di avere importanza in relazione al nostro Evento Critico e può essere tolto dal grafo.

Depressurizzazione degli ambienti causata da una rottura di un componente del sistema di distribuzione dell'aria (E.i.R)

L'evento intermedio E.i.R, può essere considerato a tutti gli effetti una causa prima. Non è inoltre necessario implementare i sistemi di controllo in quanto la causa prima *ApP* introdotta nella sequenza E.i.P rileva anche una depressurizzazione relativa a questo evento. È da notare che una rottura di un elemento della distribuzione dell'aria, per esempio un collegamento ad un filtro terminale, comporta oltre che la depressurizzazione degli ambienti anche una diminuzione di portata immessa.



Grafo 12

Se la rottura avviene dopo il sensore di portata, essa con le usuali regolazioni automatiche, può non essere rilevata come guasto in quanto tale ma rilevata sicuramente come diminuzione di pressione ambientale. Se le rotture sono piccole gli effetti saranno diversi da ambiente ad ambiente con maggior incidenza per quello direttamente interessato al guasto. Occorre quindi che i sensori di allarme connessi alla causa *ApP* siano posizionati in tutti gli ambienti del reparto o, per lo meno, in quelli principali. Quanto sopra detto è espresso nel grafo 12.

Malfunzionamento del sistema di controllo della temperatura (E.i.T) e malfunzionamento del sistema di controllo della umidità (E.i.U)

Gli eventi intermedi E.i.T ed E.i.U possono essere analizzati in modo simile a quanto fatto per l'evento E.i.P solo che in questo caso le grandezze da controllare sono rappresentate dalle portate di acqua calda e fredda alle batterie e dalla portata di vapore dell'umidificatore. Per semplicità ci limiteremo al controllo dell'afflusso dell'acqua fredda alla batteria centralizzata in regime estivo per i guasti che possono influenzare il nostro Evento Top ovvero che conducono ad un aumento di temperatura ed umidità tale da incidere sulla sudorazione degli operatori. Non entreremo nel merito degli eventi che incidono sulla affidabilità della fornitura di acqua fredda.
Iniziamo con l'analisi del sistema. In fig. 3 è mostrato che solo parte dell'aria ricircolata con la totalità dell'aria esterna di rinnovo transita sulla batteria di raffreddamento mentre una sua aliquota la cortocircuita e viene ad essa mescolata dopo il trattamento formando così la miscela che verrà inviata agli ambienti. La quantità di aria cortocircuitata deve essere determinata affinché la temperatura e l'umidità specifica della miscela siano tali

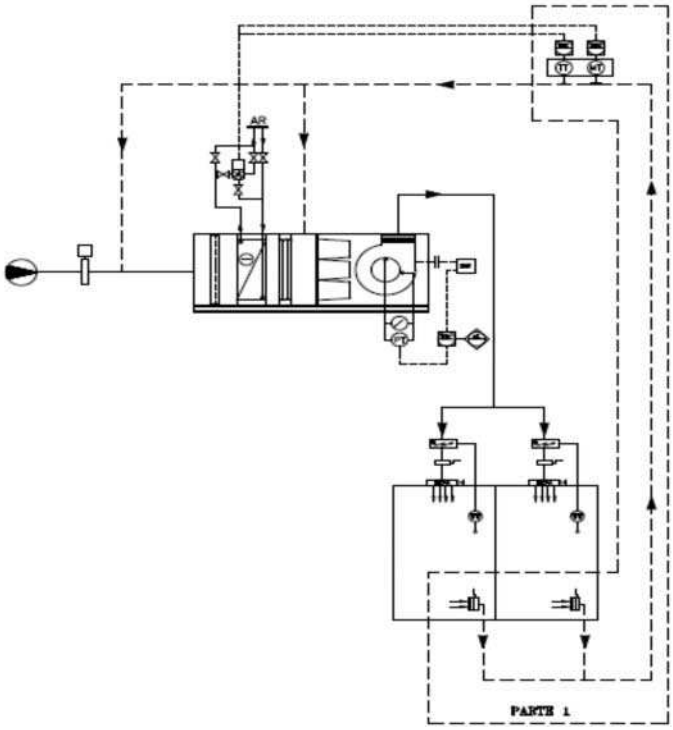
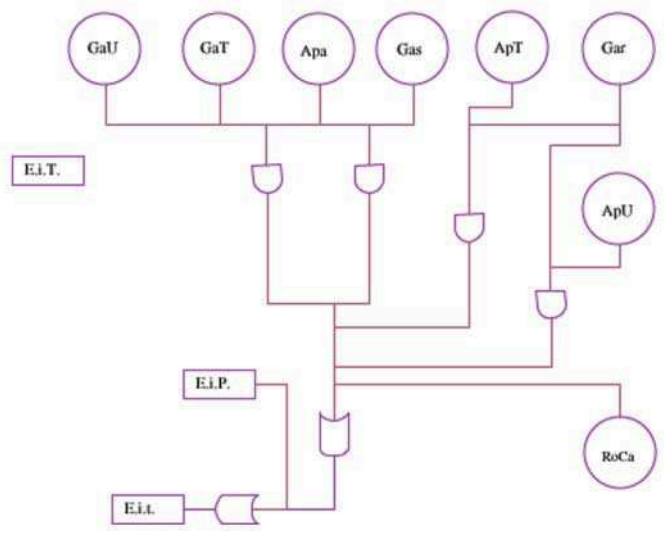


Figura 3 Schema funzionale indicativo

da garantire le condizioni interne previste, entro intervelli accettabili per la sudorazione, nell'ipotesi di massimo carico di progetto senza l'intervento delle batterie di post riscaldamento. Questo tipo di dimensionamento ha due motivazioni:
- limitazione nell'uso del post riscaldamento estivo (risparmio energetico);
- possibilità di mantenimento delle condizioni termoigrometriche entro limiti previsti in caso di rottura del sistema di regolazione della portata di acqua fredda in condizioni operative

Affinché la seconda motivazione diventi effettiva occorre però soddisfare alcune ulteriori condizioni.
Supponiamo che il sistema di rilevazione delle variabili controllate sia, diversamente da quanto mostrato in fig. 3, costituito da una semplice trasduttore di temperatura che misuri la temperatura dell'aria in uscita dalla batteria di raffreddamento e deumidificazione e che il sistema di regolazione sia programmato per mantenere tale temperatura costante e pari al valore di condensazione dell'aria corrispondente alla umidità specifica desiderata negli ambienti. Supponiamo inoltre che la batteria sia dimensionata in modo tale che la temperatura di uscita dell'aria con il massimo afflusso di acqua fredda sia pari, nelle condizioni di massimo carico, alla temperatura di condensazione dell'aria. Allora se il servomotore che regola l'adduzione di acqua fredda è del tipo normalmente aperto con molla di ritorno e la logica di regolazione è tale che in caso di assenza di segnale (*GaT*) viene tolta l'alimentazione al servomotore la seconda motiva-

zione diviene effettiva anche nel caso di rottura del servomotore stesso (*Gas*) tranne nel caso in cui, vuoi per rottura o assenza di manutenzione, subentrano delle condizioni di blocco della regolazione (*Gar*). Il soddisfacimento delle condizioni sopra esposte rende il progetto del sistema "auto-sicuro" per le condizioni di guasto ipotizzate. Possiamo, quindi introdurre anche per questa sequenza la causa *Apa*. Per attenuare il guasto *Gar* possiamo anche in questo caso introdurre, in analogia al *ApP* la causa "Assenza preallarme Temperatura".
Il sistema di regolazione sopra descritto, consistente nel controllo a punto fisso della temperatura di condensazione, benché estremamente semplice e soddisfacente può essere però migliorato dal punto di vista dei consumi energetici. Difatti esso raffredda l'aria trattata indipendentemente dalle caratteristiche dell'aria in arrivo sulla batteria. Ci possono essere situazioni in cui l'aria esterna ha basso contenuto di umidità (stagioni intermedie, inverno) con bassi carichi endogeni (condizioni di riposo). Per queste condizioni può non essere necessario raffreddare l'aria trattata fino alla temperatura di condensazione prevista. In vista di ciò lo schema che si preferisce seguire è quello mostrato nella figura 3, ovvero con due trasduttori distinti di temperatura ed umidità che rilevano le condizioni medie di ripresa. In questo caso il sistema di regolazione dovrà regolare l'apertura della valvola di adduzione dell'acqua fredda in funzione del segnale maggiore inviato dai due trasduttori. Ovviamente sarà necessario inserire, in analogia alla *ApT*, anche la causa "Assenza preallarme Umidità". Le considerazioni sopra svolte sono sintetizzate nel grafo 13 dal quale l'evento intermedio E.i.U è stato eliminato perché nelle condizioni estive e per l'impianto ipotizzato è compreso nell'evento E.i.T.
Con il grafo 13 consideriamo esaurito l'albero dei guasti relativo all'evento considerato anche se l'analisi non è stata sviluppata in modo esaustivo per tutti le cause possibili.



Grafo 13

Valutazione del rischio

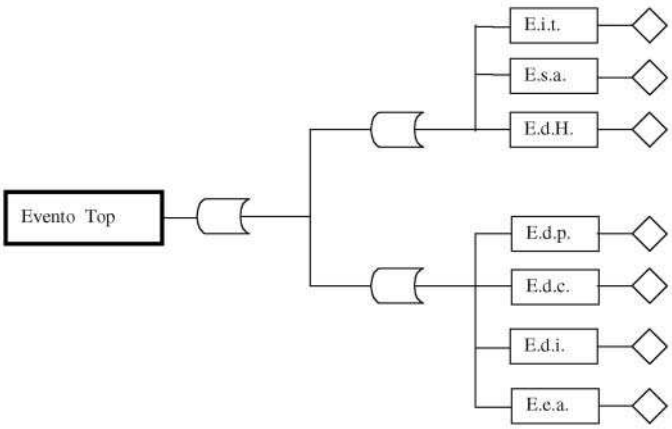
Nasce a questo punto il problema della valutazione del rischio relativo al nostro Evento TOP. Possiamo finalizzare l'analisi a vari tipi di rischio, ovvero individuare differenti tipi di danni con le relative entità:

Rischio connesso alla perdita di produzione

Se accade l'evento TOP la produzione va sospesa per il periodo di tempo necessario alla riparazione del guasto ed alla riqualificazione dell'ambiente. Non necessariamente dovrà essere rieseguita una riqualificazione completa, lo stesso albero dei guasti può indicare i punti sui quali convergere gli sforzi. In questo caso il danno economico (Severità) sarà rappresentato, intuitivamente, dalla quantità di prodotto non realizzato nel periodo di fermo per il suo valore economico, anche se tale severità potrebbe essere valutata, più approfonditamente, in base al costo della produzione e della riqualificazione.

Rischio connesso alla accettazione qualitativa del prodotto o di conformità

La deviazione del parametro incrementa la possibilità di contaminazione delle fiale che sono aperte e posizionate al di fuori del deposito sterile o comunque fuori dai flussi unidirezionali. Se le condizioni operative descritte all'inizio vengono rispettate questa evenienza non dovrebbe mai verificarsi. Unica conseguenza dell'evento TOP è, quindi, la maggior contaminazione dell'operatore. Questo induce ad interrompere la produzione ma non comporta nessun rischio per le fiale già chiuse e, se l'operatore non deve fare operazioni sotto flusso, possono essere finite di riempire anche le fiale in linea.
Se le procedure operative sono corrette l'unico rischio da valutare è quello connesso con la perdita di produttività. Precedentemente abbiamo indicato come valutare la severità dell'evento, per quanto riguarda la sua probabilità essa deve essere calcolata in funzione dell'albero dei guasti. Nel caso di eventi *indipendenti* legati da porte "OR", la probabilità risultante è pari alla somma delle probabilità dei singoli eventi. Nel caso di eventi legati da porte "AND" la probabilità è pari al prodotto delle probabilità. Con queste due semplici regole si possono valutare le probabilità delle varie sequenze di eventi che compongono l'albero.
Nel grafo 1 (pubblicato sul n. 1/2008 di Ascca News e qui riportato) l'evento critico dipendeva da una serie di eventi intermedi indipendenti legati da una porta logica "OR", quindi la sua probabilità è pari alla somma delle probabilità del verificarsi di ogni singolo evento. Occorre però fare una precisazione. Per la costruzione dell'albero noi abbiamo sempre considerato gli eventi o come veri (1) o come falsi (0) per permetterci di elaborare la concatenazione logica dei medesimi. Nel



Grafo 1

momento in cui si passa al calcolo della probabilità è necessario sostituire a detti valori i valori delle probabilità, o le frequenze. Per esempio nel grafo 13 l'evento ***ApT***, assenza preallarme temperatura, se presente assume il valore logico "0" ed annulla la sequenza connessa all'evento ***Gar***. Nel calcolo probabilistico esso interverrà solo se funziona correttamente, ovvero il valore "0" andrà sostituito con la sua probabilità di guasto. Ovviamente anche agli eventi primi ipotizzati occorrerà sostituire il valore "1" con i valori delle effettive probabilità o una loro stima.

Conclusioni

Possiamo aggiungere che la metodologia FTA è una metodologia completa che permette di valutare gli apporti al rischio, connesso con l'evento critico, di tutte le cause prime ipotizzabili siano esse legate ad errori umani, omissioni di controllo, non adeguatezza delle procedure operative o alle apparecchiature. Essa inoltre permette di definire quale delle tre azioni tipiche di: ***prevenzione, attenuazione, protezione***, è da porre in essere per rendere il rischio accettabile. Nell'esempio illustrato abbiamo cercato di mostrare ciò evidenziando anche l'impatto che ha sul rischio il progetto del sistema. L'unico limite della metodologia è rappresentato dal fatto che una analisi accurata è possibile solo se si conosce in modo approfondito il sistema in analisi.

Summary *In this part we describe the step about HVAC malfunctioning and consequent risk analysis.*

Per ulteriori informazioni segnare sull'apposito tagliando il n. 1