MONOGRAFIES D'ENGINYERIA, 1

AFFIDABILITÁ E SICUREZZA NELL' INDUSTRIA CHIMICA

per Norberto Piccinini
del Politecnico di Torino

SECCIÓ D'ENGINYERIA

SOCIETAT CATALANA DE CIÈNCIES
FÍSIQUES, QUÍMIQUES I MATEMÀTIQUES
Filial de l'INSTITUT D'ESTUDIS CATALANS

AFFIDABILITÀ E SICUREZZA NELL'INDUSTRIA CHIMICA

MONOGRAFIES D'ENGINYERIA, 1

AFFIDABILITÁ E SICUREZZA NELL' INDUSTRIA CHIMICA

per **Norberto Piccinini**
del Politecnico di Torino

SECCIÓ D'ENGINYERIA

SOCIETAT CATALANA DE CIÈNCIES
FÍSIQUES, QUÍMIQUES I MATEMÀTIQUES
Filial de l'INSTITUT D'ESTUDIS CATALANS

LA COMISSIÓ INTERDEPARTAMENTAL DE RECERCA I INNOVACIÓ
TECNOLÒGICA (CIRIT) DE LA GENERALITAT DE CATALUNYA
HA CONTRIBUÏT GENEROSAMENT
A L'EDICIÓ D'AQUEST VOLUM

ISBN: 84-7283-063-2
Dipòsit legal: B. 9.080-1985
Coberta i sobrecoberta: Maria Casassas
Foto: G. Comicci

PRESENTACIÓ

Els diversos accidents ocorreguts darrerament arreu del món, entre ells el més recent i dramàtic de Bhopal, a l'India, han posat de manifest una vegada més el perill potencial que poden presentar la indústria química en general i determinades plantes en particular.

La manca d'informació o, a vegades, la informació poc mesurada que pateix el ciutadà, juntament amb el desconeixement del grau real de perill que presenten certes instal·lacions, sovint situades a prop o fins i tot dins de nuclis urbans, aconsegueixen de crear un clima d'inquietud i de malfiança envers la indústria química.

Tot això podria semblar que comporta una forta contradicció amb el progrés científic i tecnològic entès com a millora de la condició humana, de l'entorn i del món en general, i amb la convicció que la salut, tant física com psíquica, dels individus i de la comunitat, és un valor primordial i inalienable.

És un fet que, malauradament, un cert nombre d'instal·lacions no compleixen les condicions de seguretat que haurien de tenir. Això pot ésser degut a un projecte ja originalment insatisfactori, a un mal manteniment, o a un canvi en les condicions d'explotació que ha convertit allò que un dia fou segur en perillós. D'aquesta manera augmenta la probabilitat que tinguin lloc accidents, tant pel que fa als convencionals, comuns a qualsevol activitat industrial, com als específics de la indústria química: explosions, fuites, etc.

Hi ha, doncs, dues necessitats cada cop més prioritàries: per l'un costat, el projecte d'instal·lacions segures, amb l'establiment del grau de seguretat corresponent; per l'altre, l'anàlisi de la seguretat –i, per tant, del grau de perill– de plantes ja existents.

És evident que això requereix una caracterització del *risc*, funció de les conseqüències perjudicials d'un esdeveniment indesitjat i de la probabilitat que aquest tingui lloc. La dificultat apareix, però, en tractar de determinar la probabilitat d'un esdeveniment, i també pel fet que el *risc zero* implica pràcticament la inactivitat, essent, doncs, necessari de fixar el límit acceptable de risc.

Han estat desenvolupades diverses tècniques i metodologies per a superar aquestes dificultats i per a sistematitzar l'anàlisi de la fiabilitat i de la seguretat en la indústria química. Mètodes utilitzats amb èxit en altres

camps –aviació, indústria nuclear– hi són actualment introduïts. Simultàniament, en els darrers anys, diversos països han pres mesures legislatives per a garantir una major seguretat en les denominades *plantes químiques perilloses*. L'interès per tota aquesta temàtica és cada dia més gran, essent motiu de congressos, seminaris i cursos en gairebé tots els països industrialitzats.

Aquesta inquietud ha començat a arribar al nostre país. És per això que la Secció d'Enginyeria de la Societat Catalana de Ciències Físiques, Químiques i Matemàtiques, amb el patrocini de la Comissió Interdepartamental de Recerca i Innovació Tecnològica de la Generalitat de Catalunya, ha organitzat el curs *Projecte i anàlisi de seguretat en plantes químiques perilloses*, impartit pel professor Norberto Piccinini, del Politècnico di Torino (Barcelona, març de 1985).

Pionera, doncs, en aquest camp, la Secció d'Enginyeria publica ara aquest llibre, que representa una contribució més per a la consecució d'una major seguretat en la indústria química.

Affidabilità e sicurezza nell'industria chimica enceta la nova sèrie MONOGRAFIES D'ENGINYERIA, que se suma a les altres publicacions de la nostra Societat. L'objectiu d'aquesta sèrie és la publicació, en català o, en determinats casos, en alguna altra llengua, de treballs monogràfics relacionats amb qualsevol de les branques de l'enginyeria l'interès i l'actualitat dels quals en facin aconsellable la difusió

Joaquim Casal i Fàbrega

Secretari d'Actes de la Secció d'Enginyeria de la SCCFQiM

PRESENTAZIONE

I vari incidenti occorsi ultimamente nel mondo, tra questi il più recente e drammatico di Bhopal, in India, hanno messo in evidenza ancora una volta il pericolo potenziale che possono presentare l'industria chimica in generale e determinati impianti in particolare.

La mancanza di informazione o, a volte, l'informazione poco equilibrata di cui soffre il cittadino, insieme all'ignoranza del grado reale di pericolo che presentano certi impianti, spesso situati vicino o addirittura all'interno dei nuclei urbani, contribuiscono a creare un clima di inquietudine e di diffidenza verso l'industria chimica.

Apparentemente ciò pottrebe comportare una forte contraddizione tra il progresso scientifico e tecnologico inteso come miglioramento della condizione umana, dell'ambiente e del mondo in generale, e tra la convinzione che la salute, tanto fisica come psichica, degli individui e della comunità, è un valore primordiale e inalienabile.

È un fatto che, disgraziatamente, un certo numero di impianti non possiedono le condizioni di sicurezza che dovrebbero avere. Questo può essere dovuto ad un progetto già originariamente insoddisfacente, a un cattivo mantenimento, o a un cambio nelle condizioni di sfruttamento che ha transformato quello che un giorno era stato sicuro in pericoloso. In questa maniera aumenta la probabilità che si verifichino incidenti, sia quelli comuni a qualsiasi attività industriale, come quelli specifici dell'industria chimica: esplosioni, fughe, ecc.

Ci sono, dunque, due necessità sempre più prioritarie: da una parte, il progetto di impianti sicuri, con la definizione del grado di sicurezza corrispondente; dall'altra, l'analisi della sicurezza –e, pertanto, del grado di pericolo– di installazioni già esistenti.

E'evidente che ciò richiede una caratterizzazione del *rischio*, funzione delle conseguenze pregiudiziali di un avvenimento indesiderato a della probabilità che questo succeda. La difficoltà appare, però, nel provare a determinare la probabilità di un avvenimento, e anche per il fatto che il *rischio zero* implica praticamente la inattività, essendo, dunque, necessario fissare il limite accettabile di rischio.

Sono state sviluppate diverse tecniche e metodologie per superare questa difficoltà e per sistematizzare l'analisi dell'affidabilità e della sicurezza nell'industria chimica. Si sono attualmente introdotti metodi utilizzati

con successo in altri campi –aviazione, industria nucleare–. Contemporaneamente, negli ultimi anni, diversi paesi hanno preso misure legislative per garantire una maggior sicurezza nei cosiddetti *impianti chimici pericolosi.* L'interesse per questa tematica diventa ogni giorno più grande, ed è motivo di congressi, seminari e corsi in quasi tutti i paesi industrializzati.

Questa esigenza comincia a sentirsi ormai anche nel nostro paese. E'per questo che la Secció d'Enginyeria della Societat Catalana de Ciències Físiques, Químiques i Matemàtiques, con il patrocinio della Commissió Interdepartamental de Recerca i Innovació Tecnològica della Generalitat de Catalunya, ha organizzato il corso *Projecte i anàlisi de seguretat en plantes químiques perilloses,* a cura del professor Norberto Piccinini, del Politecnico di Torino (Barcellona, marzo 1985).

Pioniera, dunque, in questo campo, la Secció d'Enginyeria publica ora questo libro, che rappresenta un contributo in più per il raggiungimento di una maggior sicurezza nell'industria chimica.

Affidabilità e sicurezza nell'industria chimica inaugura la nuova serie MONOGRAFIES D'ENGINYERIA, che si aggiunge alle altre publicazioni della nostra Societat. L'obiettivo di questa serie è la pubblicazione, in catalano o, in determinati casi, in altre lingue, di lavori monografici pertinenti a branche dell'ingegneria, il cui interesse e la cui attualità rendano consigliabile la diffusione.

Joaquim Casal i Fàbrega

Secretari d'Actes de la Secció d'Enginyeria de la SCCFQiM

SEZIONE I

INCIDENTI E RISCHI NELLE ATTIVITA' UMANE

EVOLUZIONE DEGLI INCIDENTI NELLE ATTIVITA' INDUSTRIALI

Il 1984 sarà probabilmente ricordato come l'anno "nero" dell'industria chimica. In quest'anno infatti sono occorsi tre dei più gravi incidenti mai accaduti per la rilevanza delle luttuose conseguenze che hanno comportato tra la popolazione esterna agli impianti.

Conviene sinteticamente ricordarli:

Data	Località	Tipo di incidente	n° di vittime
25/2	Stato di S.Paolo (Brasile)	Rottura di una pipe-line e conseguente incendio	800
19/11	Città del Messico	Incendio e scoppio di serbatoi di GPL	500
5/12	Bhopal (India)	Nube tossica di isocianato di metile	2700

Dall'esame di questi casi, come dei precedenti incidenti che hanno costellato lo sviluppo dell'industria chimica, possono sorgere domande del tipo:

"Che importanza hanno questi incidenti nei riguardi degli altri provocati dalle attività umane o da calamità naturali?"

"E' l'industria chimica veramente pericolosa nei riguardi delle altre attività industriali?"

In Tabella 1.1 sono riportati i disastri dovuti ad eventi naturali occorsi dal 1900 al 1975 che hanno provocato più di venti vittime; se ne deduce che in media muoiono circa 80.000 persone all'anno (1).

In Tabella 1.2 sono invece riportati gli incidenti, sempre con venti o più vittime, causati da attività industriali o avvenuti nei trasporti negli anni dal 1946 al 1975. Si ricava un valor medio di 2.700 vittime per anno che, "tutto sommato", parrebbe modesto.

Per avere però, un'idea più corretta sulla sicurezza delle attività umane e più in particolare dell'industria chimica, non ci si può fermare solo ad un primo esame delle citate statistiche. Gli eventi, riportati in Tabella 1.2, non sono infatti altro che la punta assai piccola di un iceberg assai ben più consistente.

Tabella 1.1 - Disastri causati da calamità naturali dal 1900 al 1975 con più di 20 vittime (1).

numero di vittime	numero di eventi	tipo di evento	numero di vittime nell'evento più grave (anno di accadimento)
3.100.000	439	inondazione (anche per dighe)	2.000.000 (1931)
1.400.000	262	terremoto	200.000 (1927)
1.000.000	711	evento atmosferico	450.000 (1970)
270.000	143	frana e valanga	180.000 (1920)
80.000	43	eruzione vulcanica	33.000 (1902)

Tabella 1.2 - Incidenti con più di 20 vittime nelle attività industriali o nei trasporti dal 1946 al 1975 (1)

numero di vittime	numero di eventi	tipo di evento	numero di vittime nell'evento più grave (anno di accadimento)
31.300	281	trasporto navale	6.000 (1949)
26.200	522	trasporto aereo	346 (1974)
10.300	188	trasporto ferroviario	300 (1955 e 1957)
12.100	153	incendi ed esplosioni (impianti industriali ed edifici civili)	1.700 (1949)

In Fig. 1.1 è riportata una distribuzione della frequenza degli incidenti nell'industria chimica, dovuti ad esplosioni, incendi e rilasci di sostanze tossiche, in funzione del numero delle vittime.

Dai dati di Fig. 1.1 si ricava facilmente l'istogramma di Fig. 1.2, che può essere interpretato da una curva ottenibile dalla somma di un tipo esponenziale (A) e da una gaussiana (B) (2). L'autore dello studio, infatti, suggerisce di dividere il numero di vittime per classe in due contributi (A e B) legati ad eventi dalle caratteristiche piuttosto diverse e riassunte in Tabella 1.3. (3)

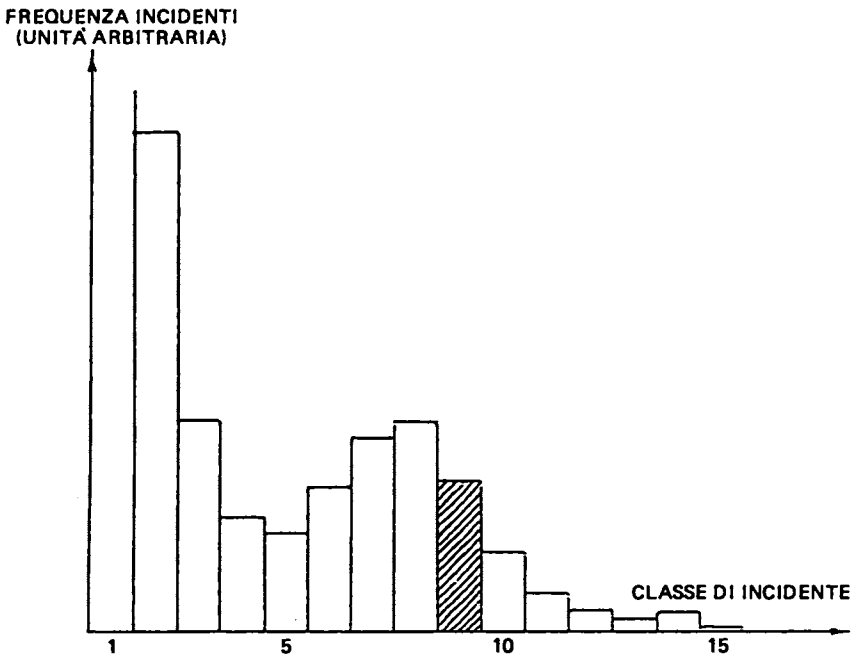


Fig. 1.1 - Distribuzione della frequenza degli incidenti nell'industria chimica secondo Mashall (2)(3).

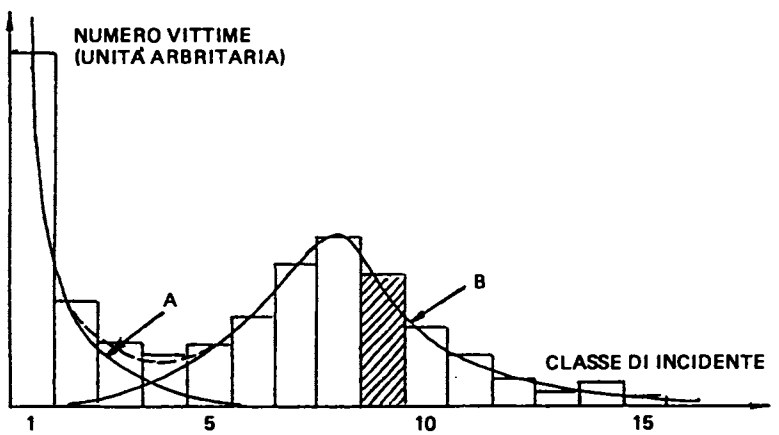


Fig. 1.2 - Numero di vittime per classe di incidente dei dati di Fig. 1.1.(3)

Tabella 1.3 - Caratteristiche degli eventi A e B di cui alla Fig. 1.2.

eventi "A" ("personal accidents")	eventi "B" ("group accidents")
mutamento dell'ambiente scarso o trascurabile	mutamento dell'ambiente di rilievo
la vittima spesso contribuisce a provocare l'incidente	la vittima di solito non contribuisce a provocare l'incidente
danni materiali leggeri	danni materiali gravi
può essere causato da un singolo errore	è generalmente causato da una catena di errori
sono ignorati dai mass-media	sono enfatizzati dai mass-media
per ridurli è consigliabile un approccio tattivo	per ridurli è consigliabile un approccio strategico
ergonomia importante	ergonomia non importante

Sono evidentemente gli eventi di tipo B (tra questi si collocano, in particolare, i rischi di incidenti di rilevante entità) quelli di maggior interesse ai fini di una loro riduzione. Ciò comporta quanto meno eseguire analisi per

- una individuazione delle cause d'incidente,
- una stima delle probabilità di insorgenza,
- una valutazione delle conseguenze.

Lo sviluppo di questi stadi dell'analisi è quanto ci si propone di mostrare in questo corso.

LE BANCHE DI DATI SU INCIDENTI

Ogni volta che, come conseguenza di una serie di eventi incontrollati che si succedono in un intervallo di tempo estremamente breve, si producono danni a persone, impianti o all'ambiente, si parla di incidente. Ad incidente avvenuto si svolgono delle indagini solitamente secondo due forme:

- La prima cerca di fare la rilevazione dei danni (a persone, proprietà, ambiente). Cerca cioè di valutare le diverse componenti della "magnitudo" dell'incidente nel contesto in cui esso è avvenuto, prescindendo dalla sequenza di eventi da cui ha avuto origine. Questa indagine tende così a valutare gli effetti dell'incidente.
- La seconda cerca di individuare la sequenza di eventi che ha originato l'incidente attraverso la raccolta di informazioni sulla situazione preesistente al manifestarsi dell'incidente stesso. Questa indagine tende ad accertare le cause e quindi a prevenire il formarsi di incidenti.

Il risultato di queste indagini, sempre che sia noto, è la storia dell'incidente.

Assai utili sarebbero poi le indagini sui "quasi-incidenti": quelle situazioni critiche occorse secondo la definizione di prima senza però che si sia prodotto il danno.

Ebbene la conoscenza dei dati storici sugli incidenti può fornire ai responsabili di una Azienda per le attività di sviluppo, progettazione, costruzione, esercizio, manutenzione ed ispezione degli impianti, indicazioni utili per:

- quantificare i rischi, in termini di probabilità e di effetti;
- individuare accorgimenti tecnici e organizzativi per ridurre la frequenza di incidenti;
- predisporre piani di emergenza;
- valutare l'attendibilità di modelli matematici per studio delle conseguenze di incidenti;
- effettuare studi statistici e stime di probabilità di incidenti.

I dati storici degli incidenti offrono inoltre corrispondenti indicazioni utili alle pubbliche amministrazioni che hanno il compito di tutela dai rischi conseguenti ad attività industriali.

L'esperienza costituita dagli incidenti diventa però efficace se:

- I dati storici degli incidenti sono sistematicamente raccolti a formare un archivio.
- L'archivio consente un pronto accesso alle prime informazioni utili, secondo i vari aspetti con cui un incidente può essere preso in esame.
- L'archivio conserva il riferimento per l'accessibilità alle fonti originali dell'informazione.
- L'archivio consente elaborazioni statistiche inerenti ad uno o più aspetti di particolare interesse.

In ogni caso queste possibilità giustificano la costituzione di una Banca Dati su Incidenti.

Innanzi tutto la forma e le caratteristiche di una Banca Dati su Incidenti può risultare fortemente dipendente dai seguenti aspetti:

a) Categoria di utenti previste;
b) Fonti di informazione e documentazione.

Il primo punto è assai ovvio e può essere legato anche strettamente al secondo. Esaminando quest'ultimo,si nota subito come siano assai numerose le istituzioni che raccolgono o sono fonte di informazioni. Queste possono risultare da:

- Fascicoli istruttori di uffici governativi;
- Rilevamenti all'interno di una specifica attività industriale;
- Avvenimenti diventati di pubblico dominio;
- Articoli scientifici su riviste o congressi specializzati;
- Atti di procedimenti giudiziari;
- Risultanze di inchieste amministrative;
- Archivi di società assicuratrici;
- Istituzioni preposte all'emergenza ambientale (Vigili del fuoco);
- Ricerche e archivi di Università, società di consulenza o di centri di ricerca.

Se molte sono le istituzioni che raccolgono dati su incidenti, poche sono quelle che organizzano i dati in modo tale da fornire un servizio per utenti esterni all'istituzione stessa. In definitiva sono assai poche le banche di dati su incidenti e poche sono anche le istituzioni che abitualmente forniscono statistiche o rapporti riassuntivi sui

dati che esse raccolgono. Nel seguito si fornisce un elenco delle principali banche o istituzioni esistenti.

- W.O.A.D. (Worldwide Offshore Accident Data Bank) (Norvegia). Dal 1983 è operativa questa banca nata da una preesistente (1975) della Det Norske Veritas.

- Banca Dati Incidenti - ENI (Italia).
Il gruppo Ricerca e Affidabilità dell'ENI (Ente Nazionale Idrocarburi), sfruttando le sue strutture e l'esistente Banca Dati di Affidabilità, ha varato la costituzione di una banca di dati incidenti.

- Banca Dati Affidabilità - TOTAL (Francia).
Analogamente all'ENI, anche la TOTAL (Compagnie Française des Petroles) gestisce una banca dati di affidabilità a cui confluiscono anche le informazioni sui vari tipi di incidenti.

- HARIS (Hazards And Reliability Information System) (UK).
E' questa la banca costituita dalla società di consulenza inglese "Risk Management Consultants" (R.M. Consultants Ltd.).

- FACT (Failure and Accidents Technical Information System) (Olanda).
E' questa probabilmente la più nota e su cui si hanno più informazioni, banca di dati su incidenti. Essa è stata costituita dal TNO in stretta cooperazione con le industrie e le autorità pubbliche olandesi.

- CHAFINCH Databank (The Chemical Accidents, Failure Incidents and Chemical Hazards Databank) (UK).
Questa banca è gestita da Risk Management Ltd (RML), nota società di consulenza inglese.

Oltre agli enti che gestiscono una banca dati la raccolta di informazioni su incidenti è fatta da numerose istituzioni che, o non pubblicano alcun tipo di notizia al riguardo, oppure rilasciano saltuari o periodi rapporti statistici o, talvolta, pubblicazioni specializzate. Si ricordano:

- NFPA (National Fire Protection Association) (USA).
E' quesa probabilmente la più nota associazione, specializzata nella prevenzione degli incendi.

- U.S. Department of Transportation (USA).
  Questo ente raccoglie sistematicamente notizie su incidenti che coinvolgono sostanze tossiche durante un trasporto di qualsívoglia natura.

- The Clorine Institute (USA).
  Questo ente, che riunisce i produttori di cloro in USA per una pronta e mutua assistenza in caso di incidenti, raccoglie notizie sugli incidenti connessi soprattutto al trasporto di cloro.

- Lloyds List (UK).
  Questi rapporti, pubblicati dai Lloyds of London Press Ltd, contengono notizie sugli incidenti connessi ai trasporti marittimi e gli impianti offshore.

In generale lo scopo di una raccolta sistematica degli incidenti è quello di essere:

- uno strumento per un miglior confronto tra attività industriali;
- la base conoscitiva per la predisposizione di norme, regolamenti o atti legislativi;
- un riferimento concreto per valutazioni di analisi di rischio.

Da quanto detto in precedenza emerge però che i problemi di sicurezza ricevono considerazione secondo punti di vista anche molto diversi, ciò naturalmente comporta differenti impostazioni delle ricerche sugli incidenti.

Ne consegue che la formazione di una Banca Dati Incidenti difficilmente può rispondere pienamente alle esigenze di ogni specifico utente, anche se una sua caratteristica essenziale dovrebbe essere quella di consentire il massimo di possibilità di uso per qualsiasi utente e contemporaneamente conservare l'accessibilità alle fonti dirette di informazioni per ogni caso specifico.

Lo stimolo maggiore ad una giusta formazione di una Banca Dati Incidenti di ampio respiro sarebbe dato da specifiche norme emanate da pubbliche autorità incaricate di:controllo delle condizioni iniziali, esame del progetto, licenza alle costruzione, licenza all'esercizio e verifiche successive di attività industriali comportanti rischi.

Su questa linea si è indubbiamente posta la Direttiva CEE 82/501 del 24/6/1982, di cui si parlerà in seguito.

EVOLUZIONE DEI CONCETTI DI RISCHIO E DI SICUREZZA

Il giorno 13.7.1973 a Postchefstroom in Sud Africa,la frattura del fondello di un serbatoio orizzontale di ammoniaca provocò la fuoriuscita di 38 tonnellate di prodotto che formarono una nube tossica di diametro 150 m e di altezza 30 m; il vento spinse lentamente la nube verso la vicina città che fu avvolta da gas tossici: 18 furono le vittime di questo disastro e 65 i feriti gravi.

Il giorno 1.6.1974 a Flixborough in Gran bretagna, a seguito del cedimento di una tubazione di processo in un impianto chimico, vennero emesse all'atmosfera 36 tonnellate di cicloesano; dopo circa 30 secondi questa nuvola di idrocarburi infiammabili trovò un punto di innesco e diede luogo ad una deflagrazione con effetti pari a quelli derivanti da 18 tonnellate di Tritolo (TNT). La sovrapressione così generata provocò la distruzione totale dell'impianto e danneggiò gravemente il vicino villaggio: 28 furono le vittime di questo disastro.

Il giorno 8.1.1979 all'isola di Whiddy, nella baia di Bantry (Irlanda) un incendio di dimensioni colossali avvolse la petroliera Betelgeuse mentre stava eseguendo le operazioni di zavorraggio al pontile della Gulf Oil. I sistemi antincendio non operarono, i soccorsi si mossero in ritardo. La nave si spezzò in più tronconi; l'intera superficie del mare, nella zona del pontile, fu coperta da olio in fiamme che giunse fino alla spiaggia. Il bilancio fu di 50 vittime.

Questi sono solo una piccola esemplificazione di alcuni dei disastri più rilevanti avvenuti negli anni 70 e riferentesi all'industria di processo. La lista completa è ovviamente assai più estesa (Es., rilascio di diossina a Seveso nel 1976, scoppio di un'autobotte carica di etilene a S. Carlos de la Rapita nel 1978, ecc.).

L'accadere di tali incidenti ha posto in evidenza i pericoli intrinseci nelle operazioni di processo e nelle diverse parti degli impianti. Essi sono legati alla movimentazione dei materiali, ai componenti chimici manipolati, ai materiali utilizzati, alle condizioni di esercizio imposte (temperatura e pressione) sia a regime che durante i transitori.

Il dibattito sociale sviluppatosi negli ultimi anni ha così provocato importanti mutamenti ai concetti generali di "rischio" e di "sicurezza". Da un lato, sotto il profilo economico-retributivo si è progressivamente accantonata la possibilità di monetizzare il rischio; da un altro lato, sotto il profilo della definizione stessa di sicurezza, si è passati da un concetto più ristretto di sicurezza fisica, si può dire meccanica, ad uno più vasto e più attento ai valori umani e ambientali. Una schematizzazione di questa definizione più ampia di sicurezza è riportata in Fig. 1.3. In pratica, ciascun componente (processo, impianto, operatore, ecc.) deve raggiungere i prescritti livelli di sicurezza durante il procedere dei singoli gradini (ideazione, progetto, ecc.).

Il verificarsi in questi ultimi anni di alcuni gravi incidenti ha portato, oltre ad un ampliamento del concetto di sicurezza anche ad una ridefinizione dei rischi come appare ad esempio dalla Tab. 1.4.(4)

Tabella 1.4 - Classificazione sommaria dei rischi derivanti da un'attività industriale.

A) - RISCHI CONVENZIONALI, collegati all'attività di lavoro e alle apparecchiature e impianti che normalmente si trovano in tutti i settori industriali (sono, per esempio, i rischi di cadute da scale, i rischi di infortuni o di morte da elettricità, i rischi derivanti dagli organi di trasmissione del moto);

B) - RISCHI SPECIFICI, relativi all'uso di particolari sostanze e prodotti chimici, che per loro natura possono determinare danni a breve o a lungo termine alle persone, alle cose e all'ambiente;

C) - RISCHI POTENZIALI di grande magnitudo, legati a incidenti del tutto anomali, le cui conseguenze consistono generalmente in esplosioni oppure nella fuoriuscita in tempi brevi di notevoli quantità di sostanze pericolose (tossiche, infiammabili, ...) in grado di interessare vaste aree sia all'interno che all'esterno dello stabilimento.

SICUREZZA DEL	NELLA FASE DI: IDEAZIONE	PROGETTO	COSTRUZIONE	GESTIONE
PROCESSO				
IMPIANTO				
OPERATORE				
AMBIENTE INTERNO				
AMBIENTE ESTERNO				

Fig. 1.3 - I diversi aspetti della sicurezza di un impianto industriale.

Dalla ricerca e dallo studio sistematico degli incidenti storicamente verificatisi, si possono trarre preziose indicazioni sulle politiche future, volte ad aumentare le condizioni generali di sicurezza dei lavoratori e della popolazione, compatibilmente con il mantenimento del livello di "qualità della vita" raggiunto.

D'altra parte, parlare di "rischio zero" è una pura astrazione senza riscontro nella realtà. Un certo livello di rischio esiste sempre, in ogni attività umana: il problema è di valutare qual'è questo livello, decidere se è accettabile o meno ed, in caso di risposta negativa, decidere il da farsi per ridurlo a valori accettabili.

Per affrontare questa problematica in modo scientifico si è venuta affermando negli anni recenti, anche nel campo della progettazione degli impianti chimici, quella disciplina che è solitamente indicata come Ingegneria della Sicurezza o Ingegneria dell'Affidabilità dei Sistemi.

Con riferimento alla Tab. 1.4 sono naturalmente quelli di tipo c), i "rischi potenziali di grande magnitudo", che investono l'intera comunità civile. Per questo alcune nazioni europee hanno già promulgato leggi che obbligano i gestori di un impianto ad elevata pericolosità, cioè in grado di generare rischi di tipo c), alla presentazione alle autorità di un "rapporto di sicurezza" analogamente a quanto si fa già da tempo per le centrali nucleari.

VALUTAZIONE PROBABILISTICA DEI RISCHI

Quantificazione del rischio

E' radicata l'abitudine di descrivere un impianto industriale in termini quantitativi: l'impianto XY si estende per una superficie di 2000 m^2, ha una capacità di produzione pari a 3000 t/anno, occupa 150 addetti, ha comportato un investimento di 30.000 milioni di lire, ecc.

Nessuno infatti riterebbe esauriente una descrizione solo qualitativa, del tipo: l'impianto XY si estende per una "vasta" superficie, ha una "notevole" capacità produttiva, occupa "alcuni" addetti ed ha comportato un "non trascurabile" investimento... E soprattutto nessuno oserebbe esprimere giudizi o trarre conseguenze operative da una siffatta descrizione solo qualitativa.

Eppure esiste un aspetto certo non secondario degli impianti industriali per cui si suole dare descrizioni ed esprimere giudizi in termini puramente qualitativi: il rischio tecnico associato agli stessi. Si suole, cioè, descrivere la pericolosità di un impianto dicendo che lo stesso è "molto" pericoloso, o "poco", o "abbastanza", o "non" pericoloso, ma assai raramente capita di descrivere un impianto dicendo "quanto" è pericoloso.(10)

La non quantizzazione del rischio tecnico ha alcune conseguenze negative:

a: I giudizi sull'entità del rischio sono fortemente soggettivi, in quanto non derivano da una seria analisi scientifica.

b: Le decisioni prese dall'autorità politica e/o dalle direzioni aziendali in merito alla accettabilità del rischio stesso non sono ancorate a concreti elementi di giudizio e quindi possono più facilmente non essere le migliori.

c: I confronti tra i rischi connessi a impianti diversi e/o diversi settori produttivi sono praticamente impossibili.

d: Gli interventi operati sugli impianti per migliorare la affidabilità (o per diminuire il rischio tecnico) derivano spesso più dalla intuizione e dalla pur rispettabile esperienza dei progettisti che non da una razionale ed oggettiva valutazione tecnica.

Con il crescere delle dimensioni degli impianti, dei relativi costi ed, inevitabilmente, dei relativi rischi potenziali, l'esigenza di una valutazione più oggettiva degli stessi si è fatta impellente. (10)

Definizione di rischio

La definizione più largamente accettata di rischio (R) è la seguente:

Rischio = (Frequenza prevista per l'evento) x (Conseguenze probabili) (1.1)

e, con una scrittura più sintetica:

Rischio = Frequenza x Magnitudo

Si suole cioè dire che, se un certo evento ha una frequenza probabile (F) di 1 volta ogni 10 anni e se le sue conseguenze (magnitudo) sono stimabili in 50 feriti, il rischio associato a quell'evento è di provocare:

R = 0.1 x 50 = 5 feriti/anno

Se quello stesso evento provocasse come conseguenza un danno economico di 700 milioni di lire, il relativo rischio economico sarebbe di:

R = 0.1 x 700.000.000 = 70.000.000 lire/anno

Se le conseguenze di un incidente fossero solo di una stessa specie il problema della scelta dell'unità di misura della magnitudo (M) non si porrebbe. Infatti se le conseguenze fossero esclusivamente danni materiali oppure solo casi mortali, un milione di lire oppure un caso mortale sarebbero, rispettivamente, convenienti unità di misura.

Ma nella maggioranza dei casi le conseguenzedi esplosioni, diffusione di nubi dannose (tossiche, radioattive, infiammabili,...) e incendi possono essere morti, feriti e danni agli impianti e guasti all'ambiente, per non parlare di effetti a lunga scadenza, non sempre noti o facilmente prevedibili. (11)

La definizione di rischio come semplice prodotto può far nascere qualche perplessità.

Si è tutti d'accordo che un evento che capita mediamente ogni 100 anni e provoca 10.000 morti equivale a una serie di 100 incidenti ogni anno, ognuno dei quali provoca un morto?

Alla formula sopraddetta possono muoversi anche altre obiezioni, tuttavia si preferisce come base di lavoro attenersi alla definizione primitiva, per la sua semplicità che, tra l'altro, si presta ad una suggestiva rappresentazione grafica (Fig. 1.4).(12)

Accettabilità del rischio

Determinare la frequenza prevista per l'accadimento dell'evento ipotizzato e la gravità delle conseguenze si chiama oggi: valutazione probabilistica del rischio, da effettuare in modo qualitativo e/o quantitativo, se quest'ultima analisi si può considerare significativa in relazione alle conoscenze del momento.

La valutazione si articola attraverso tre studi:
- individuazione degli eventi potenzialmente pericolosi,che possono dar luogo ad un incidente rilevante,
- esame dell'affidabilità del sistema e della frequenza dell'accadimento dell'evento,
- analisi delle conseguenze.

La convenienza di accettare questa definizione è legata alla possibilità di quantificare il rischio: il termine "rischio" perde così il significato vago che ha nel linguaggio comune. In questo modo si potranno effettuare confronti e stabilire graduatorie di rischio.

Nel caso il rischio non venga considerato tollerabile, in relazione ai benefici attesi dall'attività a cui si riferisce, si potrà diminuire il rischio operando sulla frequenza di accadimento (azione di prevenzione) o sulla magnitudo delle conseguenze (azione di protezione). Si veda in proposito la Fig. 1.4, nella quale sono indicate le linee di ugual rischio $R_1 > R_2 > R_3$.

Questa formulazione permette di superare il metodo del "what if"(cosa fai se...), impiegato un tempo dalle autorità preposte al controllo della sicurezza dei reattori nucleari. Questo metodo consiste nel porre una successione di domande circa i provvedimenti presi dal progettista per evitare incidenti sempre più gravi. Ma poiché non esiste un incidente massimo, si ha una escalation senza fine. E' stato osservato - e questo è di eccezionale importanza - che in tal modo la sicurezza era orientata ad evitare eventi che difficilmente sarebbero accaduti, mentre lasciava l'impianto indifeso da eventi, di conseguenze meno gravi, ma molto più probabili. (13)

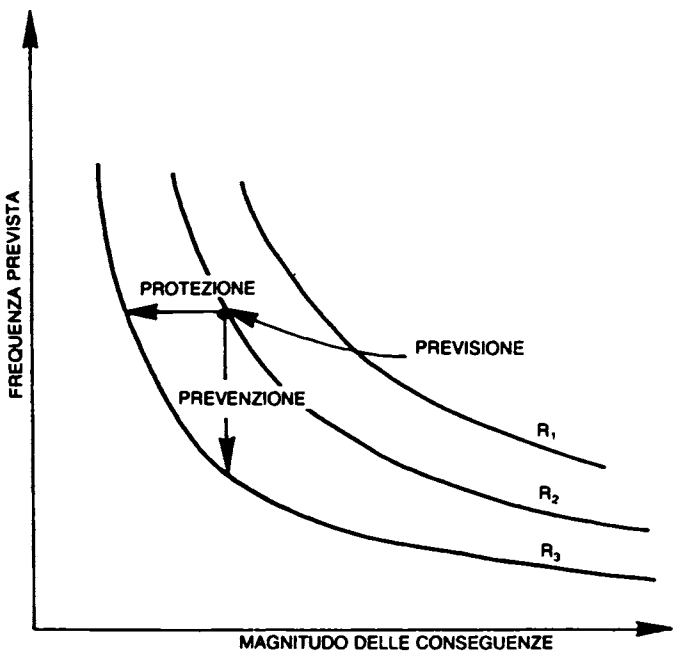


Fig. 1.4 - Linee di ugual rischio.(12, 13)

Ove si accetti, come ormai largamente si usa, la definizione di rischio, data con la relazione 1.1) ne consegue che, essendo il rischio il prodotto di due probabilità, lo stesso potrà essere molto piccolo, ma non potrà mai essere uguale a zero (Natura probabilistica del rischio).

Gli studi di valutazione probabilistica dei rischi consentono di stimare i due fattori del prodotto della relazione 1.1) e di individuare i metodi per ridurne la grandezza a valori accettabili.

Il decidere invece quale sia questa soglia di accettabilità è compito della collettività attraverso i suoi organi rappresentativi. La definizione della soglia di accettabilità normalmente passa attraverso dei bilanci rischi-benefici. Si deve cioè tenere conto dei rischi legati all'attività e dei benefici derivanti alla collettività da quella stessa attività.

La frequenza

La frequenza, generalmente espressa in a^{-1}, è l'inverso di una durata di tempo T che per eventi periodici è noto come periodo di ritorno.

La locuzione "periodo di ritorno" ha ancora un significato per eventi quasi periodici: l'espressione "ogni morte di Papa" esprime, nel linguaggio corrente,un evento piuttosto raro, al quale si assiste 4-5 volte durante la vita, cioè $1/T = 5 \times 10^{-2}$ all'anno.

Per effetti casuali cade il concetto di periodità e T è effettivamente un tempo medio. Se gli eventi che si considerano si presentano però con una certa frequenza si riescono ancora a "vedere" le fluttuazioni attorno al valore medio. Se gli eventi casuali sono invece molto rari (sono stimati capitare una volta nella vita: $1/T = 10^{-2}$ all'anno, od ogni 1000 o 10.000 anni) si perde anche questa sensazione: eventi quasi impossibili possono capitare domani e, magari, dopodomani. Ma saranno proprio fluttuazioni?

Ora negli studi sulla valutazione probabilistica dei rischi si ha a che fare spesso con frequenze molto piccole (10^{-4} - 10^{-5} all'anno o anche meno) ed è del tutto giustificata la perplessità di molti di fronte a questi numeri.(11)

Compresenza di più rischi

occorre notare inoltre come generalmente ogni impianto considerato presenti più eventi potenzialmente pericolosi, ciascuno caratterizzato da una magnitudo m_i e da una frequenza stimata f_i. Sia $r_i = m_i . f_i$ il rischio relativo all'evento i-esimo, allora il rischio dell'impianto sarà dato dalla somma dei rischi di tutti gli eventi:

$$R = \Sigma r_i = \Sigma m_i . f_i = \frac{\Sigma m_i . f_i}{\Sigma f_i} . \Sigma f_i = M . F$$

esprimibile ancora come il prodotto di una magnitudo M per una frequenza F.

Nel caso si avessero molti eventi, presi in considerazione in un campo esteso di magnitudo e di frequenze, si potrebbe ricavare una rosa di punti F = F(M) e da questa si potrebbe calcolare la frequenza cumulativa degli eventi con magnitudo minore oppure uguale o maggiore a M. Quest'ultima rappresentazione, che è indicata con F* = F*(M), relativa agli eventi con magnitudo uguale o maggiore a M, è quella comunemente usata. Nella Fig. 1.15 è riportato un grafico di questo tipo tratto dai dati della Tabella 1.5. (13)

Molto spesso i risultati di un'analisi sono indicati senza esprimere chiaramente il possibile errore associato. Poiché in alcuni problemi può capitare di avere incertezze di 1 o 2 ordini di grandezza, le conclusioni in questi casi tratte da lettori sprovveduti o da analisi interessati possono essere totalmente sbagliate o volutamente ingannevoli. (11)

Tab. 1.5 - Eventi catastrofici relativi a dighe.(13)

Anno	Luogo	Numero di vittime
1959	Bhakra (India)	10
1959	Vega de Tera (Spagna)	123-150
1959	Frejus (Francia)	421
1960	Oros (Brasile)	circa 1.000
1961	Kiev (URSS)	145
1963	Vajont (Italia)	2.600-3.000
1967	Koyna (India)	180
1977	Teton (USA)	9-11
1979	Morvi (India)	più di 3.000

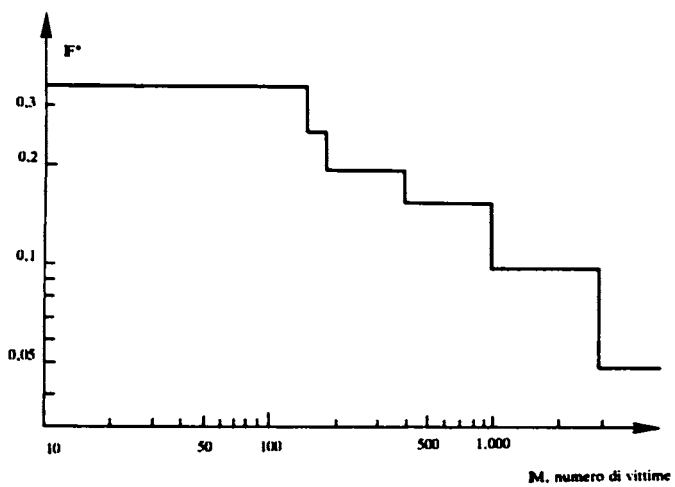


Fig. 1.5 - Eventi all'anno con magnitudo uguale o maggiore di M per i dati di Tabella 1.5.(13)

SEZIONE II

LA SICUREZZA NELL'INDUSTRIA CHIMICA

LA COSIDDETTA "DIRETTIVA SEVESO" DELLA CEE

Sotto la spinta di gravi incidenti avvenuti nell'industria chimica nei primi anni '70 ed in particolare dell'esplosione che il 1/6/1974 distrusse completamente un impianto chimico a Flixborough in Inghilterra (28 morti, numerosi feriti) e del disastro di Seveso in Italia (10/7/1976), alcune nazioni europee si sono date delle norme per la progettazione, l'installazione e la gestione di impianti di elevata pericolosità.

In particolare il Consiglio delle Comunità Europee ha emesso il 24/6/1982 una Direttiva sui "rischi di incidenti rilevanti connessi con determinate attività industriali" (82/501 CEE), più nota come "Direttiva Seveso".

Lo scopo della Direttiva, che tiene conto dei concetti di base della "valutazione probabilistica del rischio",è quello di limitare la possibilità che si verifichino incidenti di rilevante entità.

L'individuazione di questi si fonda sul seguente presupposto oggettivo: se in un impianto vi è una quantità di materiale infiammabile esplosivo o fortemente tossico in quantità tale che il suo incendio, esplosione o rilascio causa danni molto rilevanti alle persone, alle cose o al territorio, esiste la possibilità che si verifichi un incidente di rilevante entità. Per questo la Direttiva CEE presenta per le sostanze tossiche, una scala di tossicità e riporta un esteso elenco di prodotti con le quantità minime al di sopra delle quali intervengono determinati obblighi di notifica alle pubbliche autorità.

Nelle Figg. 2.1 e 2.2 si riporta sinteticamente quanto richiesto dalla Direttiva CEE, mentre come allegato si riporta integralmente il testo della stessa.

In particolare, secondo l'Articolo 5 della Direttiva, la procedura di autorizzazione alla costruzione e all'esercizio di un impianto industriale prevede che,in una o più fasi,gli organi tecnici delle Amministrazioni Pubbliche esaminino i progetti presentati dall'Imprenditore per verificare che l'iniziativa non provochi alterazioni intollerabili all'ambiente e non produca pericoli gravi per la popolazione e per gli addetti.

A. C H I U N Q U E

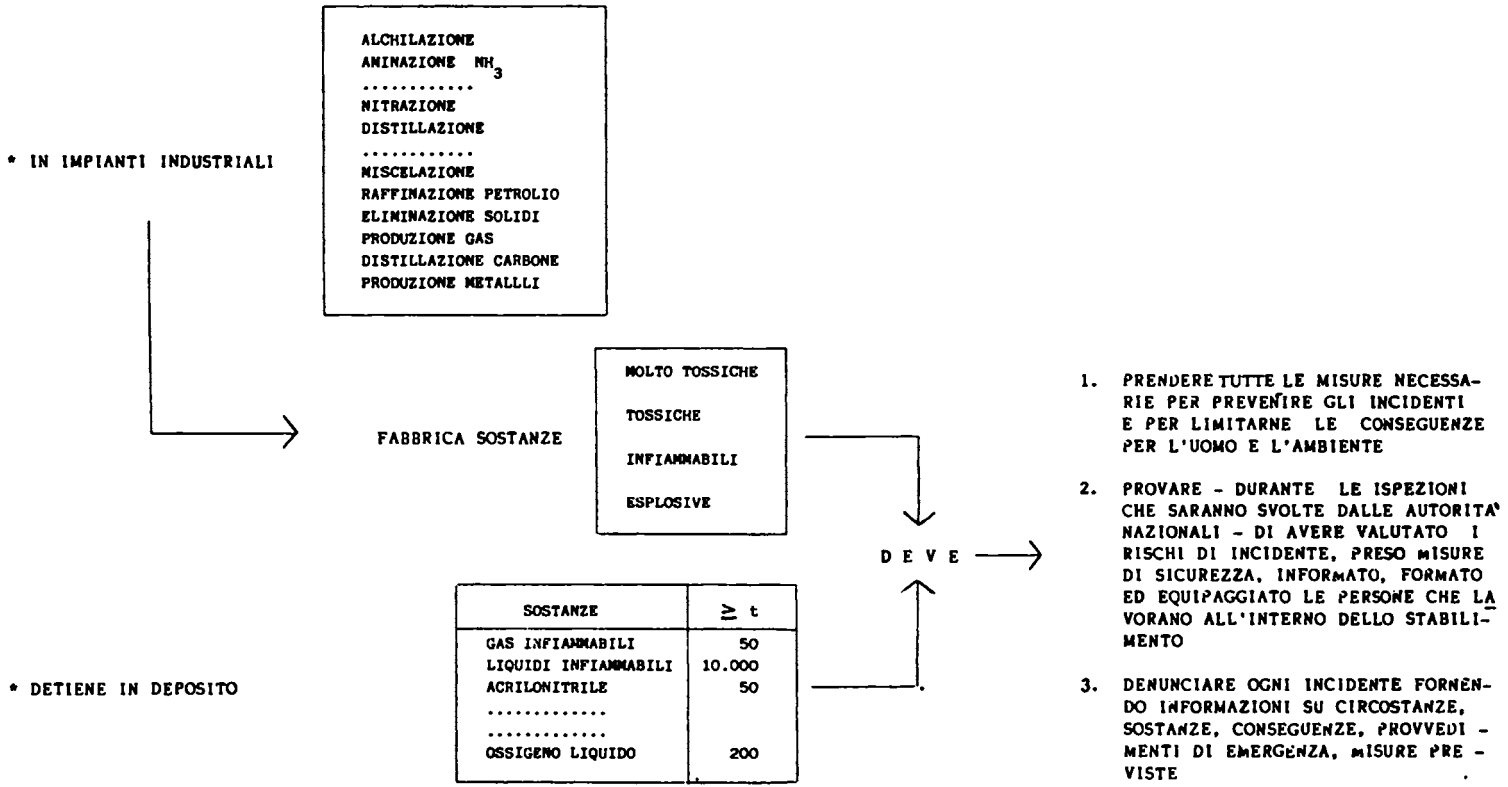


Fig. 2.1 - Prescrizioni "minime" secondo la Direttiva CEE 82/501.

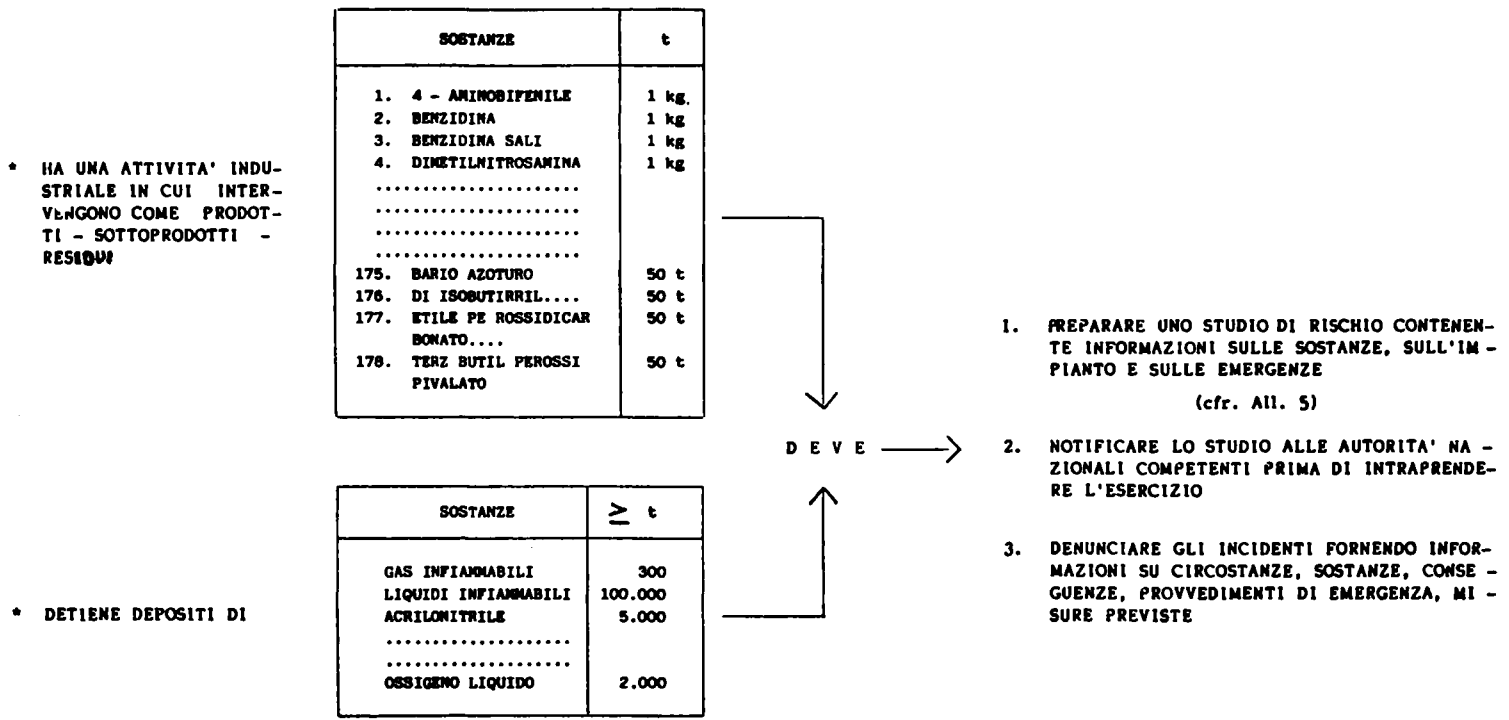


Fig. 2.2 - Prescrizioni "massime" secondo la Direttiva CEE 82/501.

E' necessario quindi che l'Imprenditore esegua preventivamente analisi di sicurezza sulla base dei dati progettuali senza l'ausilio dell'esperienza maturata dalle maestranze durante l'esercizio.

Solo in qualche raro caso è infatti possibile utilizzare l'esperienza di altri impianti uguali o simili realizzati in precedenza.

Quale sintetico commento alla Direttiva, si può affermare che essa costituisce un caposaldo fondamentale nel campo della legislazione sulla sicurezza degli impianti e la salvaguardia delle persone. Infatti, che le indicazioni da questa suggerite siano estremamente valide, si deducono dagli obblighi che essa impone ai fabbricanti, che vanno da quello di prendere tutte le misure atte a prevenire gli incidenti e a limitarne le conseguenze per l'uomo e per l'ambiente, a quello di notificare alle autorità competenti, tutte le informazioni relative alle sostanze prodotte, agli impianti, ai piani di emergenza. Non solo; le persone residenti nei pressi di un impianto che produce sostanze pericolose che devono essere informate , devono essere messe al corrente delle misure di sicurezza e delle norme da seguire nei malaugurato caso che il rischio si avveri.

IL RAPPORTO DI SICUREZZA PER IMPIANTI PERICOLOSI

La caratteristica principale del documento previsto dalla Direttiva CEE 82/501 è quella di richiedere un esame della sicurezza di un impianto nella sua globalità ivi comprese le situazioni di emergenza nel caso di effettivo incidente.

E' naturale che la Direttiva non entri nei particolari delle metodologie da adottare ma è scontato che sono da impiegare tutte le risorse offerte dalla scienza e dalla tecnica. Se è il caso, inoltre, per completare il quadro delle conoscenze, sono da affrontare studi e ricerche ad hoc.

La via che si è affermata è quella di introdurre nell'analisi di sicurezza degli impianti chimici i concetti ed i metodi dell'affidabilità tecnologica, che sono stati applicati con enorme successo nell'industria aeronautica, elettronica e nucleare.(14-16)

Trattasi di un insieme di metodologie, nessuna delle quali completamente esaustiva e non tutte univocamente codificate, che però, se adottate nel momento opportuno, soprattutto nelle successive fasi della progettazione, sono in grado di far nascere un impianto "ragionevolmente" sicuro.

Più precisamente, la sicurezza e l'affidabilità di un impianto, e quindi anche la sua disponibilità, sono collegate alla possibilità che eventi non desiderati si realizzino, alla probabilità che ciò avvenga e alle loro possibili conseguenze immediate o future.

Appare evidente che l'analisi di sicurezza ed affidabilità degli impianti deve partire dall'individuazione degli eventi indesiderati presenti con l'obiettivo di rimuoverli per quanto possibile.

Innanzitutto è necessario eliminare tutte le cause di eventi dannosi collegati ad attività non indispensabili.

Per quelli non eliminabili è necessario, mediante l'analisi di affidabilità, valutare la frequenza, per prendere quelle decisioni capaci di diminuirla e per individuare le possibili azioni che possano limitare l'entità dei danni conseguenti.

Le tecniche di analisi sono diverse: alcune prevalentemente qualitative, altre si spingono fino a costruire relazioni analitiche che forniscono una misura della frequenza che un evento accada, altre, infine, tendono a prevedere in modo quantitativo la gravità dei danni.

Il grado di approfondimento con il quale condurre l'esame degli impianti dal punto di vista della sicurezza si fa dipendere, generalmente, dalla gravità del danno conseguente al realizzarsi di un determinato evento. Ciò significa che la scelta della tecnica di analisi non si fa dipendere né da una stima "a priori" della probabilità con la quale l'evento può realizzarsi né dalla valutazione della frequenza con la quale si è avverato in impianti esistenti.

Dall'analisi della letteratura corrente e dalle esperienze maturate in questi ultimi anni, si può ricavare un procedimento per l'analisi della sicurezza globale di un impianto ad elevata pericolosità, sintetizzato nelle sue linee essenziali in Fig. 2.3 e così riassumibile (17-21):

1 - Dapprima il progetto iniziale può essere esaminato nel suo complesso mediante l'uso di "check list" già pronte. Si tratta di un primo esame sommario per vedere se sono state affrontate certe problematiche relative alla sicurezza e come sono state risolte.

2 - Il progetto viene quindi definito con maggiori dettagli e sono così elaborati diversi documenti (flow sheet, pipe and instrument flow diagram, ecc.).
In questa fase deve essere effettuata l'analisi del processo per identificare i punti deboli del sistema ed i possibili eventi di origine "interna" non desiderati.
A questo punto il progetto deve essere opportunamente modificato per tenere nel debito conto dei rilievi emersi con l'analisi del processo, viene così ad assumere un aspetto consolidato "quasi" definitivo.

3 - E' ora necessario individuare tutti i possibili eventi non desiderati procedendo con un'indagine sistematica in modo, possibilmente, che nessun aspetto connesso con la sicurezza venga escluso.

3.1 Eventi esterni. Si tratta di esaminare i possibili eventi che dall'esterno dell'impianto possono produrre direttamente o indirettamente incidenti.

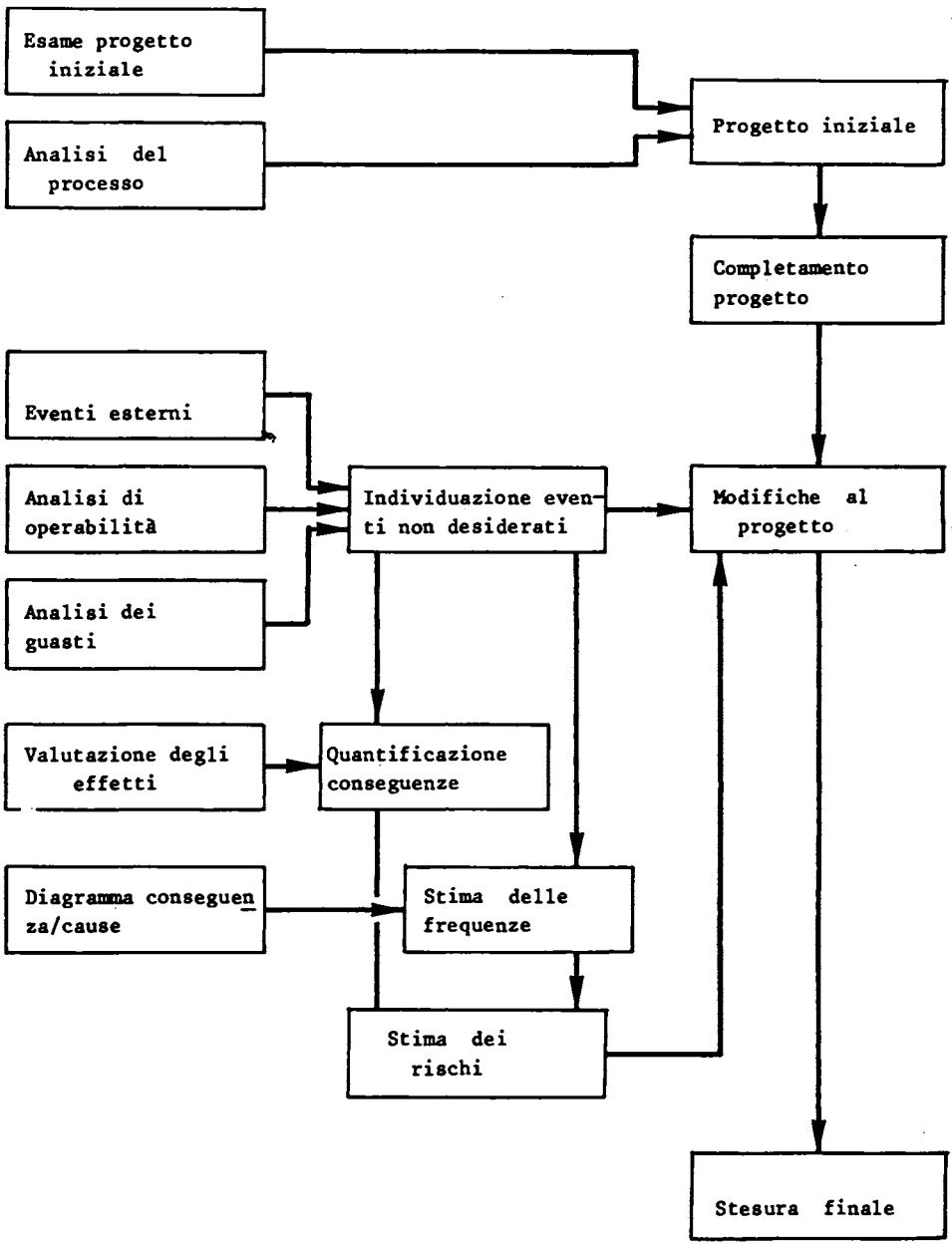


Fig. 2.3 - Schema per lo sviluppo di un'analisi di sicurezza.

3.2 Eventi interni. l'individuazione degli eventi interni non desiderati può essere compiuta con metodologie diverse. Quelle di maggior interesse sono l'"analisi di operabilità" e l'"analisi dei guasti". La prima studia le conseguenze degli scostamenti dai valori di progetto delle grandezze fisiche del processo (es. portata, temperature, pressioni, ecc.), la seconda invece esamina la possibilità di malfunzionamenti della parte meccanica dell'impianto (valvole, strumenti, ecc.).

4 - In seguito alle indagini precedenti il progetto dell'impianto viene modificato di conseguenza. l'esame della sicurezza procede quindi su due vie parallele.

4.1 Una, attraverso lo studio degli effetti di un incidente, tende a valutarne le relative conseguenze. A determinare cioè la "magnitudo" delle conseguenze di un evento non desiderato.

4.2 L'altra invece, tende a stimare la frequenza con la quale l'evento non desiderato potrà presentarsi nel tempo. La più nota delle metodologie per questo tipo di indagine è l'analisi che si sintetizza nel diagramma "conseguenze/cause" o "albero di guasto".
E' questa una struttura logica nella quale sono individuate le diverse cause che portano ad una determinata conseguenza.

5 - La combinazione della "magnitudo" dell'evento e della sua frequenza permette di valutare il rischio tecnologico dell'evento non desiderato in studio. Se questo è giudicato troppo elevato, il progetto dell'impianto deve essere modificato di conseguenza.
Procedendo in questo modo si giunge alla stesura finale del progetto. (22)

CONTENIMENTO DELLE PERICOLOSITA' NELLE FASI INIZIALI DI PROGETTAZIONE

Analisi con "check list"

L'esame del progetto iniziale è di fatto una fase preliminare e preparatoria all'analisi vera e propria dei rischi: quest'ultima, avendo come obiettivo la stima della frequenza degli incidenti possibili e la valutazione della entità delle loro conseguenze, è essenzialmente quantitativa, mentre questo esame non può che essere prevalentemente qualitativo.

Ciò nonostante lo studio è della massima importanza, in quanto serve a porre le basi per la successiva analisi quantitativa, a individuare le aree dove questa eventualmente è superflua e a stabilire delle priorità per quelle dove invece è necessaria. (23)

Per progetto iniziale si intende qui l'insieme della documentazione che definisce, nelle sue linee essenziali, l'impianto. Questa può essere individuata in:

- basi del progetto;
- descrizione del processo, schema semplificato di lavorazione;
- elenco delle sostanze che prendono parte al processo (materie prime, intermedi, prodotti, sottoprodotti);
- portata e composizione degli effluenti;
- lay-out preliminare;
- planimetria dello stabilimento in cui l'impianto sarà inserito (se il caso).

Spesso per rendere l'analisi sistematica, si fa uso di check list, cioè di questionari opportunamente preparati. Un esempio è riportato in Tabella 2.1.(24)

Analisi del processo

Una volta completato l'esame del progetto iniziale, inizia la prima fase di progettazione dell'impianto, quella che va sotto il nome di progettazione di base (process flow sheet, pipe and instruments flow diagram, plot plant and elevation). In questa fase quindi viene effettuata l'analisi del processo che costituisce il primo passo per l'identifi-

Tab. 2.1 - Questionario preliminare per le informazioni di processo.

1) Descrizione sommaria del processo con specificazione delle temperature e pressioni approssimative (ordine di grandezza).

2) Schema semplificato.

3) Elenco completo delle materie prime e dei chemicals e relative specifiche e analisi.

4) Elenco dei prodotti, intermedi e sottoprodotti noti e relative specifiche o analisi.

5) Per ognuna delle reazioni che normalmente avvengono nel processo occorre conoscere, per quanto possibile:
   - tonalità termica
   - eventuali sottoprodotti.

6) Caratteristiche chimico-fisiche, tossicologiche, ecc. delle varie sostanze di cui ai punti precedenti.

7) Esistono operazioni che richiedono, per la loro natura particolare, l'uso di particolari attrezzature di protezione da parte degli operatori?

8) Esistono operazioni che richiedono, per la loro natura, da parte dell'operatore cautele, addestramento, diligenza minima superiore alla media?

9) Dove scaricano le valvole di sicurezza, i dischi di rottura, le guardie idrauliche, ecc.?

10) Informazioni sugli effluenti
   - scarichi liquidi
   - scarichi gassosi in torcia.

11) Esistono nell'impianto sostanze intrinsecamente instabili o che presentano una elevata reattività?

12) Esistono sostanze che in caso di incendio non siano compatibili con acqua o schiuma?
   - se sì: quali?
   - quali sistemi di estinzione son previsti?

13) Quale frequenza è richiesta per operazioni che comportino l'apertura di apparecchiature contenenti fluidi pericolosi? e/o l'ingresso in essi di persone?
   - in questi casi sono richiesti particolari sistemi di bonifica? quali?
   - in questi casi sono richiesti particolari sistemi di protezione individuale? quali?

cazione degli eventi, di origine "interna" non desiderati (malfunzionamenti generici, blocco dell'impianto, incidenti). Quest'analisi consiste essenzialmente nel controllare il comportamento dell'impianto e delle sue parti componenti al variare dei parametri operativi del processo e nello stabilire gli intervalli dei parametri entro i quali la marcia dell'impianto può considerarsi sicura. (23)

L'analisi del processo è certamente un momento chiave dell'intera progettazione: conviene infatti che la sicurezza dell'impianto sia intrinseca, per quanto possibile, al processo stesso. Si ottengono cioè elevati standard di sicurezza e quindi elevata disponibilità di un impianto quanto più il processo è stato studiato per far fronte alle possibili cause di emergenza senza che debbano intervenire sofisticati dispositivi di regolazione o di blocco.

Un esempio dettagliato è riportato nell'articolo: "Process Safety Analysis for Better Reactor Cooling System Design in the Ethylene Oxide Reactor",(25)

Individuazione delle pericolosità esterne all'impianto

Accanto alle cause "interne" al processo e alla sua realizzazione industriale devono essere tenuti presenti anche gli eventi esterni che possono causare incidenti. E' comune distinguerli come eventi naturali (evento sismico: frana; inondazione; uragano, tromba d'aria; ecc.) ed eventi artificiali (esplosione, incendio, nubi dannose provenienti da impianti vicini; crollo di dighe; eventi provocati dal traffico stradale; eventi provocati dal traffico aereo; sabotaggio). (23)

Anche questo esame può essere agevolato con l'uso di check list; un esempio è riportato in Tabella 2.2.(24)

Tab. 2.2 - informazioni preliminari circa l'ubicazione dell'impianto.

1) In quale stabilimento verrà ubicato l'impianto?
2) In quale isola si è ipotizzata la realizzazione dello impianto?
3) Fornire una planimetria preliminare dell'impianto e relativi stoccaggi.
4) Gli stoccaggi sono previsti adiacenti all'impianto o presso un parco serbatoi separato?
5) Indicare, numero, capacità e ubicazione dei serbatoi situati sia in impianto che al parco serbatoi.
6) Come si prevede che verranno movimentate e con che frequenza le materie prime, ausiliari e prodotti?
7) Caratteristiche climatiche e topografiche della zona. In particolare procurarsi i dati relativi ad inonda - zioni e sismi.
8) Sono previsti sistemi di alimentazione di emergenza per:
   - energia elettrica?
   - acqua di raffreddamento?
   - inerti?
   - altri?
   - indicare quali.
9) Quali e quanti sistemi di fognatura sono previsti?
10) Quali sezioni dell'impianto è previsto realizzare al chiuso e quali all'aperto ed in base a quali criteri?

INDIVIDUAZIONE DELLE PERICOLOSITA' DI ORIGINE INTERNA

Quando il progetto di un impianto ha raggiunto uno stadio in cui risulta essere già sufficientemente delineato, si rende opportuno, se non necessario, sottoporlo ad una analisi volta ad evidenziare, in tutti i suoi aspetti, le modalità di realizzeazione dell'impianto stesso (con le eventuali modifiche da apportare allo schema) ed, in particolare, ad individuare i punti particolarmente critici che necessitano di uno studio più approfondito.

Un tale tipo di esame deve preferibilmente rispondere ad alcuni requisiti:

- deve essere sistematico: deve cioè essere compiuto su tutti i componenti del sistema seguendo un filo logico in modo da non tralasciare alcun punto che si possa trasformare nell'elemento debole del sistema;
- deve essere formalizzato: deve cioè essere condotto in modo prefissato e ripetibile in modo che a distanza di tempo sia ricostruibile passo a passo anche da persone diverse da quelle responsabili della primitiva stesura. E' importante inoltre che questa formalizzazione non si trasformi in mera burocrazia;
- deve coinvolgere il maggior numero di persone tra quelle partecipanti alla realizzazione del progetto in modo da consentire una discussione vivace e costruttiva.(26-28)

L'analisi di operabilità e l'analisi dei guasti soddisfano a tutti questi requisiti. I due metodi sono molto simili fra di loro: lo studio di operabilità, centrato sugli aspetti funzionali, è forse più idoneo per lo studio iniziale del progetto, mentre nell'analisi dei guasti prende maggior rilievo la realizzazione meccanica dell'impianto.

Entrambe le metodologie impiegano approcci di tipo discorsivo, sono facilmente comprensibili anche ai "non addetti ai lavori", non fanno ricorso a tecniche matematiche che possono presentare difficoltà per i non specialisti.

Il meccanismo intimo che sta alla base di ogni considerazione affidabilistica è però già presente. Si deve infatti procedere prima per via qualitativa per identificare gli eventi anomali; solo successivamente si potrà sviluppa-

re una metodologia quantitativa, che cerca di misurare effetti e conseguenze da una parte, frequenze dall'altra. In molti casi può rivelarsi non necessario giungere ad un esame quantitativo.

Analisi di Operabilità

L'analisi di operabilità consiste in una forma di esame critico basato sul fatto che un malfunzionamento od un problema sorga solo se ci si allontana dalle normali condizioni di esercizio. Quindi l'analisi di operabilità si propone di esaminare in modo sistematico ogni possibile deviazione dalle condizioni di regime e di ricercare le cause e le eventuali conseguenze di tale scostamento. A tale scopo vengono studiati, a secondo del grado di accuratezza richiesto, o il flow-sheet preliminare (analisi grossolana) o lo schema meccanico dell'impianto (analisi dettagliata).

Nell'analisi di operabilità l'attenzione si fissa essenzialmente sulla funzione che un particolare elemento dell'impianto svolge nel processo. occorre pertanto:

- decomporre l'impianto nei suoi elementi funzionali fondamentali (per esempio pompe per il trasferimento dei reagenti in un reattore, generatore Diesel per la produzione di energia elettrica,...);
- esaminare elemento per elemento quali possono essere le deviazioni da tali funzioni di progetto (portata elevata, quantità totale troppo bassa, ...);
- valutare quali sono le conseguenze e le possibili azioni correttive da intraprendere (allarme, entrata in esercizio di riserve, sistema di blocco, ...). (29)

Per quanto riguarda la metodologia da seguire essa fa ricorso ad alcune parole guida, cioè a certi vocaboli che hanno lo scopo di indirizzare e stimolare la mente dell'operatore nella ricerca delle deviazioni. Le più comuni fra tali parole guida sono riportate in Tabella 2.3. (26)

L'analisi di operabilità prosegue in pratica con la compilazione di una tabella la cui titolazione fa riferimento ad altre parole base di cui si dà la definizione nella Tabella 2.4.

In definitiva la sequenza dettagliata delle operazioni da eseguire per la stesura dell'analisi di operabilità è riportata in Fig. 2.4. (27-28)

Tab. 2.3 - Parole guida utilizzabili nell'analisi di operabilità. Esse sono da applicarsi alle "intenzioni" di progetto.(26,27)

- Non	indica una mancanza, è la negazione completa della funzione prevista;
- Più	indica un aumento della funzione in esame;
- Meno	indica una diminuzione della funzione in esame;
- Altro	indica una sostituzione, capita qualcosa di completamente diverso da ciò che ci si attendeva;
- Così come	indica un comportamento analogo a quello di un'altra funzione;
- Parte di	indica sostituzione parziale;
- Inverso	indica un'opposizione logica all'intenzione.

Tab. 2.4 - Significato dell'intestazione della tabella da compilarsi in un'analisi di operabilità.

- Intenzione: indica come ci si aspetta che operi la parte in esame, può essere descrittiva o diagrammatica;
- Deviazione: indica lo scostamento dall'intenzione, è ricavata tramite l'impiego sistematico delle parole guida;
- Cause : sono le ragioni per cui ha origine una deviazione. Ogni volta che una deviazione ha origine da una causa ragionevole e realistica va considerata come significativa;
- Conseguenze : sono i risultati della deviazione, indicano la possibilità di danno alle persone e alle cose;
- Azioni richieste: sono gli interventi che devono essere compiuti per controllare e rinormalizzare la situazione di emergenza.
  Possono essere automatici o manuali;
- Note e modifiche proposte allo schema: contengono annotazioni significative sulla deviazione in esame e sulle sue possibili cause e conseguenze.
  Riportano inoltre le variazioni da apportare allo impianto o al manuale operativo ai fini di aumentare la sicurezza.

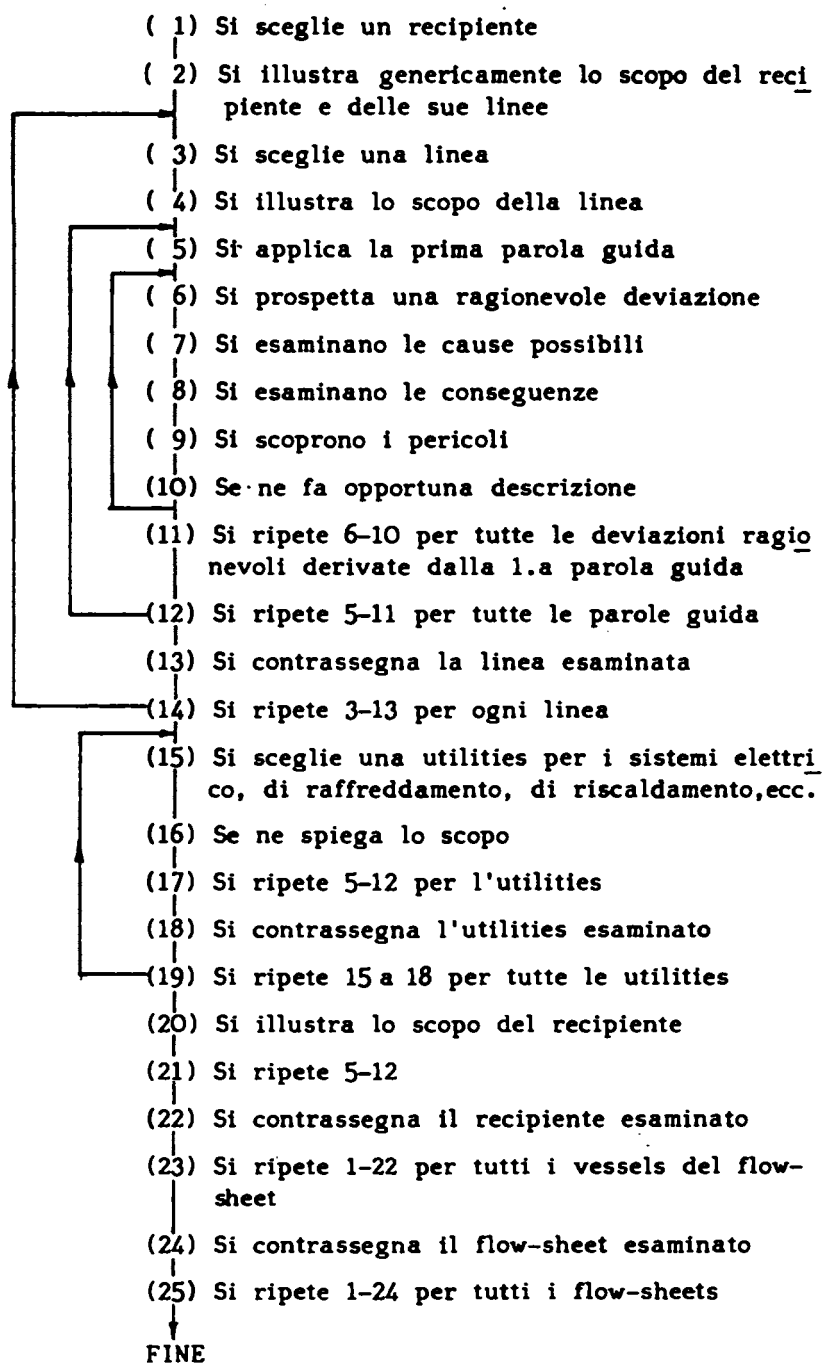


Fig. 2.4 - Sequenza delle operazioni da eseguire per la stesura di un'analisi di operabilità.(26, 27)

Un'esemplificazione chiarirà meglio il significato delle parole guida e il loro impiego.

Si consideri lo scarico del prodotto da un'autocisterna in un serbatoio, come mostrato schematicamente nella Figura 2.5. Uno studio di operabilità (parziale) potrebbe svilupparsi come indicato nella Tabella 2.5.

Analisi dei guasti

Con l'analisi dei guasti si intende la tecnica comunemente nota come Failure Modesand Effects Analysis (F.M.E.A.).

Questo metodo di analisi si sviluppa sulla base di un quesito classico che si pone chiunque voglia studiare le conseguenze di un evento: "che cosa fai...se...?" (What if...?)

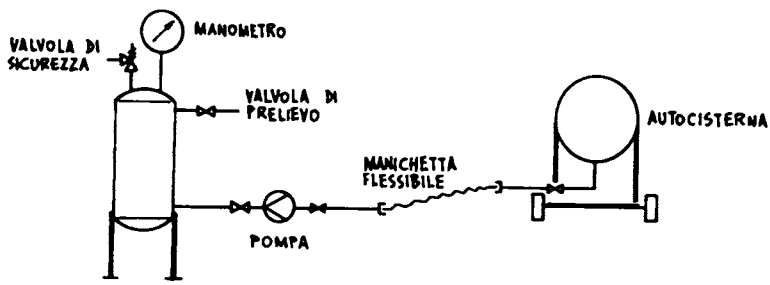


Fig. 2.5 - Scarico di un prodotto da un'autocisterna.(29)

(1) PAROLA GUIDA	(2) DEVIAZIONE	(3) CAUSE POSSIBILI	(4) CONSEGUENZE	(5) AZIONE RICHIESTA
Non	non vi è portata	— manichetta non collegata	non avviene il trasferimento	ricontrollare il circuito
		— pompa ferma	idem	idem
		— valvola chiusa	idem	idem
		— tubo tappato	idem	idem
Troppo	si trasferisce troppo prodotto	— indicatore livello guasto	fuoriuscita del prodotto dal troppo pieno	— controllo periodico dell'indicatore di livello
		— l'operatore non ha controllato il livello iniziale	idem	— rispetto delle procedure operative
Invece	si trasferisce prodotto errato	— si collega un'autocisterna errata	miscelamento di due prodotti	— rispetto delle procedure operative — identificazione delle manichette

Tab. 2.5 - Studio di operabilità (parziale) dello schema di Fig. 2.5.(29)

Questo quesito chiave è stato formalizzato in una metodologia che si sviluppa nei seguenti punti:

- identificazione di tutti i componenti che costituiscono sistemi individuali o che possono essere considerati tali;
- determinazione dei modi di guasto per ciascun componente e della sua pericolosità;
- determinazione, per ciascun modo di guasto, degli effetti su altri componenti il sistema;
- determinazioni degli effetti globali sul sistema;
- stima delle conseguenze di ciascun guasto.

Questo schema vale sia che si parta dalla considerazione del guasto di un componente, sia che si parta dal guasto di più componenti contemporaneamente. La caratteristica specifica di questo metodo è che il flusso logico di informazioni comincia con il guasto di uno o più componenti e si dirige verso l'evento finale, termine ultimo della sequenza.

In questo esame si fissa l'attenzione sul singolo componente fisico del sistema. Per ognuno si considerano tutti i possibili modi tramite i quali esso può "guastarsi", ossia deviare dal suo comportamento normale.

In pratica si procede nel modo seguente:

- si decompone l'impianto nei suoi componenti fisici (reattore, pompa di circolazione, regolatore di pressione...);
- si esaminano elemento per elemento le modalità di guasto possibili (foratura del reattore per corrosione, fermata della pompa di circolazione per mancanza di energia elettrica, regolatore di pressione starato...);
- si valutano per ognuno di questi guasti quali sono le manifestazioni, quali sono le possibili contromisure, e le conseguenze che ne derivano (formazione di un'atmosfera localmente esplosiva, entrata in servizio della pompa di riserva azionata a turbina, apertura della valvola di sicurezza...).

Ripetendo questo procedimento per ognuno degli elementi del sistema si ottiene un quadro abbastanza dettagliato del sistema.

Nella Tabella 2.6 è indicata l'analisi parziale di questo tipo, sviluppata per lo scarico di un prodotto da un'autocisterna a un serbatoio, il cui schema è già stato riportato in Fig. 2.5.

COMPONENTE	MODALITÀ DI GUASTO	MANIFESTAZIONE	AZIONE CORRETTIVA	CONSEGUENZE
Manichetta	— forata	fuoriuscita liquido	sostituzione manichetta	perdita all'esterno
	— tappata	il flusso non avviene o ha portata limitata	ricontrollo della manichatta	mancato o ridotto trasferimento
	— tipo arrato	=	=	corrosione a foratura; inquinamento del prodotto
Pompa	— non si avvia	pompa ferma	controllo alim. elettrica; controllo meccanico	non avviena il trasferimento
	— perdita dalla tenuta	fuoriuscita liquido	fermata a intercettazione della pompa	perdita all'asterno
	— lesione della carcassa	idem	idem	idem
Indicatore di livello	— intercettato	nessuna, salvo il caso di fuoriuscita del prodotto dal troppo pieno	controllo livello	se il serbatoio è pieno e vi si trasferisce prodotto, si ha fuoriuscita del prodotto

Tab. 2.6 - Analisi dei guasti dello schema di Fig. 2.5.(29)

L'analisi può essere ulteriormente approfondita, con l'obiettivo di classificare gli effetti dei guasti dei componenti. Gli effetti possono essere classificati secondo la gravità delle conseguenze, seguendo una graduatoria simile a quella riportata nella Tabella 2.7.

Come per lo studio di operabilità si esaminano le funzioni elementari dei diversi componenti, per una valvola di intercettazione si potrebbero avere le funzioni e le relative modalità di guasto, come quelle indicate nella Tab. 2.8.

Si procede nell'analisi similmente a quanto si è fatto nello studio di operabilità, compilando un modulo del tipo di quello mostrato nella Tabella 2.9.

Un importante parametro, che però non può essere stimato nella prima fase di indagine, è la stima della frequenza delle modalità di guasto.

Tab. 2.7 - Classificazione di gravità di guasti.(29)

CLASSE	DEFINIZIONE	CARATTERISTICHE
IV	molto modesta	il guasto del componente non provoca il blocco del sistema e non coinvolge il personale
III	modesta	il guasto del componente provoca il blocco del sistema, ma non coinvolge il personale
II	grave	il guasto non porta a danni importanti nel sistema, ma coinvolge il personale
I	molto grave	il guasto porta importanti danni al sistema o gravi lesioni al personale

Tab. 2.8 - Modalità di guasto di una valvola.

FUNZIONI ELEMENTARI DI UNA VALVOLA D'INTERCETTAZIONE	MODALITÀ DI GUASTO
Chiudere il flusso	rimane aperta chiude parzialmente
Pe.mettere il flusso	rimane chiusa apre solo parzialmente
Rimanere chiusa	apre completamente apre parzialmente
Rimanere aperta	chiude completamente chiude parzialmente
Contenere il fluido entro il sistema	perde verso l'esterno

Tab. 2.9 - Intestazione del modulo per un'analisi dei modi di guasto e dei loro effetti.

IMPIANTO ..... SISTEMA ..... COMPONENTE .....
condizioni iniziali .....
condizioni esterne .....

N.	FUNZIONE DELL'ELEMENTO	MODALITÀ DI GUASTO	MANIFESTAZIONE DEL GUASTO	AZIONE CORRETTIVA	EFFETTI	OSS.	CLASSE

VALUTAZIONE DELLA RISPOSTA DI UN IMPIANTO AL VERIFICARSI DI GUASTI O MALFUNZIONAMENTI

Il processo di identificare e descrivere le sequenze di eventi che si generano in un impianto in seguito al verificarsi di guasti o malfunzionamenti, è un complesso di procedimenti mentali sia di tipo induttivo che di tipo deduttivo.

Questi due tipi di procedimenti, complementari e in un certo senso in opposizione nella mente del medesimo analista, sono rappresentati efficacemente il primo dal diagramma causa/conseguenze o dall'albero degli eventi, il secondo invece dall'albero di guasto o diagramma conseguenza/ /cause.

L'albero di guasto è una sintesi grafica di un processo di pensiero induttivo: dal fatto che avvenga l'evento di riferimento ("top event"), cioè l'effetto visibile, si risale agli eventi primari, cioè si inducono gli eventi causali possibili.

Il diagramma causa/conseguenze e l'albero degli eventi hanno natura deduttiva. Anche in queste due metodologie gli effetti possibili (in termini di sequenze di eventi) di eventi causa sono espressi in forma grafica (alberi logici).

I metodi citati non sono in alternativa, ma possono integrarsi per effettuare in modo più approfondito, le analisi di rischio.In particolare il metodo degli "event trees" consentirà di identificare le sequenze di eventi da analizzare, mentre allo scopo di quantificare le probabilità di tali sequenze è utile sfruttare al massimo il metodo del "fault tree" (per evitare pesanti procedimenti manuali),che si presta a risoluzioni automatizzate con un calcolatore.

Il diagramma logico causa/conseguenze

Uno dei metodi sistematici per individuare le anomalie di sistemi è quello denominato diagramma causa/conseguenze.

Lo studio si effettua esaminando le possibili conseguenze di diverse cause. Possono essere cause di anomalie: guasti alle apparecchiature, errata manovra a un quadro di comando, fuoriuscita di sostanza infiammabile da una tubazione.

Per poter applicare il metodo occorre disporre di una descrizione dettagliata del sistema in esame, sotto forma di schema a blocchi o flow sheet, con l'indicazione di tutti i dettagli che si vogliono prendere in considerazione.

Non esistono convenzioni sulla simbologia da impiegare; in Fig.2.6 è riportata quella di Nielsen che ha sviluppato per primo il metodo (1974).

La causa in esame è detta evento iniziatore e nel grafico viene rappresentata simbolicamente da un rettangolo (nel riquadro la descrizione dell'evento).

Vengono utilizzate scatole decisionali, a un ingresso e due uscite, riferite a ogni componente del sistema in esame. l'ingresso è costituito dalla presenza di una situazione che richiede l'intervento del componente, cui è riferita la scatola decisionale. Le due uscite rappresentano le due situazioni che si hanno in conseguenza del verificarsi o meno dell'evento: per il verificarsi dell'evento SI, si intende il funzionamento del componente in modo corretto e conforme a specifica; il caso contrario è indicato con NO.

Il diagramma si sviluppa dall'alto verso il basso a partire dal simbolo dell'evento iniziatore. Vengono tracciate linee orientate, ciascuna delle quali rappresenta una possibile modalità di sviluppo. Un simbolo opportuno indica la conseguenza finale.

Nella figura sono indicati i simboli comunemente usati per la costruzione di questo diagramma. Si notino in particolare i significati delle porte AND, OR ESCLUSIVO e OR.

Il metodo viene esposto ora attraverso la presentazione di un esempio.

Si esamini il circuito elettrico rappresentato nella Fig. 2.7, costituito da una batteria, un interruttore e due lampade in parallelo.

Si supponga che la pila P, l'interruttore I, i fili di collegamento e le connessioni siano efficienti. A interruttore chiuso, che cosa succede se la lampada LI e/o la lampada L2 sono nello stato guasto? La risposta è elementare, ma serve a introdurre i diagrammi in studio.

Il diagramma mostrato nella Fig. 2.8 è chiaramente uno solo dei possibili che si possono costruire, avendo considerato come eventi iniziatori i guasti alle lampade ed esse sono soggette a possibili guasti.

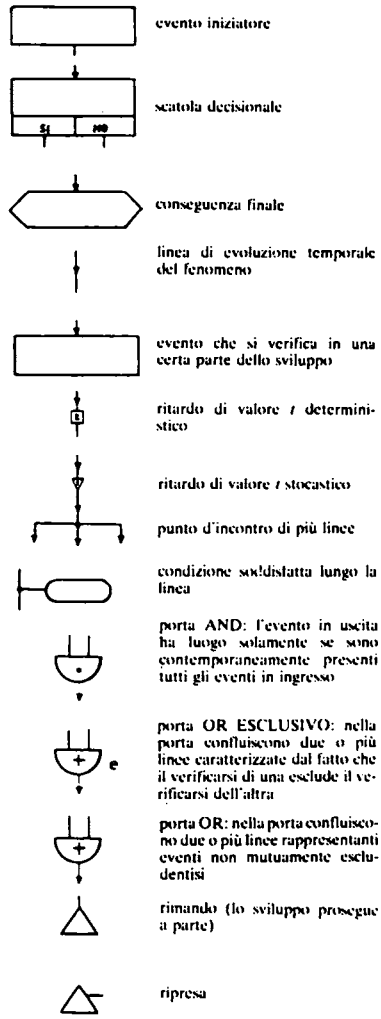


Fig. 2.6 - Simbologia di Nielsen per il diagramma causa/ /conseguenze.(13)

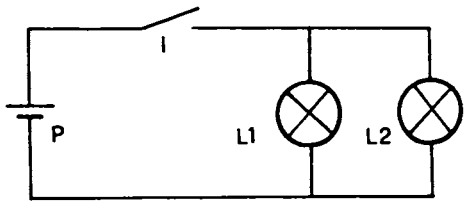


Fig. 2.7 - Schema di circuito elettrico.

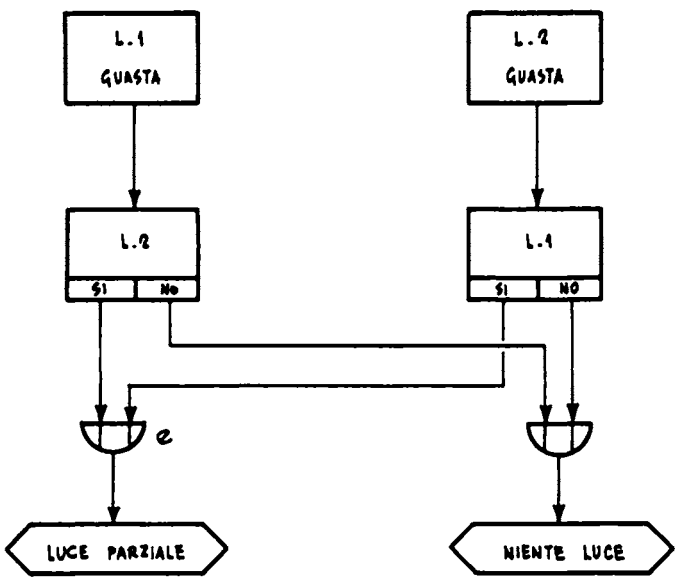


Fig. 2.8 - Diagramma causa/conseguenze del circuito elettrico di Fig. 2.7 (Sviluppo parziale).

La tecnica dei diagrammi causa/conseguenze è in linea di principio applicabile a tutti i problemi di analisi di affidabilità che si possono incontrare in pratica. Infatti con essa è possibile rappresentare compiutamente le evoluzioni nel tempo di qualsiasi sistema oppure di diversi sistemi coinvolti in uno stesso fenomeno.

Per problemi di una certa complessità l'utilizzo di questo metodo, tuttavia, non risulta più vantaggioso a causa dell'eccessiva complessità del modello grafico; l'utilizzo si rivela di grande utilità (e probabilmente senza alternative) ove occorra eseguire valutazioni estremamente dettagliate di sistemi, semplici dal punto di vista della numerosità dei componenti, quanto si voglia complessi dal punto di vista delle caratteristiche di funzionamento e della natura dei collegamenti.

A titolo esemplificativo si riporta in Fig. 2.9 uno studio della Total sui rischi legati alla perforazione di più pozzi dalla stessa piattaforma.

Con questa metodologia si possono studiare due categorie di problemi.

Il primo gruppo comprende quei problemi in cui la durata dei fenomeni analizzati è relativamente limitata, per cui la variabile tempo non rientra se non con un significato di successione. Il concatenamento fra gli eventi è in pratica esclusivamente logico.

Problemi tipici di questo tipo sono quelli in cui si ipotizza il malfunzionamento dei componenti: l'applicazione del metodo consente di evidenziare con chiarezza tutti i possibili modi di sviluppo dell'anomalia, a seconda di come si comportano i sistemi di protezione predisposti a intervenire. Può rientrare in questa categoria anche lo studio delle conseguenze di un evento grave e rapido, come lo scoppio di un reattore.

Il secondo gruppo comprende quei problemi in cui la durata dei fenomeni è rilevante. Si pensi per esempio a guasti a cui è possibile rimediare con interventi di servizi ausiliari in stand-by e all'evoluzione di un incendio secondo l'efficacia dei diversi interventi dei sistemi di protezione.

Il diagramma può servire inoltre per uno studio non semplicemente qualitativo, ma di tipo quantitativo.

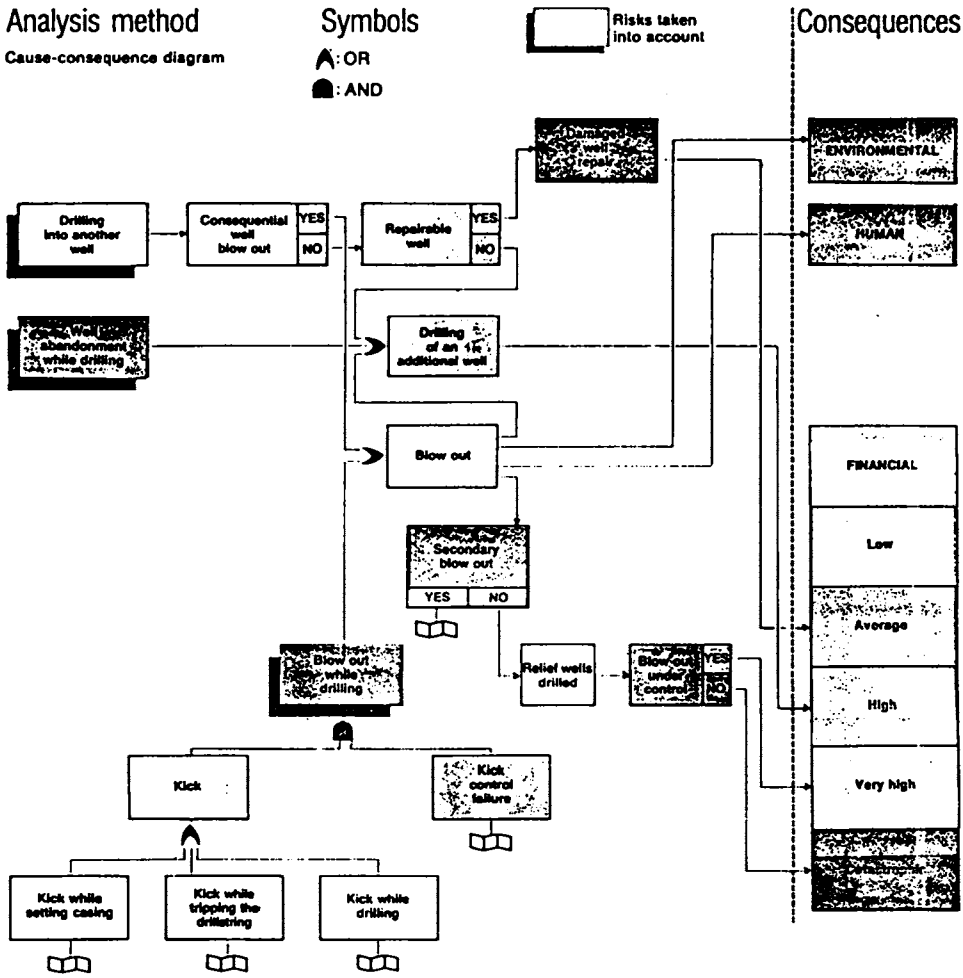


Fig. 2.9 - Studio sui rischi legati alla perforazione. di più pozzi da una stessa piattaforma.

Albero degli eventi

La quantificazione del rischio d'impianto può richiedere l'esplicitazione di un grosso numero di sequenze di eventi e pertanto si pone l'esigenza di un approccio ordinato e sistematico che consenta di valutare correttamente i molti fattori che potrebbero influenzare il corso dei potenziali incidenti.

La struttura tipica di un albero degli eventi è quella mostrata in Fig. 2.10. Partendo da un "evento iniziatore" l'albero si sviluppa a seconda del successo o del fallimento dei componenti, sistemi o funzioni necessari per mitigare le conseguenze dell'evento stesso, in relazione con il parametro di rischio prescelto nello studio.

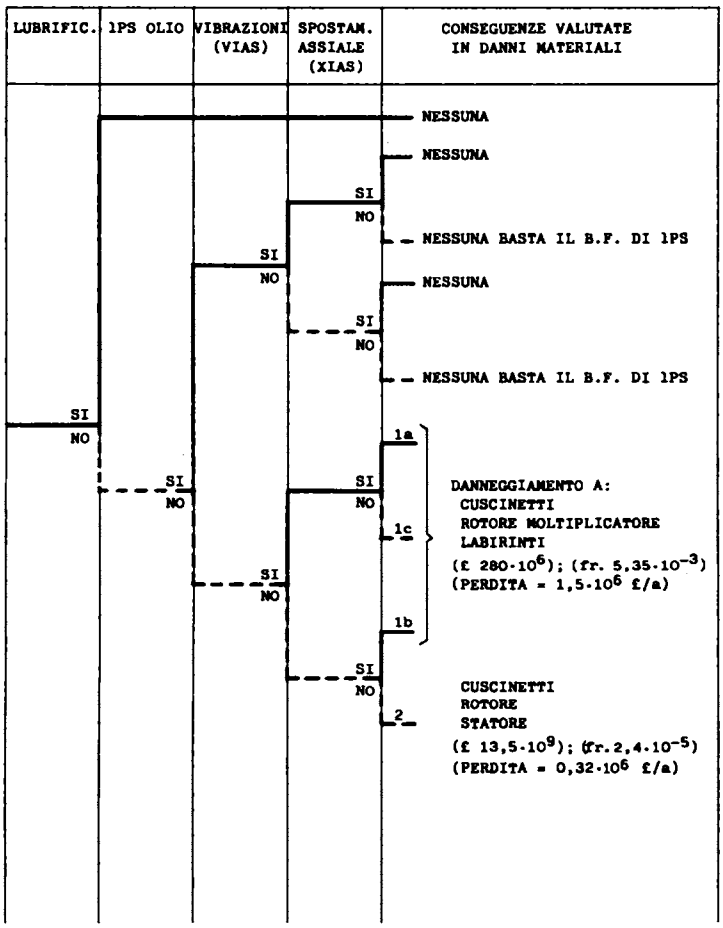
Particolare cura bisogna porre per assicurare che gli eventi che costituiscono le intestazioni dell'albero (nodi dell'albero) siano consistenti con i reali modi di risposta dell'impianto e possano essere precisamente correlati a criteri di successo dei sistemi. Tali criteri saranno poi in seguito utilizzati per definire gli eventi iniziali, "top event", degli alberi dei guasti.

Il posizionamento degli eventi nell'albero (nodi) si basa sia sulla sequenza temporale, sia su un ordine logico che rispecchia le interdipendenze operazionali.

Le varie sequenze sono rappresentate dai camini che si sviluppano seguendo le linee verticali ed orizzontali in corrispondenza degli eventi. Ad un punto di congiunzione, per convenzione, il sistema ha successo se la linea verticale va verso l'alto.

La funzione dell'esempio mostrato in Fig. 2.10, è unicamente quello di illustrare la logica adottata nello sviluppo degli alberi degli eventi, mettendo in evidenza come la metodologia adottata permetta di ridurre ampiamente il numero delle possibili sequenze incidentali che richiedono una analisi di maggior dettaglio.

Poiché, per definizione, un evento iniziatore è il punto iniziale della sequenza incidentale, è necessario innanzi tutto compilarne una lista esauriente al fine di garantire che un'analisi con gli alberi degli eventi contenga tutte le sequenze incidentali di maggior rilevanza.



- SI = Buon Funzionamento
- NO = Mancato Funzionamento
- tratteggiate le vie di insuccesso
- a tratto continuo le vie di successo
- 1PS pressostato sul collettore di mandata olio di lubrificazione
- VIAS misura di vibrazioni
- XIAS misura di spostamento assiale
- MF mancato funzionamento

L'insieme delle combinazioni danno luogo a 8 conseguenze, di queste solo 4 comportano danni materiali.

I percorsi da analizzare sono quindi i seguenti:

- percorso *1a* dovuto a MF di 1PS
- percorso *1b* dovuto a MF di 1PS + VIAS
- percorso *1c* dovuto a MF di 1PS + XIAS
- percorso *2* dovuto a MF di 1PS + VIAS + XIAS

Fig. 2.10 - Albero degli eventi relativo ad un compressore centrifugo; top event = danno per insufficiente lubrificazione.

Il processo di selezione degli eventi iniziatori consta fondamentalmente di due stadi:

1. Definizione degli eventi possibili.
2. Categorizzazione degli eventi iniziatori identificati, in base o alle funzioni richieste per la loro mitigazione o alle possibili risposte del sistema.

Si possono individuare fondamentalmente due approcci. Il modo forse più corretto per l'identificazione degli eventi iniziatori è quello di prendere in esame le informazioni da una precedente analisi di operabilità. Tali informazioni sono poi elaborate e ordinate in una lista di eventi iniziatori.

Una volta che gli eventi iniziatori sono stati identificati e raggruppati, è necessario determinare la risposta dell'impianto a ciascuna categoria di eventi.

Vari sono i metodi per organizzare logicamente e temporalmente questo tipo di analisi sull'impianto. Molto utile è lo sviluppo di un albero funzionale per ciascuna categoria di eventi iniziatori, come passo intermedio per identificare le complesse relazioni tra gli eventi iniziatori stessi e la risposta dei sistemi mitigatori. L'albero funzionale viene costruito considerando le funzioni richieste per prevenire il danno all'impianto e per ridurre le eventuali conseguenze mettendo in evidenza le relazioni tra le funzioni richieste.

Ciascuna funzione di sicurezza rappresentata da un nodo dell'albero funzionale è garantita da un insieme di sistemi. Alcuni sistemi possono adempiere più di una funzione o porzioni di svariate funzioni, a seconda del progetto dell'impianto.

Vi sono poi sistemi, quali i sistemi di acque di raffreddamento o i sistemi di distribuzione dell'energia elettrica, che spesso non adempiono direttamente alcuna funzione specifica in relazione agli eventi considerati, ma che possono contribuire significativamente all'indisponibilità dei sistemi o gruppi di sistemi che sono preposti al diretto adempimento delle funzioni specifiche per l'evento.

E' opportuno sottolineare che l'intero sviluppo degli alberi degli eventi è essenzialmente un processo iterativo: l'identificazione e la categorizzazione degli eventi iniziatori viene modificata e aggiornata col raffinamento delle informazioni dovuto al procedere del lavoro.

Il diagramma logico conseguenza/cause

Analogo al diagramma causa/conseguenze è il diagramma conseguenza/cause. Esso esprime graficamente, per un certo sistema, le connessioni logiche tra gli eventi-causa e l'evento-conseguenza.

L'albero di guasto, come è anche chiamato il metodo, consiste quindi in un diagramma che identifica tutte le sequenze di eventi che possono portare al verificarsi di uno specificato evento pericoloso. Il metodo si articola nei seguenti punti:

- identificazione dell'evento finale pericoloso che interessa, detto anche "Top Event";
- stima delle conseguenze di questo evento;
- identificazione, nel contesto del sistema e dei suoi dintorni, degli eventi precursori dell'evento finale;
- tale identificazione deve essere continuata fino all'individuazione degli eventi iniziatori, detti eventi primari;
- assegnate delle probabilità agli eventi primari, si può calcolare infine la probabilità che l'evento finale si verifichi.

La caratteristica specifica di questo metodo è che il flusso logico di eventi comincia con il Top Event e termina con gli eventi primari.

L'analisi tramite l'albero di guasto parte da una conseguenza (un'anomalia di funzionamento, uno scoppio, un incendio...) e si sviluppa alla ricerca degli eventi-causa che l'hanno provocata, evidenziando con porte AND, OR ESCLUSIVO e OR i tipi di legame logici tra i vari eventi. Per lo studio è necessario disporre di una descrizione dettagliata del sistema da sottoporre ad analisi (flow sheet).

Non esiste convenzione comunemente adeguata per la simbologia da adottare. Nel seguito si userà quella riportata in Fig. 2.11. Per chiarezza alcune volte saranno specificate le porte anche con la scritta di richiamo AND od OR. Il metodo viene esposto attraverso la presentazione di alcuni esempi.

Si consideri il circuito elettrico mostrato nella Fig. 2.7 e costituito da un generatore, un interruttore e due lampade in parallelo. Si prende come top event l'assenza totale di luce a interruttore chiuso, considerando come possibili eventi primari il guasto al generatore, all'inter

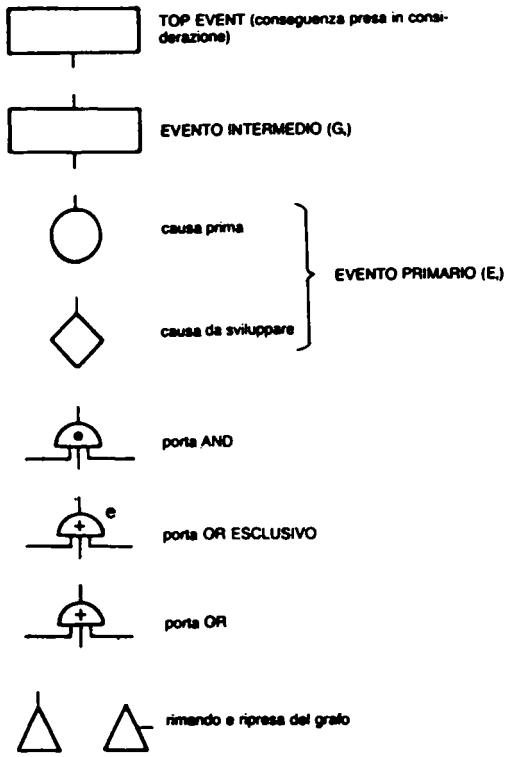


Fig. 2.11 - Simbologia relativa all'albero di guasto.(13)

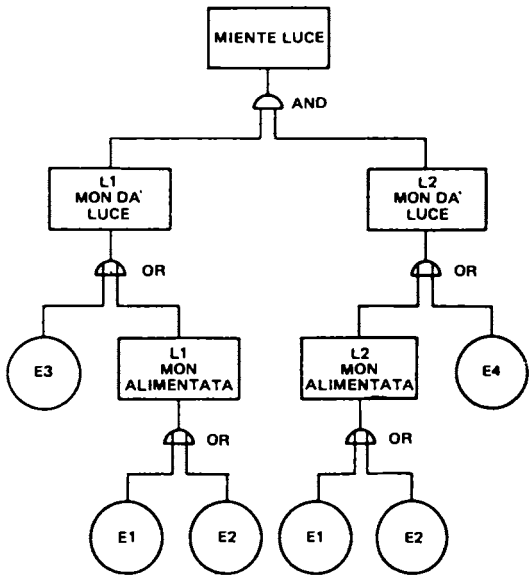


Fig. 2.12 - Albero di guasto relativo al circuito elettrico di Fig. 2.7.
Eventi primari: E1 = pila guasta; E2 = interruttore guasto; E3 = lampada L1 guasta; E4 = = lampada L2 guasta.

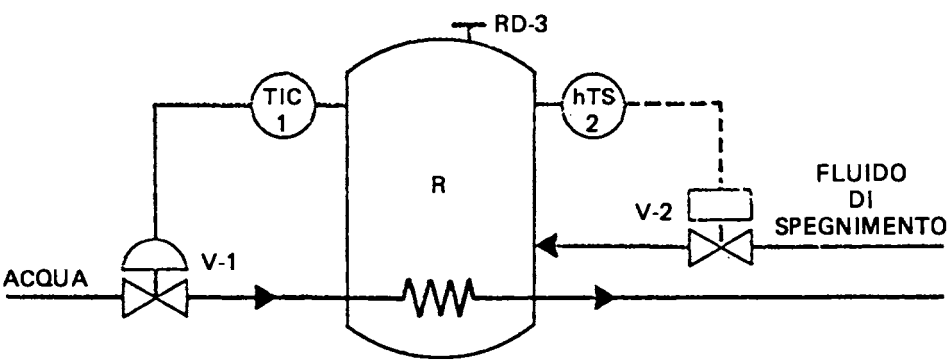


Fig. 2.13 - Schema di reattore chimico.(10)

ruttore e alle due lampade (e non, per esempio, ai fili, ai connettori,...). L'albero di guasto di questo sistema è mostrato nella Fig. 2.12.

Facciamo un altro esempio: si voglia determinare la frequenza probabile di cedimento meccanico del reattore R, schematizzato nella Fig. 2.13.

Nel reattore R avviene una reazione che comporta un aumento della temperatura e della pressione; la reazione è normalmente controllata asportando calore a mezzo dell'introduzione di acqua fredda, la cui quantità è regolata a mezzo del regolatore TIC-1 e della valvola V-1. Come ulteriore sicurezza, nel caso la reazione tenda a sfuggire, il reattore viene inondato da un fluido di spegnimento attraverso la valvola V-2, su comando del termostato hTS-2.

Ove il sistema di spegnimento non funzioni e quindi la pressione interna tenda a salire a valori pericolosi, il disco di rottura RD-3 aprirà uno sfogo verso l'esterno, prima che la pressione raggiunga il valore di rottura del recipiente del reattore.

E' a priori assai difficile rispondere alla domanda: "Quale è la probabilità che il reattore ceda?", in quanto l'evento disastroso è fortunatamente così raro che richiederebbe un periodo di indagine statistica assai lungo (centinaia o migliaia di anni) e comunque sarebbe assurdo l'attendere che si verifichi proprio quanto si vorrebbe impedire.

Si può notare però come l'evento finale sia scomponibile in una serie di eventi elementari logicamente concatenati, abbastanza individuati ed abbastanza frequenti da poter essere analizzati statisticamente.

Così, ad esempio, possiamo scrivere che perché avvenga l'esplosione di R occorre che (1°) la pressione interna superi il valore limite e contemporaneamente (2°) il disco di rottura non apra; o graficamente come rappresentato in Fig. 2.14a.

Perché la pressione superi il valore limite occorre poi che (1°) l'acqua sia introdotta in quantità insufficiente e contemporaneamente (2°) non funzioni il sistema di spegnimento (Fig. 2.14b).

Se poi consideriamo l'evento "Sistema di spegnimento non funziona" lo stesso può dipendere da vari eventi elementari in alternativa: (1°) il termostato hTS-2 è guasto oppu

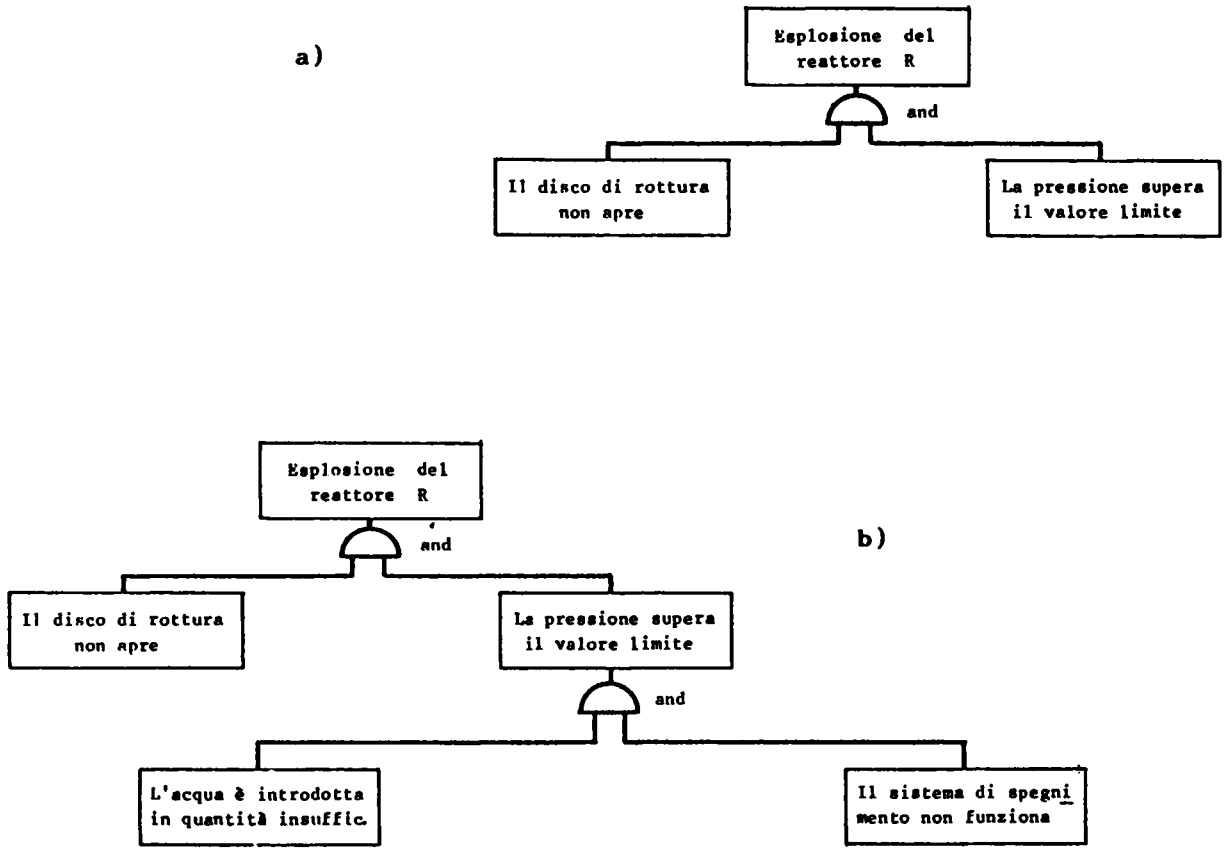


Fig. 2.14 - Stadi successivi per costruire l'albero di guasto del reattore di Fig. 2.13.

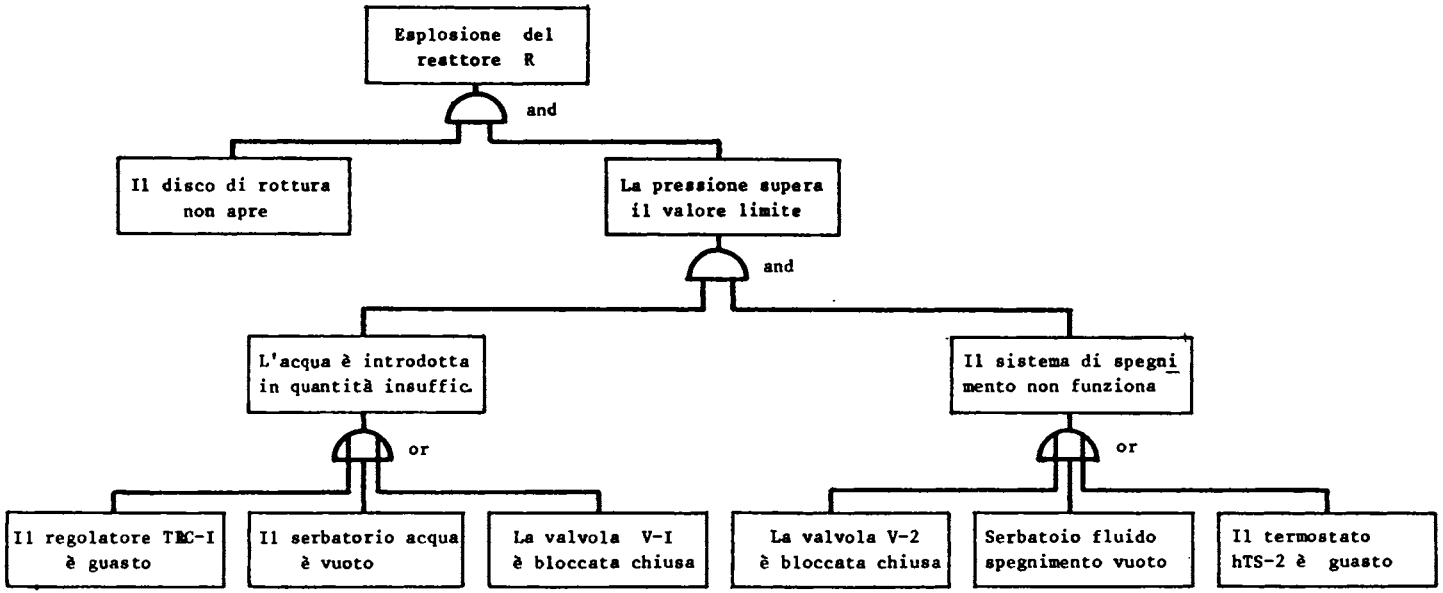


Fig. 2.14 - Stadi successivi per costruire l'albero di guasto del reattore di Fig. 2.13.

re (2°) la valvola V-2 è bloccata chiusa oppure (3°) il serbatoio del fluido di spegnimento è vuoto, ecc.

Analogamente si può scomporre l'evento "Acqua introdotta in quantità insufficiente" in eventi elementari, ottenendo la struttura logica finale riportata in Fig. 2.14c.

Questo procedimento di scomposizione può continuare fino a raggiungere eventi elementari abbastanza individuati ed abbastanza frequenti da poter essere analizzati statisticamente. L'evento finale disastroso è normalmente indicato come "Top Event", gli eventi elementari come "Foglie", la struttura logica che li lega come "Albero di guasto".

L'importante risultato ottenuto è che, ove si riescano a quantizzare le frequenze attese degli eventi elementari, si può risalire alla frequenza attesa dell'evento disastroso finale, che sarebbe impossibile definire a priori senza questo processo di scomposizione logica.

Ad ogni modo, la costruzione dell'albero anche solo qualitativo permette di approfondire la conoscenza di un sistema in esame, ne favorisce un uso appropriato e al tempo stesso, agevola la tempestiva diagnosi di eventuali anomalie.

L'albero di guasto pone in evidenza le connessioni logiche fra gli eventi-causa e l'evento-conseguenza in un dato sistema ed è un utile strumento per studiare e migliorare l'affidabilità del sistema stesso: il suo esame permette di evidenziare le varie sequenze di eventi che portano al top event, di confrontarle fra loro e individuare quelle sequenze (path), che preferenzialmente portano all'evento finale, in quanto costituite da eventi meno numerosi e/o più suscettibili di manifestarsi. La modifica di tali sequenze, realizzata mediante opportuni interventi sul sistema, permette di rendere più difficile il verificarsi del top event.

Solo in possesso di un diagramma sicuro e disponendo di dati affidabili si può procedere a un'analisi di tipo quantitativo.

STIMA DELLA FREQUENZA DI EVENTI

Nell'esame delle diverse metodologie dell'affidabilità si è fatto finora riferimento esclusivamente a considerazioni di tipo qualitativo. Per procedere a un'analisi quantitativa è necessario disporre di metodi matematici quali la logica, il calcolo delle probabilità, la statistica.

Si ritiene opportuno fare rapidissimi cenni ad alcuni di questi argomenti e indicare le formule di uso più comune.

Dopo un cenno agli insiemi sono richiamate le regole dell'algebra logica, che permettono di scrivere relazioni relative a diagrammi logici (diagramma causa/conseguenze, albero di guasto). Per un albero di guasto le relazioni logiche possono essere utilizzate per due scopi:

- ottenere, in base all'applicazione dell'algebra di Boole, le condizioni di successo o di insuccesso del top event;
- valutare la probabilità che il sistema si trovi, per esempio, nello stato guasto, in funzione della probabilità che vi si trovino gli elementi nei quali il sistema è stato decomposto.

Richiami sugli insiemi e l'algebra logica

Insiemi

Si chiama insieme una raccolta di elementi M, N, ... che possono rappresentare oggetti, enti, situazioni,... e si scrive:

$$I = \{M, N, \ldots\}$$

Ad esempio:

I1 = (numero 13)
I2 = (pompa n. 1, pompa n. 2, pompa n. 3)
I3 = (Diesel in esercizio, Diesel fermo, Diesel in riparazione, Diesel in manutenzione).

Relazioni fra insiemi

A = B Gli elementi di A e di B sono gli stessi.
A $\subset$ B Tutti gli elementi di A sono compresi fra gli elementi di B. Si dice A sottoinsieme o parte di B.

Operazioni fra insiemi

R = A + B. L'insieme R è formato dagli elementi di A e di B. L'operazione si dice somma logica o unione. Il segno di somma viene spesso indicato con OR: questo ricorda che ogni elemento di R appartiene ad A oppure a B oppure a entrambi.

S = A $\oplus$ B. E' pure una somma logica, indicata con EOR o OR esclusivo: ogni elemento di S appartiene ad A oppure a B,ma non a entrambi.

T = A . B o semplicemente T = AB.

L'insieme T è il prodotto logico di A e di B o intersezione dei due insiemi. Il segno di moltiplicazione viene spesso indicasto con AND: questo ricorda che ogni elemento di T appartiene ad A e a B.

Le operazioni indicate possono essere eseguite anche fra gli elementi di un insieme.

E' conveniente introdurre qualche altra defínizione e altri simboli, e precisamente:

U Universo. E' l'insieme contenente tutti i possibili elementi del problema in esame.

$\overline{A}$ Insieme complemento di A, tale che $\overline{A} + A = U$.
Il simbolo $\overline{A}$ si legge NON A e l'operazione, detta qualche volta negazione, si può indicare con NOT.

$\emptyset$ Insieme vuoto. E' l'insieme che non contiene alcun elemento.

In relazione a quanto è stato sopra definito si ha:

$$A + \emptyset = A$$
$$A.\emptyset = \emptyset$$
$$U + A = U$$
$$U.A = A$$

Inoltre se $A.B = \emptyset$ i due insiemi A e B si dicono mutuamente escludentisi o disgiunti. Gli insiemi, in questo caso, non hanno alcun elemento in comune. E' facile estendere questi concetti a più insiemi. In particolare si ricorda che i sottoinsiemi E1, E2, ... En formano una partizione S se:

$$S = E1 + E2 + \ldots En$$

$$Ei \; . \; Ej = \emptyset$$

per $i \neq j$ (cioè i sottoinsiemi sono, a coppie, mutuamente escludentisi).

Algebra logica

Con gli insiemi A, B, ... o con gli elementi di un insieme si può sviluppare un'algebra logica analoga all'algebra corrente. Molte relazioni delle due algebre sono formalmente uguali, altre non lo sono per la diversa definizione delle operazioni somma e prodotto.

Valgono le proprietà commutativa, associativa e distributiva, che si possono scrivere:

$$A.B = B.A$$
$$A + B = B + A$$
$$A.(B.C) = (B.C).A$$
$$A + (B + C) = (A + B) + C$$
$$A.(B + C) = A.B + A.C$$

Ma, attenzione:

$$A + A = A$$
$$A + A.B = A$$
$$A.A = A$$

Applicando le regole dell'algebra logica si possono eseguire "semplificazioni". Così, per esempio:

$$A + A.B + B.C + A.B.C =$$
$$= A + A.B + A.B.C + B.C = A + B.C$$

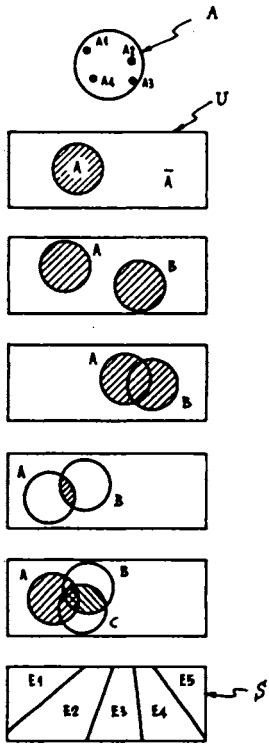
E' valida la legge di dualità: se a due elementi di un'operazione logica si sostituiscono i complementi e se si scambia il prodotto logico con la somma e viceversa, il risulta to non cambia. Di particolare importanza i due teoremi di Morgan:

$$\text{I} \quad \overline{(A + B)} = \overline{A.B}$$
$$\text{II} \quad \overline{(A . B)} = \overline{A} + \overline{B}$$

I diagrammi di Venn

Per ricordare le regole elementari dell'algebra logica e verificare rapidamente molti teoremi è conveniente riferirsi ai diagrammi di Venn.

In questa rappresentazione gli elementi di un insieme sono indicati da punti di un piano e l'insieme da una figura chiusa (spesso un cerchio) che li racchiude. L'universo è indicato spesso con un rettangolo. Alcuni esempi sono mostrati nella Fig. 2.15.



A = {A1, A2, A3, A4}

U = A + $\bar{A}$

A e B, insiemi mutuamente escludentisi o disgiunti

S = A + B (parte tratteggiata)

T = A·B (parte tratteggiata)

K = A + B·C (si noti che i due termini A e B·C, indicati con tratteggi diversi, non sono disgiunti)

E1, E2, E3, E4 ed E5 sono una partizione dell'insieme S

Fig. 2.15 - Diagrammi di Venn.(32)

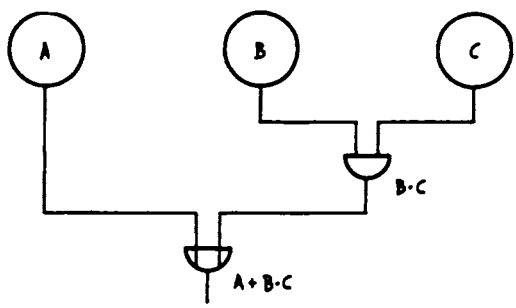


Fig. 2.16 - La relazione A + B . C espressa con un albero logico.

Per relazioni fra più di due insiemi i diagrammi di Venn risultano di difficile lettura, per cui è conveniente ricorrere a grafici in cui si collegano insiemi diversi con porte di tipo AND, OR ESCLUSIVO e OR, come già visto nel capitolo precedente.

Così l'espressione A + B.C può essere rappresentata come nella Fig. 2.16. Viceversa dallo schema si può risalire all'espressione logica.

Uno schema di questo tipo si chiama diagramma di flusso o, con espressione molto felice, albero logico.

L'algebra binaria o di Boole

In molte questioni di affidabilità per ogni evento sono considerati possibili solo due stati: uno strumento, per esempio, può essere considerato efficiente oppure guasto. Questo modo di schematizzare è in generale una grossolana idealizzazione, che risulta però estremamente vantaggiosa nella trattazione di molti problemi.

Esiste una logica binaria, detta comunemente algebra da Boole, che considera esclusivamente enti a due valori, indicati con i simboli 1 e 0. Così si possono indicare con:

1 il verificarsi di un evento (luce accesa, componente efficiente, apparecchiatura guasta, ...);
0 non verificarsi dell'evento (luce spenta, componente non efficiente, apparecchiatura funzionante,...).

Applicando le regole dell'algebra logica si ricava facilmente la seguente tavola delle operazioni elementari, per il caso a due valori:

1 + 1 = 1	0 • 0 = 0
1 + 0 = 1	0 • 1 = 0
0 + 1 = 1	1 • 0 = 0
0 + 0 = 0	1 • 1 = 1

L'analisi diretta attraverso l'albero di guasto

L'analisi dell'albero di guasto, condotta solo da un punto di vista qualitativo diventa quantitativa immediatamente se si utilizzano le formule base dell'affidabilità e si fa uso delle relazioni che danno le frequenze e/o le probabilità nel caso della combinazione di più eventi tramite somma o prodotto logico.

Si riprenda l'albero di guasto relativo al circuito elettrico di illuminazione, presentato in Fig. 2.7. Esso è riprodotto introducendo i simboli E (top event) e G (gate) ai risultati delle operazioni logiche in Fig. 2.17.

La trascrizione dell'albero risulta, passo per passo:

$$G1 = E1 + E2$$
$$G2 = E1 + E2$$
$$G3 = E3 + G1 = E1 + E2 + E3$$
$$G4 = E4 + G2 = E1 + E2 + E4$$
$$E = G3 \cdot G4 = (E1 + E2 + E3) \cdot (E1 + E2 + E4)$$

Ricordando le regole dell'algebra logica si ottiene:

$$E = (E1 + E2) \cdot (E1 + E2) + (E1 + E2) \cdot E4 + E3 \cdot (E1 + E2) + E3 \cdot E4 =$$
$$= (E1 + E2) + (E1 + E2) \cdot (E3 + E4) + E3 \cdot E4 =$$
$$= E1 + E2 + E3 \cdot E4 \qquad (1)$$

Per via di alcune considerazioni che si faranno successivamente, la (1), per la legge di dualità, si può scrivere:

$$\overline{E} = \overline{E1} \cdot \overline{E2} \cdot \overline{(E3 \cdot E4)}$$

e, per il II teorema di MORGAN:

$$\overline{E} = \overline{E1} \cdot \overline{E2} \cdot (\overline{E3} + \overline{E4}) \qquad (2)$$

Introducendo i nuovi simboli:

$$K = \overline{E}$$
$$K1 = \overline{E1}$$
$$K2 = \overline{E2}$$
$$K3 = \overline{E3}$$
$$K4 = \overline{E4}$$

la (2) risulta quindi:

$$K = K1 \cdot K2 \cdot (K3 + K4) \qquad (2 \text{ bis})$$

L'algebra binaria permette di dare un'interpretazione chiara e persuasiva dell'albero di guasto, riportato nella Fig. 2.17.

Ponendo infatti la seguente corrispondenza:

pila guasta $E1 \longrightarrow 1$ oppure $K1 \longrightarrow 0$
pila efficiente $E1 \longrightarrow 0$ oppure $K1 \longrightarrow 1$

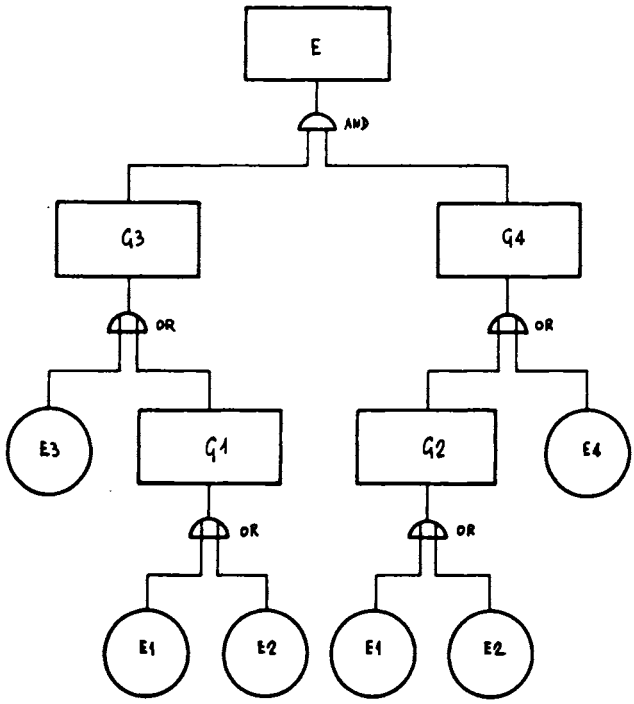


Fig. 2.17 - Albero di guasto del circuito elettrico di Fig. 2.7.

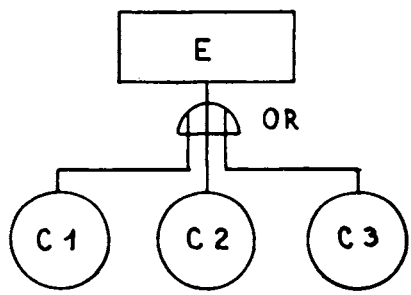


Fig. 2.18 - Albero di guasto ridotto agli insiemi minimi di taglio del circuito di Fig. 2.7.

La relazione (1) può essere "letta": "a interruttore chiuso non ho luce se o la pila è guasta o l'interruttore è guasto oppure entrambe le lampade sono guaste", mentre la (2 bis) dice: "a interruttore chiuso ho luce se la pila, lo interruttore e almeno una delle due lampade sono efficienti".

Naturalmente per conoscere il valore numerico della frequenza di accadimento del top event, occorre conoscere i valori dei ratei di guasto, delle indisponibilità ...nonché i parametri caratteristici della manutenzione (come, per esempio, la distanza di tempo fra un test e il successivo per un'apparecchiatura che dà un guasto che non si autodenuncia).

Se l'albero è di modeste proporzioni - con un numero ridotto di "porte" e un piccolo numero di "eventi primari" che non si ripetono, e si suppongono costanti nel tempo tutti i parametri - l'elaborazione è immediata. Si tratta sostanzialmente di effettuare, partendo dalle frequenze dei guasti e/o dalle indisponibilità, somme e prodotti e giungere in tal modo, risalendo dagli "eventi primari" al top event, alla frequenza dello stesso.

Anche in questa forma l'analisi può essere di grande aiuto al progettista, non tanto per avere il valore assoluto di una frequenza, quanto per fare confronti fra "rami" dell'albero rappresentanti sistemi diversi (di regolazione, di controllo, di protezione...). Anzi si suggerisce di procedere proprio in questo modo, prima di applicare metodi più sofisticati. L'analisi così condotta affina la sensibilità del progettista nello sviluppo della sua attività.

L'analisi di tipo logico dell'albero di guasto

Se l'albero è imponente - con molte "porte" e centinaia di eventi primari, molti dei quali si ripetono in più "rami" e i parametri sono funzione dell'età dei componenti - la procedura diretta è praticamente impossibile da applicare.

Si ricorre in questo caso a una particolare analisi di tipo logico. Per la sua comprensione è conveniente richiamare il concetto di "tavola della verità", attraverso l'applicazione di un esempio.

Si consideri il solito circuito elettrico schematizzato nella Fig. 2.7 e costituito da una pila P, un interrut

tore I e da due lampade L1 ed L2 in parallelo. Questi sono gli unici componenti che sono considerati nel seguito; si supponga ancora che essi possano trovarsi (indipendentemente) nello stato efficiente (1) o nello stato guasto (0).

Si dica successo del sistema l'avere luce a interruttore chiuso (K = 1) e insuccesso il contrario (K = 0). Siano K1 , K2, K3 e K4 gli eventi associati all'efficienza della pila, dell'interruttore e delle lampade L1 e L2: si indicherà 1 per dire efficiente e 0 per dire stato guasto dei singoli componenti.

Si considerino tutte le $2^4 = 16$ combinazioni degli stati possibili dei 4 componenti del sistema: da queste ha origine la "tavola della verità", mostrata nella Tab. 2.10.

Delle 16 combinazioni, o insiemi di stati dei componenti, 3 danno successo e 13 insuccesso o "taglio" (come si usa dire nella teoria degli insiemi). Alcuni di questi insiemi possono essere considerati critici.

Ci sono due categorie di insiemi critici:

a) gli insiemi di successo, tali che basta che uno qualsiasi dei componenti efficienti passi allo stato guasto,perché lo stato finale passi da successo a insuccesso:vengono chiamati insiemi minimi di successo (minimal success set);

b) gli insiemi di insuccesso, tali che basta che uno qualsiasi degli elementi guasti diventi efficiente, perché il sistema passi da uno stato di insuccesso a uno di successo: vengono chiamati insiemi minimi di taglio (minimal cut set).

Nel caso particolare in esame le combinazioni 14 e 15 sono insiemi minimi di successo e le combinazioni 8, 12 e 13 insiemi minimi di taglio. Si confrontino questi risultati con le relazioni logiche:

$$K = K1 \cdot K2 \cdot (K3 + K4) \qquad (K = 1 \text{ successo})$$

$$E = E1 + E2 + E3 \cdot E4 \qquad (E = 1 \text{ insuccesso})$$

e l'albero di guasto, riportato per esteso in Fig. 2.17.

In base a queste considerazioni l'albero originale può essere "sfoltito", riducendolo a quello mostrato nella Fig. 2.18 ove C1 = E1, C2 = E2 e C3 = E3 . E4 sono gli insiemi minimi di taglio.

La generalizzazione del risultato precedente è immediata. Dall'esame di un albero di guasto in cui il top event

Tab.2.10 - Tavola della verità relativa al circuito di cui alla Fig. 2.7.

P	I	L1	L2	sistema	
0	0	0	0	0	
0	0	0	1	0	
0	0	1	0	0	
0	0	1	1	0	
0	1	0	0	0	
0	1	0	1	0	
0	1	1	0	0	
0	1	1	1	0	
1	0	0	0	0	
1	0	0	1	0	
1	0	1	0	0	
1	0	1	1	0	
1	1	0	0	0	
1	1	0	1	1	successo
1	1	1	0	1	successo
1	1	1	1	1	successo

è E e gli eventi primari E1, E2... e con sole porte AND e OR (in questo caso l'albero è detto coerente) è possibile applicando le regole della logica semplificare l'espressione:

$$E = \text{funzione di } E1, E2 \ldots \quad (3)$$

in modo da ridurla a una somma logica di monomi "insiemi"minimi di taglio" C1, C2 ...

$$E = C1 + C2 + C3 + \ldots \quad (4)$$

Si indica con r il numero degli eventi primari coinvolti nel monomio dell'insieme minimo di taglio, detto anche ordine dell'insieme.

Da un generico grafo quindi, risalendo dal basso all'alto, si può scrivere una relazione logica del top event che, dopo aver effettuato le opportune "semplificazioni", apparirà nella forma finale:

$$E = E1 + E2 + E3 \cdot E4 + E3 \cdot E5 + E3 \cdot E6 \cdot E7 + \ldots$$

L'ordine dei termini della somma è quindi il numero di eventi che lo formano.

In questo caso si hanno:

2 eventi del 1° ordine
2 eventi del 2° ordine
1 evento del 3° ordine e così via .

Il significato è di estremo rilievo e, al fine della sicurezza, è tutto sommato il risultato più importante. Infatti il top event si verificherà per il solo evento E1 o per il solo evento E2. Eventi del 1° ordine non dovrebbero mai essere tollerati.

L'analisi degli insiemi minimi di taglio costituisce un'analisi di sensitività a livello logico del sistema: gli eventi primari che appartengono agli insiemi minimi di taglio di ordine più basso, m per esempio, sono quelli qualitativamente più importanti; gli eventi primari che appartengono a insiemi di ordine (m + 1) li seguono in ordine di importanza, e così via.

Nell'esempio precedente gli insiemi minimi di taglio erano stati scoperti attraverso agevoli "semplificazioni" dell'espressione logica del top event e poi ritrovati tramite la tavola della verità.

Per i casi reali, molto più complessi, questi modi sono praticamente impossibili: ci sono però metodi sofisticati che permettono la soluzione di questo problema con l'uso di opportuni algoritmi, elaborati generalmente da programmi di calcolatori numerici.

Calcolo della probabilità dello stato guasto del sistema

Per il calcolo della probabilità dello stato guasto del sistema occorre partire dalla (4).

Se gli insiemi minimi di taglio fossero mutuamente escludentisi, il valore cercato sarebbe semplicemente:

$$p(E) = p(C1) + p(C2) + p(C3) + \ldots$$

Questo però non accade in generale, per cui occorre applicare la formula completa della probabilità totale. Il calcolo risulta estremamente gravoso, se gli eventi primari sono molti e gli insiemi minimi di taglio numerosi.

Sono stati studiati diversi metodi che permettono di risolvere il problema: qui viene indicato brevemente quello di Messinger e Shooman, forse il più comunemente adottato.

Il metodo si sviluppa attraverso due fasi:

- individuazione degli insiemi minimi di taglio;
- impiego della formula

$$p(E) = S1 - S2 + S3 - \ldots (-1)\ Sr \qquad (5)$$

ove:
p(E) è la probabilità del sistema di essere nello stato guasto;
S1 è la somma delle probabilità di ogni insieme minimo di taglio di essere nello stato guasto;
S2 è la somma delle probabilità delle intersezioni a due a due degli insiemi minimi di taglio e così via.

Per probabilità per un insieme minimo di taglio di essere nello stato guasto si intende il prodotto delle probabilità di essere nello stato guasto dei diversi elementi primari. Questo deriva direttamente dalla definizione di insieme minimo di taglio.

Il calcolo, eseguito supponendo gli eventi primari indipendenti, si approssima, quando il caso, attraverso la seguente procedura:

i) ignorando gli insiemi minimi di taglio di ordine più elevato (per esempio con r = 3);

ii) trascurando nella (5) le somme dopo le prime. Poiché i termini tendono a diventare sempre più piccoli e la somma ha segni alternati, è possibile intendere facilmente l'errore che si compie arrestandosi a un certo termine.

Prendendo in considerazione la probabilità di essere nello stato guasto degli eventi primari p(Ei) e degli insiemi minimi di taglio p(Cj) è possibile fare un'analisi quantitativa di sensitività.

Si possono infatti definire come "pesi" degli insiemi minimi di taglio e degli eventi primari le espressioni approssimate:

$$W(Cj) \cong \frac{p(Ei)}{p(E)} \qquad (6)$$

per gli insiemi minimi di taglio

$$W(Ei) \cong \sum W(Cj) \qquad (7)$$

per gli eventi primari

La sommatoria deve intendersi estesa a tutti gli insiemi minimi di taglio ai quali partecipa l'elemento Ei.

Conseguentemente si possono ordinare gli insiemi minimo di taglio e gli eventi primari per "peso" decrescente, cioè secondo il diminuire della loro importanza.

I dati di ingresso per il calcolo dello stato di guasto del sistema p(E) sono le probabilità p(E1), p(E2) ... p(En) relative ai singoli eventi primari. Spesso queste probabilità sono funzioni del tempo e quindi anche il risultato è funzione del tempo. Si intuisce quindi come un'elaborazione completa del problema sia impresa piuttosto ardua e come risultati indispensabile l'uso del calcolatore.

I dati numerici per l'analisi quantitativa

I dati necessari per valutare la frequenza (a mezzo tecniche del tipo albero di guasto o simili) sono spesso chiamati dati "affidabilistici". Occorre cioè raccogliere ed elaborare sistematicamente le informazioni sulle avarie dei componenti per ricavarne indici di valore generale.

La struttura scientifico-organizzativa che raccoglie, elabora e ridistribuisce i dati si chiama "Banca Dati di Affidabilità".

E' conveniente suddividere i dati affidabilistici in tre categorie a seconda che riguardino:

a) Componenti ridondabili;
b) Componenti non ridondabili;
c) Operatore umano.

Da questo breve elenco si può ricavare un'idea delle difficoltà insite in un'analisi quantitativa del rischio tecnologico e del lungo lavoro di raccolta delle informazioni che ciascuna analisi richiede. Va tenuto sempre presente quindi che l'incertezza del risultato numerico finale è strettamente dipendente dalle incertezze dei vari dati elementari introdotti nel modello. E' inutile quindi correre alla sofisticazione della modellistica fino a che la base dei dati numerici disponibile per l'impiego nei modelli non è ragionevolmente "affidabile".

A) Componenti ridondabili

Viene esaminato in dettaglio il problema dei dati affidabilistici su componenti ridondabili, cioè su componenti di impianto generalmente presenti in più esemplari, di cui alcuni aventi funzione di "riserva installata".

Appartengono a questa categoria pompe, compressori, motori, agitatori, strumenti di regolazione, sistemi di allarmi e blocco...

Per ottenere dati affidabilistici su questo tipo di componenti lo strumento normalmente impiegato è la Banca Dati di Affidabilità.

La Banca Dati di Affidabilità è l'archivio, ordinato e continuamente aggiornato, dei dati che descrivono lo stato di efficienza delle apparecchiature e degli impianti.

Questi dati riguardano la frequenza dei guasti, le loro cause e le loro conseguenze sull'esercizio; dalla Banca vengono evidenziati i legami che esistono tra la frequenza dei guasti, le caratteristiche costruttive e di funzionamento delle apparecchiature, il tipo e la periodicità degli interventi e i costi associati.

L'esperienza di gestione degli impianti genera con continuità una massa di informazioni di enorme valore per una verifica sperimentale della validità delle soluzioni ingegneristiche e dei criteri di esercizio e manutenzione a-

dottati. Questo flusso di informazioni, se opportunamente disciplinato e organizzato, costituisce la base da cui ricavare valutazioni sull'affidabilità dei componenti degli impianti.

E' pertanto possibile, per esempio, richiedere a una Banca Dati informazioni relative a:

- valvole di sicurezza
- tarate a più di 20 kg/cm^2,
- operanti su GPL,
- con materiale del corpo in AISI 304,

che hanno manifestato avarie del tipo:

- perdita all'esterno di fluido di processo,
- causata da usura delle sedi.

E' ovvio che a un maggior dettaglio di specificazione dei parametri corrisponde inevitabilmente una riduzione del data base di partenza. E' quindi indispensabile un certo compromesso da stabilire di volta in volta.

Altre informazioni ottenibili sono del tipo:

- valor medio del tasso di guasto per ciascun individuo appartenente all'insieme selezionato;
- valor medio del tasso di guasto per l'intero insieme;
- identificazione della migliore distribuzione statistica (scelta fra la normale, l'esponenziale, la log-normale, la weibulliana e la uniforme);
- identificazione delle apparecchiature costituenti le code dell'insieme;
- identificazione dei parametri "attivi", cioè influenzanti direttamente il tasso di guasto;
- studio delle funzioni che legano il tasso di guasto ai valori dei parametri attivi.

Problemi non indifferenti nascono quando, ed è quasi la norma, i dati ottenuti devono essere impiegati in analisi di situazioni diverse da quelle che li hanno generati. Per esempio quando dati raccolti da impianti esistenti sono impiegati nello studio di impianti da costruire o, peggio ancora, quando dati raccolti in una certa realtà industriale devono essere impiegati in una realtà diversa.

E' lecita l'estrapolazione? Quale margine di errore comporta? La conclusione è che questo prodotto (i dati affidabilistici) non è in generale di quelli facilmente disponibili sul mercato.

B) Componenti non ridondabili

Si intendono inclusi in questa categoria componenti del tipo: recipienti a pressione, reattori chimici, colonne di distillazione... caratterizzati dal fatto di essere dei "pezzi unici" e in generale non ridondabili allo scopo di influenzare l'affidabilità dell'impianto. Questi componenti possono comparire nelle analisi di rischio degli impianti chimici in quanto un difetto di tenuta o un cedimento degli stessi può innescare sequenze di eventi potenzialmente pericolosi. Eventi di questo tipo sono solitamente così rari da essere difficilmente analizzabili da Banche di dati. Esistono tuttavia alcune sorgenti di dati inerenti a questi componenti che permettono di definire almeno l'ordine di grandezza dei fenomeni d'interesse.

C) Operatori umani

Le possibili sorgenti di informazioni relative alla inaffidabilità dell'uomo quando è chiamato a svolgere un certo compito possono distinguersi in:

1 - esperienza di esercizio in impianti
2 - simulatori di impianto;
3 - studi di laboratorio;
4 - interviste con esperti.

I dati di tipo 1 sono di gran lunga migliori, in quanto provengono da una situazione non simulata (tipo 2 e 3), né "ricordata soggettivamente" (tipo 4), ma dalla realtà della vita dell'impianto. Purtroppo la loro raccolta è estremamente difficile.

Metodi di ricerca di tipo 2 e 3 sono assai più facilmente realizzabili.

Sfortunatamente i dati ottenuti fuori dalla realtà dell'impianto soffrono in modo drammatico di questo loro vizio di origine e il loro impiego in analisi di rischio richiederebbe l'introduzione di una serie di coefficienti di correzione (condizioni ambientali, di stress, di angoscia) difficili da determinarsi. Inoltre la reattività tipica dell'operatore umano con i mezzi di indagine indicati (l'operatore se sa di essere investigato agisce in modo diverso dall'usuale) introduce nei risultati un errore probabilmente non trascurabile.

I metodi di tipo 4 (intervista con esperti) presentano un elevato grado di interesse in quanto godono di queste caratteristiche:

- se gli esperti sono scelti con cura la sorgente delle informazioni è indubbiamente un'espressione della realtà dell'impianto;
- se i dati raccolti sono mediati su un campione di esperti abbastanza ampio i punti singolari legati all'individualità di esperienze e di giudizio di ciascun intervistato risultano smussati;
- alcuni dati ottenuti mediante i giudizi di esperti possono essere verificati sperimentalmente su un impianto;
- il metodo è poco costoso e richiede un tempo di indagine ragionevolmente breve.

A titolo di esempio gli analisti di rischio danno, abitualmente, per i diversi tipi di attività le seguenti probabilità di errore per l'operatore umano: attività semplice, di routine, 0,001; attività complicata, di routine,0,01; attività non di routine, 0,1.

Naturalmente questi valori vengono corretti con coefficienti che considerano il tempo disponibile per l'esecuzione dell'operazione, lo stato di angoscia, la qualità dell'operatore, le condizioni ergonomiche ambientali e così via.

ENTITA' DELLE CONSEGUENZE DI UN INCIDENTE

E' stato definito rischio relativo a un incidente il prodotto della sua frequenza per la magnitudo delle sue conseguenze.

Nel presentare questa definizione, sono state indicate le difficoltà di una misura della magnitudo, in quanto le conseguenze di un incidente possono essere molto diverse fra di loro ed essere contemporaneamente presenti: morti, aborti, feriti, distruzione di cose, inquinamento dell'ambiente, ...

In problemi di questo tipo alcuni tecnici, per esempio gli assicuratori, riportano tutto a un valore monetario: se l'obiettivo del calcolo è solo quello di fare dei confronti il metodo in linea di principio sembra ragionevole.

Nel seguito si presenta una traccia per giungere a una valutazione a priori dei danni finali di un incidente. La vastità dell'argomento impedisce di fare di più, ma l'inquadramento della problematica può riuscire una guida per chi voglia intraprendere uno studio sistematico.

Tipi di incidente

Tipici incidenti dell'industria chimica sono:

- lo scoppio di un reattore;
- la rottura di un contenitore o di una tubazione;
- lo scarico di una valvola di sicurezza (che preserva da uno scoppio, ma può dar luogo alla dispersione di sostanze tossiche e/o infiammabili);
- l'accensione di una miscela esplosiva;
- i rilasci continui di gas, vapori, liquidi;
- il BLEVE (Boiling Liquid expanding Vapour Explosion).

In definitiva nell'industria di processo, se si prescinde dall'infortunistica convenzionale (che è affrontata con altri mezzi ed altre tecniche, gli eventi che solitamente possono creare situazioni di incidenti con conseguenze rilevanti, sono raggruppabili nelle seguenti categorie:

a) Rilasci di sostanze tossiche e/o infiammabili:
- Gas e vapori (inquinamento dell'aria, nubi esplosive, ecc.)
- Liquidi (inquinamento delle acque)
- Solidi (polveri, scorie di lavorazione, ecc.)

b) Rilasci di energia:
- Energia termica (incendi)
- Energia di pressione (esplosioni).

Per valutare le conseguenze di questi rilasci è necessario definire l'entità probabile del rilascio, l'area interessata, gli effetti del rilascio sulle persone e sulle proprietà.

Ad esempio, se l'evento rischio esaminato è il rilascio accidentale di ammoniaca nell'atmosfera, occorre valutare:

- Quanta ammoniaca può essere rilasciata.
- Come è rilasciata (durata, intensità del rilascio, condizioni chimico-fisiche del prodotto rilasciato)
- Come l'ammoniaca si diffonde nell'area circostante (concentrazioni al suolo alle varie distanze, nelle varie condizioni metereologiche)
- Quale è la popolazione esposta al rischio ed a quale livello di rischio (mappa dei rischi)
- Qual'è la tossicità dell'ammoniaca nelle concentrazioni calcolate
- Cosa si può fare per minimizzare gli effetti del rilascio sulla popolazione esposta (piani di emergenza).

Ne consegue che, per stimare le conseguenze dei rilasci accidentali di gas tossici, occorre disporre di una serie di modelli matematici previsionali in grado di descrivere con ragionevole accuratezza il fenomeno; data la complessità della relativa modellistica occorre poi disporre degli strumenti di calcolo automatico per utilizzare i modelli.

La modellistica disponibile è lungi dall'essere definitiva: un gran numero di ricerche è in corso presso numerose università ed istituti specializzati per meglio definire i necessari algoritmi di calcolo e per sottoporli a verifiche sperimentali.

Dati i limiti della presente trattazione, ci si limita a citare l'elenco dei modelli necessari per effettuare analisi di questo tipo:

- fluidodinamlica nei condotti di scarico
- rilasci con jet turbolenti
- diffusione di gas leggeri
- diffusione di gas pesanti
- diffusione di polveri
- stima di esplosioni non confinate
- stima di esplosioni confinate
- diffusione di liquidi insolubili in acqua
- diffusione di liquidi solubili in acqua
- evaporazione da pozza
- irraggiamento termico da incendi di liquidi
- irraggiamento da rilasci gassosi.

Questo elenco può fornire un'idea della complessità della modellistica e della professionalità necessaria per il suo approntamento e la sua gestione. In particolare non si può tracciare una mappa dei rischi, né approntare un credibile piano di emergenza, senza aver prima studiato le modalità di evoluzione dei possibili rilasci critici di materia e/o di energia ed il loro impatto con l'ambiente.

Fenomeni fisici e chimici

Come si può intuire dalle semplici esemplificazioni, fatte nel paragrafoi precedente, i fenomeni fisici e chimici che intervengono nei vari tipi di incidente sono assai vari. Nell'impossibilità di trattare anche solo i principali in modo adeguato, ci si limita solo a presentare le problematiche relative al rilascio di gas e vapori.

Il rilascio di gas e vapori

La produzione, l'utilizzazione e la movimentazione di prodotti chimici richiedono frequentemente rilasci controllati di gas e vapori da torce e ciminiere e lo scarico di liquidi opportunamente diluiti.

Si possono però avere anche rilasci accidentali, dovuti a rottura di organi di tenuta posti su apparecchiature o tubazioni, a interventi di valvole di sicurezza e di dischi di rottura per anomale condizioni di esercizio e - in casi del tutto eccezionali - collassi di contenitori.

Diversi liquidi si trovano nei contenitori o refrigerati o sotto pressione, così che, uscendo all'esterno, vaporizzano, dando luogo a volumi di fluidi eccezionalmente grandi rispetto a quello occupato dal liquido.

I modelli della diffusione e dispersione di gas e vapori devono tener conto delle caratteristiche del rilascio (in particolare della quantità di fluido, della temperatura, della velocità di efflusso), delle caratteristiche chimico-fisiche del fluido (in particolare la densità rispetto all'aria) e delle condizioni atmosferiche.

Esistono molti studi in proposito, non esiste però a tutt'oggi una teoria completa ed esauriente che sia in grado di prendere in considerazione tutti i fattori in gioco: si è solo in grado di fare delle stime attendibili in situazioni ideali, come per esempio in siti pianeggianti, interessati da vento costante parallelo al suolo.

Un classico modello di questo tipo è quello accennato qui di seguito: un pennacchio di fumo viene schematizzato supponendo che la concentrazione di un inquinante vari in modo gaussiano intorno al suo asse e che esso abbia una propagazione con asse parallelo al suolo. Si veda in proposito la Fig. 2.19.

Si è supposto il gas rilasciato con densità vicina a quella dell'aria e la velocità del vento costante, parallela al suolo e non superiore a 6 m/s.

Poiché dati meteorologici accurati sono raramente disponibili, numerosi autori hanno suggerito una suddivisione delle caratteristiche di turbolenza atmosferica in classi di stabilità determinabili in base a dati facilmente ottenibili, quali la velocità del vento al suolo, il grado di insolazione se di giorno o il grado di copertura se di notte. Una delle classificazioni più comunemente adottate è riportata nella Tabella 2.11.

Pasquill ha ricavato in base alla stabilità atmosferica, i coefficienti di dispersione laterale e verticale del pennacchio (corrispondenti alle deviazioni standard σ_y e σ_z della gaussiana) in funzione della distanza dalla sorgente. Due tipiche rappresentazioni sono mostrate nella Fig. 2.20.

Si intuisce che sarebbe errato, per studi di previsione delle emissioni provenienti da un certo impianto, servirsi acriticamente di questo risultato.

Le condizioni fisiche del rilascio sono spesso lontane da quelle ipotizzate nel modello accennato.

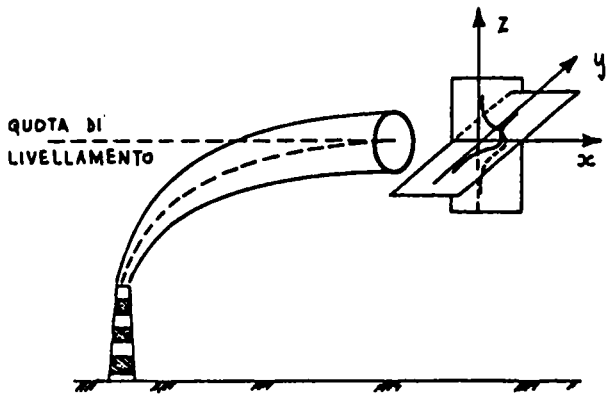


Fig. 2.19 - Diffusione a dispersione di un pennacchio di fumo.

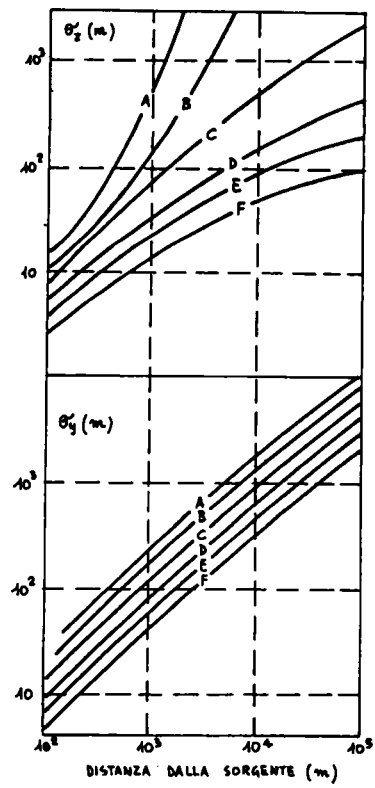


Fig. 2.20 - Coefficienti di dispersione laterale e verti cale secondo Pasquill.

VELOCITA' DEL VENTO AL SUOLO (m/s)	INSOLAZIONE DIURNA			CONDIZIONI NOTTURNE	
	FORTE	MODERATA	DEBOLE	COPERTURA ≥ 4/8	COPERTURA < 4/8
< 2	A	A-B	B		
2	A-B	B	C	E	F
4	B	B-C	C	D	E
6	C	C-D	D	D	D
> 6	C	D	D	D	D

A: Condiz. estremamente instabili.
B: Condiz. moderatamente instabili.
C: Condiz. leggermente instabili.
D: Condiz. neutre.
E: Condiz. leggermente stabili.
F: Condiz. moderatamente stabili.

Tab.2.11 - Suddivisione delle caratteristiche di turbolenza atmosferica in classi di stabilità secondo Pasquill.

Va infine ricordato, per concludere, che i rilasci hanno spesso proprietà inusuali, non facilmente sintetizzabili in una densità (omogenea) e in una velocità. Si ha talvolta evaporazione con formazione di aerosol, trasporto di particelle solide e di liquido in seno a una nube di gas,e così via.

Modelli di vulnerabilità alle conseguenze di incidenti

L'analisi dei rischi di un impianto industriale viene svolta secondo una procedura che prevede l'identificazione degli eventi incidentali, la stima della loro probabilità, il calcolo delle loro conseguenze fisiche e la stima dei danni alla popolazione esposta ed all'ambiente.

Le conseguenze fisiche sono solitamente espresse sotto forma di mappe dell'intensità dell'irraggiamento termico da incendi, delle sovrapressioni da esplosione e delle concentrazioni da rilasci tossici.

I danni all'uomo ed alla proprietà dipendono dall'entità alle conseguenze fisiche degli incidenti e dalla capacità di resistenza dei soggetti colpiti.

I modelli previsionali che consentono di stimare i danni in funzione delle caratteristiche dell'aggressione fisica sono noti come "modelli di vulnerabilità". Questi modelli consentono di tentare una risposta a domande del tipo:

- Data una certa concentrazione tossica in un'area popolata, qual'è il tasso probabile di ospedalizzazione e di mortalità?
- Data una certa distribuzione di sovrapressioni da esplosivo, qual'è la probabilità di ferite alla popolazione esposta e di distruzione degli immobili?
- Data una certa mappa di irraggiamento termico da incendio, qual'è la percentuale di persone esposte che sarà ustionata?

E così via. In altre parole i modelli di vulnerabilità consentono di passare dalla mappatura delle conseguenze fisiche alla stesura di vere e proprie mappe di danni probabili all'uomo e alle cose (mappe di rischio).

E' tuttavia opportuno sottolineare che per molti scenari incidentali non esistono adeguati modelli, o i modelli esistenti consentono solo stime con larghi margini di incertezza. Questo è in particolare vero per i modelli di studio

della vulnerabilità da inalazione di sostanze tossiche, tuttora assai lacunosi per carenza di credibili dati tossicologici e ovvie difficoltà di sperimentazione.

Molta cautela deve, in ogni caso, essere esercitata nell'impiego di modelli ed in particolare nella definizone delle condizioni al contorno per evitare da un lato ingiustificati catastrofismi, dall'altro pericolosi ottimismi.

Inoltre va tenuto presente che i modelli sono stati sviluppati, in generale, assumendo caratteristiche medie della popolazione a rischio (ad esempio individui adulti di buona salute) e che quindi possono essere gravemente in difetto per campioni di caratteristiche lontane dai valori medi (ad es. bambini, vecchi, malati, ecc.).

I modelli di vulnerabilità ricevono in input la descrizione delle conseguenze fisiche dell'incidente (es. durata e concentrazione tossica in una certa area geografica) e forniscono in output la previsione dei danni per le persone e per le proprietà esposte all'impatto (es. numero di feriti, numero di vittime, ecc.).

I principali modelli fisici sono relativi alle conseguenze di:

- incendi;
- esplosioni;
- rilasci tossici.

Conseguentemente si hanno modelli di vulnerabilità per le:

- radiazioni termiche;
- esplosioni;
- inalazioni di sostanze tossiche.

I modelli di vulnerabilità si basano in generale su una funzione matematica di probit del tipo:

$$Pr = a + b \ln x$$

dove:

a, b sono costanti funzioni dello specifico scenario incidentale,

x è la variabile che descrive l'entità dell'impatto fisico,

Pr è una misura della percentuale del danno sulle risorse (umane e/o materiali) esposte.

La variabile dipendente Pr è denominata probit (probability unit); essa è una variabile casuale a distribuzione gaussíana con valore medio 5 e varianza 1, cioè ad una

percentuale del 5% corrisponde un valore di probit Pr = 5.

Il legame matematico tra la probabilità di danno P e la variabile di probit Pr è del tipo:

$$P = \frac{1}{(2\pi)^{\frac{1}{2}}} \int_{-\infty}^{Pr-5} \exp\left[-\frac{x^2}{2}\right] dx$$

Nella Tab. 2.12 è riportata la relazione tra probit e probabilità.

Tab. 2.12 - Relazione Probit-Probabilità.

%	0	1	2	3	4	5	6	7	8	9
0	—	2.67	2.95	3.12	3.25	3.36	3.45	3.52	3.59	3.66
10	3.72	3.77	3.82	3.87	3.92	3.96	4.01	4.05	4.08	4.12
20	4.16	4.19	4.23	4.26	4.29	4.33	4.36	4.39	4.42	4.45
30	4.48	4.50	4.53	4.56	4.59	4.61	4.64	4.67	4.69	4.72
40	4.75	4.77	4.80	4.82	4.85	4.87	4.90	4.92	4.95	4.97
50	5.00	5.03	5.05	5.08	5.10	5.13	5.15	5.18	5.20	5.23
60	5.25	5.28	5.31	5.33	5.36	5.39	5.41	5.44	5.47	5.50
70	5.52	5.55	5.58	5.61	5.64	5.67	5.71	5.74	5.77	5.81
80	5.84	5.88	5.92	5.95	5.99	6.04	6.08	6.13	6.18	6.23
90	6.28	6.34	6.41	6.48	6.55	6.64	6.75	6.88	7.05	7.33
—	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
99	7.33	7.37	7.41	7.46	7.51	7.58	7.65	7.75	7.88	8.09

SEZIONE III

PRINCIPI E METODI DELL'AFFIDABILITA'

CONCETTO DI AFFIDABILITA'

In termini elementari, l'affidabilità è la proprietà di un'apparecchiatura di non guastarsi durante il suo funzionamento. Quando un'apparecchiatura lavora correttamente, rispondendo a tutte le funzioni per cui è stata progettata, questa apparecchiatura è detta affidabile. L'affidabilità è misurata dalla frequenza di guasto dell'apparecchiatura nel tempo, o meglio, in un intervallo di tempo prefissato. Se non si verificano affatto guasti, l'apparecchiatura é affidabile al 100%, se la frequenza di guasto è molto bassa, il livello di affidabilità può essere ancora accettabile. Se la frequenza di guasto è alta, l'apparecchiatura è detta inaffidabile.

In affidabilità si distinguono tre tipi principali di guasti che sono intrinseci all'apparecchiatura e si verificano senza che l'operatore abbia commesso alcun errore.

a) Guasti infantili (primi guasti). Sono i guasti caratteristici del periodo iniziale della vita di un dispositivo. I guasti infantili nella maggior parte dei casi sono il risultato della inadeguatezza delle tecniche di costruzione e di controllo della qualità durante il processo di produzione. Questi guasti infantili si possono eliminare mediante il processo di "rodaggio" o di "avviamento".

b) Guasti da usura (o da invecchiamento). I guasti causati da usura dei pezzi componenti un dispositivo si verificano soltanto se questo non è sottoposto a perfetta manutenzione; essi sono un sintomo del progressivo invecchiamento dei componenti. Nella maggior parte dei casi, i guasti da usura si possono prevenire con sostituzione ad intervalli regolari dei componenti o con progettazione di questi a "lunga vita".

c) Guasti casuali. I guasti casuali sono quelli

che nessun rodaggio, nè alcuna manutenzione possono eliminare. Questi guasti sono provocati da improvvisi accumuli di sollecitazioni, oltre la resistenza massima di progetto del componente; per cui i guasti da usura si verificano ad intervalli casuali, in modo improvviso e del tutto inaspettato. Normalmente non è facile eliminare i guasti casuali. Si sono però sviluppate tecniche di affidabilità che ne riducono la probabilità o addirittura eliminano completamente l'eventualità che l'apparato si arresti a causa del guasto casuale di un componente.

La definizione iniziale può ora formularsi in modo più corretto: "l'affidabilità è la probabilità di corretto funzionamento, per un prefissato periodo di tempo, di un'apparecchiatura che operi in determinate condizioni di impiego". A questa probabilità si dà anche il nome di "probabilità di sopravvivenza".

Si consideri ora un sistema complesso costituito da più apparecchiature o componenti (Es. una rete di distribuzione di energia elettrica). Si chiama disponibilità del sistema la frazione di tempo in cui il sistema è efficiente. Di solito la disponibilità è espressa in per cento. Si definisce infine probabilità di intervento la probabilità che un sistema ausiliario, in attesa o in stand-by, risponda alla domanda. Poiché, anche se non in funzione, queste unità possono guastarsi, esse sono periodicamente controllate ("test"). Si hanno quindi le seguenti definizioni:

TT (test time) = intervallo fra un test ed il successivo;

MTTT (mean time to test) = durata media di un test;

MTTR (mean time to repair) = tempo medio di riparazione;

MTBF (mean time beyween failures) = tempo medio tra due guasti.

Per i sistemi complessi l'affidabilità si stima mediante un calcolo esatto di probabilità, i cui dati

di partenza sono le affidabilità delle parti componenti; cosicchè la precisione della stima dell'affidabilità del sistema è funzione delle approssimazioni dei valori di affidabilità delle singole parti componenti.

Si ricordi inoltre che i calcoli di affidabilità , in quanto calcoli di probabilità, si applicano a modelli ideali. Quando poi si confronta la stima con il valore osservato durante il funzionamento reale, si constaterà una buona concordanza solo se è stato elevato il numero di osservazioni su cui si é fondata la stima.

Negli studi di affidabilità, è essenziale una definizione precisa di ciò che sta sotto alla dizione: "prestazione soddisfacente" o "prestazione adeguata", per la implicita considerazione che l'oggetto dello studio è la probabilità di ottenere questa prestazione adeguata. Il concetto di "prestazione soddisfacente" e quello di "guasto" sono quindi complementari. Si tratta di due eventi mutuamente escludentesi per cui l'apparecchiatura, durante il suo impiego o si trova nello stato di corretto funzionamento o nello stato di guasto.

La frequenza del verificarsi di guasti e cattivi funzionamenti costituisce così un parametro della formulazione matematica dell'affidabilità. A tale parametro si dà il nome di "Tasso di guasto" o "Indice di guasto", solitamente indicato con λ, e lo si misura in numero di guasti per unità di tempo (anni) di impiego. Il suo inverso (m) è detto anche tempo medio tra i guasti (MTBF) ed è misurato in anni.

$$E' \; m = \frac{1}{\lambda}.$$

Quando i guasti si verificano a caso durante l'impiego di un dispositivo, il tasso di guasto si può ricavare dal numero di avarie registrate in un periodo di impiego sufficientemente lungo e l'affidabilità dell'apparecchiatura si può quindi calcolare in base a semplici formule matematiche.

Nel seguito si farà uso della seguente simbologia:

R (reliability) = affidabilità
F (unreliability) = inaffidabilità
A (availability) = disponibilità
Q (unvailability) = indisponibilità

Valgono, per qualsiasi condizione, le seguenti relazioni:

$$R + F = 1$$
$$A + Q = 1$$

DISTRIBUZIONE DEL PRIMO DANNO DI UN COMPONENTE

Il passaggio di un elemento dallo stato efficiente allo stato guasto (con riferimento ad una specifica funzione) è un evento caratterizzabile da una o più variabili. Nel seguito si considera una sola variabile continua: il tempo (t).

Con riferimento ad un generico num.N_o di componenti tutti uguali e funzionanti al tempo t=0, si hanno le seguenti definizioni:

N_o = numero dei componenti in prova

dopo un certo tempo t si ha

$N_s(t)$ = numero componenti sopravvissuti

$N_g(t)$ = numero componenti che si sono guastati in un qualsiasi istante si ha:

$$R(t) = \frac{N_s(t)}{N_o}$$ = affidabilità; probabilità di sopravvivenza.

$$Q(t) = \frac{N_g(t)}{N_o}$$ = inaffidabilità o probabilità di guasto.

$$\frac{dF}{dt} = f(t) = \frac{1}{N_o} \frac{dN_g}{dt}$$ = funzione densità di guasto; distribuzione dei guasti riferita ad un solo componente (frequenza unitaria di guasto).

$$h(t) = \frac{1}{N_s(t)} \frac{dN_g}{dt}$$ = probabilità istantanea di guasto o tasso di guasto

$$h(t) = \frac{N_o}{N_s(t)} \cdot f(t) = \frac{f(t)}{R(t)} \quad \text{od anche}$$

$$f(t) = h(t) \cdot R(t)$$

A maggior chiarimento di queste funzioni si può ancora precisare quanto segue.
R (t) - Affidabilità. Esprime anche la probabilità che l'elemento sopravviva all'istante t, ossia che la sua durata sia superiore al tempo t:

$$R(t) = \int_t^\infty f(t)\, dt$$

F(t) - Inaffidabilità o distribuzione cumulativa di guasto (Failure distribution function). Esprime la probabilità che il guasto (si intende sempre in questa parte il primo guasto) si verifichi fra il momento iniziale e l'istante t.
Si ha:

$$F(t) = \int_0^t f(t)\, dt$$

La funzione F(t) esprime anche la probabilità che il componente sia nello stato guasto al tempo t.
f(t) - Frequenza di guasto (failure frequency). La funzione è una densità di probabilità, in quanto f(t) • dt esprime la probabilità che il primo guasto si verifichi nell'intervallo di tempo t ⟼ t + dt. E' dimensionalmente l'inverso di un tempo.
h(t) - Tasso di guasto (failure rate o hazard function). Esprime,per un componente sopravvissuto fino al tempo t, la probabilità che si guasti nel successivo intervallo di tempo dt.

Anche h(t) è dimensionalmente l'inverso di un tempo.

Nella Fig. 3.1 è tracciato l'andamento tipico della funzione h(t), a forma di "vasca da bagno", e quello della f(t) relativa.

Si ha inizialmente per h(t) un andamento rapidamente decrescente: è il periodo dei guasti precoci (early failure o infant mortality period). Segue il periodo con il tasso di guasto h(t) pressoché costante, noto co-

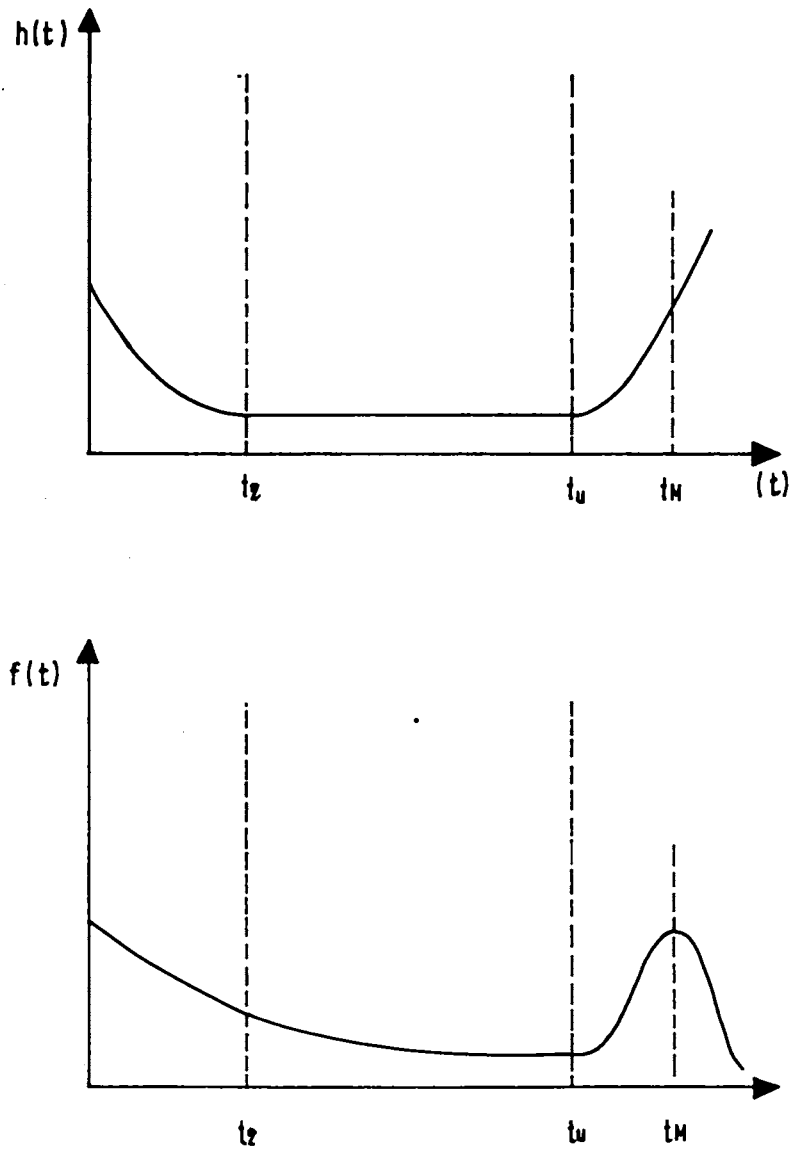


Fig. 3.1 - Andamento del tasso di guasto di un componente in funzione del tempo.

me periodo di vita utile (prime of life): l'essere costante h(t) vuol dire che, in questo periodo, l'apparecchiatura si guasta indipentemente dalla sua età, cioè a caso. Si entra poi nel periodo di usura (wear-out failure period) con tasso di guasto crescente.

La funzione h(t) può essere ricavata sperimentalmente procedendo nel seguente modo.

Al tempo t > 0 si mettono in funzione un gran numero di componenti tutti dello stesso tipo e tutti nuovi. Se tra questi sono presenti pezzi di struttura più debole del normale, la curva indicherà un alto tasso di guasto iniziali.

Man mano, che i componenti più deboli si eliminano durante il periodo di rodaggio h(t) si stabilizza ad un valore pressochè costante λ al tempo Tr. Dopo il rodaggio quindi i componenti raggiungono così il più basso valore del tasso di guasto, che rimane approssimativamente costante durante un certo periodo di tempo detto "vita utile". Quando poi i componenti raggiungono l'età Tu comincia a farsi sentire l'usura. Da questo momento in poi il tasso di guasto cresce rapidamente. Dei molti componenti sopravvissuti fino al tempo Tu circa la metà verrà eliminata nell'intervallo di tempo che va da Tu a Tm. Il tempo Tu è la "vita media per usura" della popolazione.

Fra le diverse funzioni che possono rappresentare bene la frequenza di guasto vi è la funzione di Weibull a due parametri:

$$f(t) = \beta \lambda (\lambda t)^{\beta-1} \exp\left[-(\lambda t)^{\beta}\right]$$

Infatti, questa funzione rappresenta bene il periodo dei guasti precoci quando il parametro $\beta < 1$.

Durante il periodo di vita utile si ha invece $\beta = 1$. In questo caso è $h(t) = \lambda$, valore costante. Si ottiene così facilmente:

$$f(t) = \lambda \exp(-\lambda t)$$

cioè la frequenza di guasto è di tipo esponenziale negativo. Si hanno quindi anche le relazioni:

$$F(t) = 1 - \exp(-\lambda t)$$
$$R(t) = \exp(-\lambda t)$$

Nel periodo di usura la funzione f(t) può essere ben espressa da una funzione di Weibull, con $\beta > 1$ od anche da una funzione di Gauss.

Il fatto che la funzione di Weibull si adatti a tutti i tre periodi appare molto attraente per rappre - sentare l'intero ciclo di vita di un componente. Il suo impiego, però in pratica non è estremamente diffuso.

L'esecuzione di test per determinare l'affidabilità di sistemi o componenti, specialmente se comples - si, è normalmente costosa, pur facendo un minimo di prove. D'altra parte, le vere probabilità sono basate sui risultati di infiniti o estremamente grandi campioni. Quando vengono sottoposti a test solo pochi elementi, i risultati possono non essere veramente rappresentativi. Alzando due o tre volte una moneta si può avere sempre testa. Ciò può portare alla conclusione erronea che il risultato sarà "sempre" testa. I successivi tre lanci possono dare tutti testa, tutti croce o una combinazione di esse. Con sempre più numerosi lanci, la probabilità media di avere testa (o croce) si avvicina allo 0,50. Nasce quindi il problema di quanta fiducia può essere accordata ai risultati ottenuti per predire i risultati futuri: si usa a questo scopo il termine "livello di confidenza".

Se la previsione di un risultato futuro si ritiene errata per non più di cinque volte su cento, il li - vello di confidenza è del 95%. Esistono tabelle che danno la relazione tra i risultati delle prove, l'affidabilità ed il livello di confidenza.

A titolo esemplificativo si veda la Tabella 3.1.

Tabella 3.1

Numero di prove che devono essere effettuare senza disfunzione per avere una affidabilità specifica ai vari livelli di confidenza

Affidabilità minima (%)	Livello di confidenza 90%	95%	97,5%	99%	99,5%
75	8	11	13	16	19
80	11	14	17	21	24
85	15	19	23	29	33
90	22	29	35	44	51
95	45	59	72	90	103
96	57	74	91	113	130
97	76	99	122	152	174
98	115	149	184	229	263
99	230	299	370	460	530

CARATTERISTICHE DI AFFIDABILITA' DI UN COMPONENTE

Mentre i guasti infantili e quelli da usare possono essere eliminati con appropriate tecniche, non c'è tecnica che possa eliminare i guasti casuali. Se si provasse a sostituire i componenti ancora funzionanti non si otterrebbe alcun miglioramento, anzi si rischia di peggiorare la situazione. Non si dimentichi però che nessun componente deve essere mantenuto in servizio dopo il suo tempo Tu di sostituzione preventivo.
Per una buona affidabilità occorre quindi:

1) Nel periodo di vita utile sostituire i componenti appena si guastano;

2) Prima della fine del periodo di vita utile effettuare una sostituzione preventiva di tutti i componenti benché non guasti;

3) Eseguire un rodaggio appropriato dei componenti prima dell'assemblaggio ed una ispezione completa sul sistema prima dell'impiego.

Supponendo che queste regole siano rispettate,ci si sofferma ad esaminare meglio il comportamento dei componenti nel periodo di vita utile.

In questo periodo l'affidabilità di un dispositivo è espressa dalla semplice formula:

$$R(t) = e^{-\lambda t} \qquad (1)$$

l'affidabilità è quindi la probabilità che il dispositivo non entri in avaria durante il periodo di impiego t. Il grande vantaggio di questa probabilità (R) nei confronti di altre distribuzioni statistiche consiste nel fatto che essa é definita da un solo parametro: il tasso di guasto λ. Inoltre è indipendente dall'età del componente, almeno finchè vale la condizione di un tasso di guasto costante. Durante la vita utile quindi l'affidabilità è approssimativamente la stessa per periodi di impiego di durata eguale. Così, ad es., l'affidabilità è la stessa nelle prime 10 ore e nelle ultime 10 ore di vita utile del dispositivo.

Se durante il funzionamentole sollecitazioni ambientali subiscono una variazione da un livello ad un altro livello costante, si passerà dal tasso di guasto λ'relativo al tempo t' di funzionamento sotto il primo livello di sollecitazione, ad un altro tasso di guasto costante λ" relativo al tempo t" di funzionamento sotto le seconde condizioni di sollecitazione. L'affidabilità del componente per il tempo totale $t = t'+t"$ è allora:

$$R(t) = e^{-\lambda' t'} \cdot e^{-\lambda" t"} = e^{-(\lambda' t' + \lambda" t")} \qquad (2)$$

Analoghe considerazioni si applicano a sistemi a più componenti.

Utilizzando il tempo medio tra i guasti $m = \frac{1}{\lambda}$, l'affidabilità, detta in questo caso, anche probabilità di sopravvivenza, si può anche esprimere nella forma:

$$R(t) = e^{-t/m} \qquad (3)$$

Riportando in un grafico questa funzione si ottiene la cosiddetta "curva di sopravvivenza (Fig. 3.2).

Il tempo t è detto anche tempo "di missione" in quanto la (3) serve a prevedere la sopravvivenza per una missione di durata t. Naturalmente si assume che il dispositivo abbia superato le missioni precedenti e che non incontri il termine della sua vita utile nel corso della missione considerata. Queste missioni, non solo sono più brevi della vita utile del dispositivo o del sistema, ma sono anche molto più brevi del loro tempo medio tra guasti m. Quindi le previsioni di affidabilità si estendono solo agli intervalli di tempo corrispondenti al tratto superiore della curva di sopravvivenza.

Derivazione della funzione di affidabilità

Dalla definizione di probabilità si ricava facilmente la formula dell'affidabilità (1).

La probabilità che accada un evento ("testa") è definita come il rapporto tra il numero di esiti favorevoli all'evento "testa" e il numero totale di prove eseguite. Qualora per ogni prova, come nel lancio di una moneta, possa verificarsi o l'esito favorevole all'evento o l'esito sfavorevole ("croce") e si verificano x esiti favorevoli e y esiti sfavorevoli, allora la probabilità dell'evento "testa" è:

$$P(\text{testa}) = \frac{x}{x+y} \qquad (4)$$

Si identifichi l'evento testa con la sopravvivenza di un componente e l'evento croce con il suo guasto. Se si provano N_o componenti, dopo un certo tempo t si avrà che N_s sopravvivono alla prova e N_g che si sono guastati.

Naturalmente $N_o = N_s(t) + N_g(t)$ (5)

è costante durante tutto il corso della prova.

Ad un qualsivoglia tempo t durante il corso della prova, l'affidabilità, o probabilità di sopravvivenza va

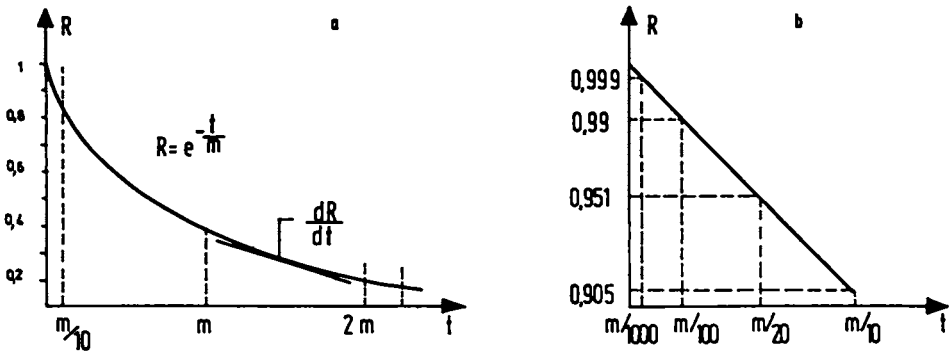


Fig. 3.2 - Curva di sopravvivenza di un componente in funzione del tempo.

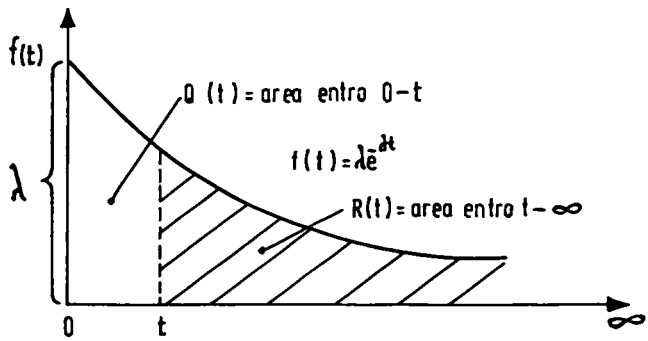


Fig. 3.3 - Funzione di densità di guasto.

le:

$$R(t) = \frac{N_s(t)}{N_o} \qquad (6)$$

e la probabilità di guasto:

$$F(t) = \frac{N_g(t)}{N_o} \qquad (7)$$

In qualunque istante è quindi $R(t) + F(t) = 1$
La (6) può anche scriversi:

$$R(t) = \frac{N_o - N_g(t)}{N_o} = 1 - \frac{N_g(t)}{N_o} \qquad (8)$$

derivando rispetto al tempo si ha:

$$\frac{dR}{dt} = -\frac{1}{N_o}\frac{dN_g}{dt} \quad \text{che può scriversi:} \qquad (8')$$

$$\frac{dN_g}{dt} = -N_o \frac{dR}{dt} \qquad (9)$$

Questa relazione esprime il ritmo di cedimento dei componenti. Dividendo entrambi i membri della (9) per N_s, a sinistra si ottiene la probabilità istantanea di guasto $h(t)$, già chiamata con il nome di tasso di guasto:

$$h(t) = \frac{1}{N_s(t)}\frac{dN_g}{dt} = -\frac{N_o}{N_s(t)}\frac{dR}{dt} \qquad (10)$$

Poichè, per definizione, è $R(t) = \frac{N_s(t)}{N_o}$, la (10) diventa:

$$h(t) = -\frac{1}{R(t)} \cdot \frac{dR}{dt} \qquad (11)$$

che è la più generale espressione per il tasso di guasto, valida per qualunque tipo di funzione R ed h.

In generale infatti h è una funzione del tempo di funzionamento t. Separando le variabili ed integrando la (11) si ha:

$$h(t)\ dt = -\frac{dR}{R(t)}$$

$$\int_0^t h(t)\ dt = -\int_1^R \frac{dR}{R(t)} = -\ln R$$

dato che per $t = 0$ è $R = 1$

$$\ln R = -\int_0^t h(t)\ dt \qquad \text{e quindi}$$

$$R(t) = \exp\left[-\int_0^t h(t)\ dt\right] \qquad (12)$$

La (12) descrive matematicamente l'affidabilità R con il massimo di generalità e si applica a tutte le possibili distribuzioni di guasto.

In particolare se $h(t) = \lambda$ = costante, si ottiene la relazione (1).

Il termine $\frac{dR}{dt}$ dell'equazione (8') rappresenta ovviamente la pendenza della curva della Fig. 3.2 ed ha valori costantemente negativi. Il segno negativo è insito nella stessa equazione (8') dove $\frac{dN_g}{dt}$ rappresenta la frequenza di guasto ad un istante qualsiasi.

Riportando in un grafico $\frac{d\,N_g}{dt}$ al variare di t, si ottiene la distribuzione cronologica dei guasti per tutti gli N_o elementi iniziali.

Riportando invece in un grafico $\frac{1}{N_o} \cdot \frac{d N_g}{dt}$, si ha la distribuzione dei guasti riferita ad un solo componente. Questa curva di frequenze unitarie é già stata chiamata funzione densità di guasto f(t), cioè:

$$f(t) = \frac{1}{N_o} \frac{d N_g}{dt} = - \frac{dR}{dt} \qquad (13)$$

Nel caso particolare di λ = costante, si ha:

$$f(t) = - \frac{dR}{dt} = - \frac{d\, e^{- \lambda t}}{dt} = \lambda\, e^{- \lambda t} \qquad (14)$$

Ricordando che $\frac{dR}{dt} = - \frac{dF}{dt}$ si può scrivere inoltre:

$$f(t) = \frac{dF}{dt}$$ che integrata dà:

$$F(t) = \int_0^t f(t)\, dt \qquad (15)$$

questa relazione associa la probabilità di guasto F(t) al tempo t con l'area compresa tra 0 e t nel grafico della funzione di densità di guasto (Fig. 3.3).

Con il procedere del tempo quest'area aumenta insieme alla probabilità di guasto. Perciò F(t) è la funzione cumulativa di probabilità di guasto. Inversamente la probabilità di sopravvivenza deve diminuire con il procedere del tempo.

Probabilità di un componente di essere nello stato guasto

La probabilità F(t) che un componente sia nello stato guasto al tempo t dipende, in generale, dai parametri della distribuzione di guasto e dalle politiche di riparazione, manutenzione e test.

Le situazioni reali di maggior interesse sono le seguenti:

- il guasto si autodenuncia, cioè il suo accadere è subito riconosciuto ed è possibile, in linea di principio, intervenire immediatamente e cambiare il pezzo o ripristinarlo come nuovo;

- il guasto non si autodenuncia, ma si rivela solo in occasione di un test (si pensi per esempio a un generatore Diesel di riserva).

Il componente è riparato, se guasto

Essendo h(t) il tasso di guasto del componente e $\mu(t)$ il tasso di ripristino (definito in modo analogo), e assumendo che sia h(t), sia $\mu(t)$ dipendano dal tempo, ma non dalla "storia" precedente del componente, la probabilità F(t) che il componente sia nello stato guasto al tempo t si ottiene risolvendo l'equazione:

$$dF(t) = h(t) \cdot R(t)\, dt - \mu(t)\, F(t)\, dt$$

che dà la variazione della probabilità F(t) come bilancio fra guasti e riparazioni (i guasti si riferiscono ai componenti sopravvissuti integri e le riparazioni ai componenti che si sono guastati).
Sostituendo a R(t) l'espressione 1 - F(t) si ha:

$$\frac{dF(t)}{dt} = h(t) - \left[h(t) + \mu(t)\right] F(t) \qquad (16)$$

In generale la risoluzione di questa equazione differenziale richiede un'integrazione numerica.
Nel caso particolare in cui i tassi di guasto e di ripristino non dipendono dal tempo, cioè se:

$$h(t) = \lambda = \text{costante}$$
$$\mu(t) = \mu = \text{costante}$$

l'equazione differenziale è di tipo omogeneo e la sua soluzione analitica è data da:

$$F(t) = \frac{\lambda}{\lambda + \mu} \{1-\exp [-(\lambda+\mu)t] \} \qquad (17)$$

Si ha conseguentemente:

$$R(t) = 1- \frac{\lambda}{\lambda + \mu} \{1-\exp[-(\lambda+\mu)t] \} \qquad (18)$$

Nel caso di tasso di guasto costante e di componente non ripristinabile ($\mu = 0$) si ritrovano le espressioni:

$$F(t) = 1-\exp(-\lambda t)$$
$$R(t) = \exp(-\lambda t)$$

L'andamento di R(t) nei due casi considerati è mostrato nella Figura 3.4.
Il componente è sottoposto a test periodico.
In questo caso sono comunemente valide le seguenti ipotesi:

- il tasso di guasto del componente è indipendente dal tempo;
- l'intervallo di tempo θ fra un test e il successivo è costante e tale che $\theta << 1/\lambda$;

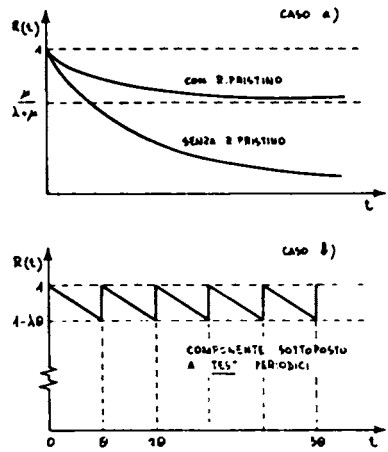


Fig. 3.4 - Affidabilità in funzione dell'età del componente.
a) componente con guasto che si autodenuncia;
b) componente con guasto che non si autodenuncia.

- la durata del test è trascurabile rispetto a θ;
- indipendentemente dallo stato del componente all'inizio di operazioni di test, alla fine di tale operazione il componente è riportato nelle condizioni di funzionamento.

Si ha allora nell'intervallo $0 \longmapsto t = \theta$

$$F(t) = 1-\exp(-\lambda t)$$

e se $\lambda t \ll 1$ si ha $F(t) \cong \lambda t$ (19)

La funzione F(t) varia quasi linearmente fra 0 e $\lambda\theta$ in ogni intervallo di ampiezza θ. L'andamento è a "dente di sega". Nella Figura 3.4 è riportato l'andamento di

$$R(t) = 1-F(t) \cong 1-\lambda t$$

Disponibilità di un componente

Per i due casi già visti nel paragrafo precedente, la disponibilità e l'indisponibilità possono essere agevolmente calcolate. Dalle definizioni già date si ha:

MTBF = MTTR + MTTF. Molto spesso è inoltre MTTF $\gg$ MTTR.

In generale si ha anche $\theta \ll$ MTTF.
Nei due casi l'indisponibilità vale:

a) il guasto si autodenuncia

$$Q = \frac{MTTR}{MTBF} = \frac{\lambda}{\mu} \qquad (21)$$

b) il guasto non si autodenuncia. In questo caso il guasto avverrà, in media, a metà dell'intervallo θ.

$$Q = \frac{\theta/2 + MTTR}{MTBF} \cong \frac{\theta}{2 \cdot MTBF} = \frac{\theta\,\lambda}{2} \qquad (22)$$

Le due formule si ricavano facilmente dalle definizioni già date.

Nelle unità in attesa d'intervento si verificano generalmente due tipi di guasti: il guasto pericoloso (fail danger failure) e quello non pericoloso (fail safe failure).

I primi si presentano quando l'operazione richiesta non viene eseguita: un sistema di allarme domanda il suono della sirena e la sirena non suona.

Se invece la sirena suona, senza essere richiesta dal sistema di allarme, si ha un intervento spurio, non pericoloso di per sé, ma non gradito.

Un altro esempio può essere presentato riferendosi ad un impianto chimico. Un sensore misura la pressione in un reattore: se questa supera un certo livello il sensore comanda, attraverso un opportuno sistema, l'apertura di una valvola normalmente chiusa (e in attesa di chiamata), che permette l'immissione di un inibitore.

Se la valvola si guasta "incollandosi" non è più pronta ad aprirsi, in caso di pericolo; se la valvola si guasta aprendosi, permette l'immissione dell'inibitore e la reazione si spegne: si ha una fermata spuria dell'impianto e danni solo economici.

AFFIDABILITA' DI SISTEMI

I concetti e le definizioni relativi all'affidabilità e alla disponibilità di un componente si possono estendere a un sistema costituito da più componenti collegati in modi diversi.

I sistemi per i quali nella pratica corrente si richiedono valutazioni di affidabilità si possono distinguere in due tipi:

- sistemi operativi, che svolgono in modo continuo una determinata funzione operativa;

- sistemi in attesa d'intervento, come i sistemi di protezione e blocco di un impianto.

Sistemi operativi

Serie e parallelo di componenti

Nel caso di sistemi complessi costituiti da più componenti il calcolo dell'affidabilità è ancora un calcolo di probabilità. La condizione indispensabile per far ciò è che si conoscano le affidabilità dei singoli componenti, l'esattezza del risultato non dipende chiaramente dal calcolo. Ecco le regole da usarsi nei calcoli di probabilità:

a) se un componente ha affidabilità R_1 ed inaffidabilità F_1 ed un altro componente ha rispettivamente R_2 e F_2, la probabilità di sopravvivenza di entrambi i componenti è:

$$R_s = R_1 \cdot R_2 = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} = e^{-\lambda_1+\lambda_2/t} \qquad (23)$$

b) la probabilità di guasto di almeno uno dei due componenti è:

$$F_s = 1-R_s = 1-R_1.R_2 = 1-(1-F_1)(1-F_2) =$$

$$= 1-(1-F_2-F_1-F_1+F_1.F_2) = F_1+F_2- F_1.F_2 \qquad (24)$$

c) la probabilità di guasto di entrambi i componenti è invece:

$$F_p = F_1 \cdot F_2 = (1-R_1)(1-R_2) = 1-R_2-R_1+R_1R_2 =$$

$$= 1-(R_1+R_2-R_1R_2) = 1-R_p \qquad (25)$$

ne consegue quindi; per come è sta ricavata R_p, la seguente definizione:

d) la probabilità di sopravvivenza di almeno uno dei due componenti vale:

$$R_p = R_1 + R_2 - R_1 \cdot R_2 \qquad (26)$$

I casi a) e b) rappresentano eventi complementari: R_s e F_s definiscono l'affidabilità e l'inaffidabilità di una connessione in serie di componenti, dove, quindi, il guasto di un solo componente implica il guasto del sistema.

I diagrammi logici relativi allo stato di funzionamento e allo stato di guasto del sistema costituito da due elementi in serie sono mostrati nella Fig.3.5.

Anche i casi c) e d) rappresentano eventi complementari per cui è $R_p + F_p = 1$. Chiamiamo R_p e F_p affidabilità e inaffidabilità di una connessione in parallelo di componenti, tale che, se un componente si guasta, un altro componente, funzionante in parallelo al primo, è in grado di compiere la missione richiesta al sistema.

In definitiva, il sistema "parallelo di componenti" non va in avaria per il guasto di un solo componente.

In Fig. 3.6 sono rappresentati i diagrammi logici per il caso di due elementi in parallelo.

Se nel sistema serie $(\lambda_1 + \lambda_2)t \ll 1$ le espressioni (23) e (24) si possono così semplificare:

$$R_s \cong 1-(\lambda_1 + \lambda_2)\, t$$

$$F_s \cong (\lambda_1 + \lambda_2)t \qquad (27)$$

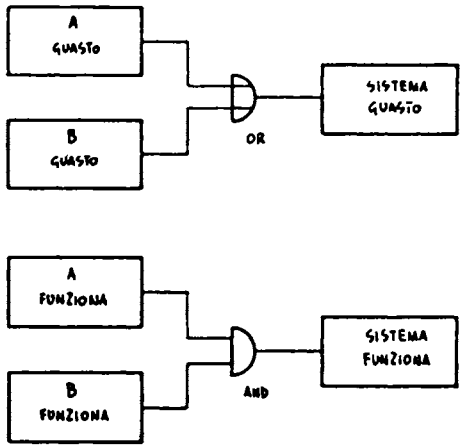


Fig. 3.5 - Diagrammi logici per un sistema tipo serie.

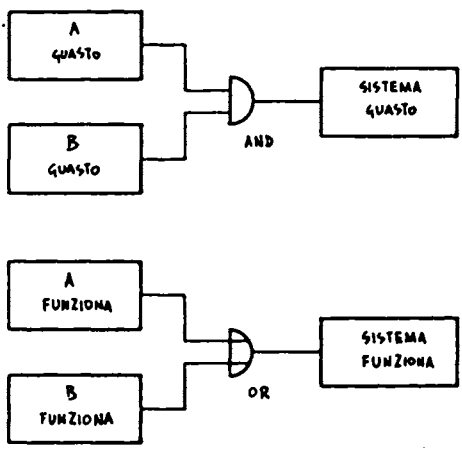


Fig. 3.6 - Diagrammi logici per un sistema tipo parallelo.

Nel caso il sistema consenta la riparazione dei suoi componenti, detti μ_1 e μ_2 i tassi di ripristino (costanti nel tempo), le espressioni dell'indisponibilità Q_s, e della disponibilità A_s del sistema risultano:

$$\begin{aligned} Q_s &= Q_1 + Q_2 - Q_1 Q_2 \cong Q_1 + Q_2 \\ A_s &= 1 - Q_s \end{aligned} \qquad (28)$$

Tenendo conto, secondo la (21), che:

$$Q_1 = \frac{\lambda_1}{\mu_2}$$

$$Q_2 = \frac{\lambda_1}{\mu_2}$$

si ottiene:

$$\begin{aligned} Q_s &= \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2} \\ A_s &= 1 - \left(\frac{\lambda_1}{\mu_2} + \frac{\lambda_2}{\mu_2}\right) \end{aligned} \qquad (29)$$

Nel caso invece di un sistema tipo parallelo, se $\lambda_1 t$ e $\lambda_2 t$ sono molto minori dell'unità, si ha:

$$\begin{aligned} F_p &\cong \lambda_1 \lambda_2 t^2 \\ R_p &\cong 1 - \lambda_1 \lambda_2 t^2 \end{aligned} \qquad (30)$$

Nel caso il sistema consenta la riparazione dei suoi componenti si ottiene:

$$\begin{aligned} Q_p &= Q_1 \cdot Q_2 \\ A_p &= 1 - Q_p \end{aligned} \qquad (31)$$

$$\begin{aligned} Q_p &= \frac{\lambda_1}{\mu_1} \cdot \frac{\lambda_2}{\mu_2} \\ A_p &= 1 - \frac{\lambda_1}{\mu_1} \cdot \frac{\lambda_2}{\mu_2} \end{aligned} \qquad (32)$$

Generalmente un sistema completo consiste di un gran numero di componenti montati in serie. Talvolta però alcuni di questi, meno affidabili, vengono affiancati da componenti identici montati in parallelo, così da aumentare l'affidabilità mediante una ridondanza dei componenti deboli. Tuttavia queste connessioni in parallelo possono essere considerate come una singola unità in serie con gli altri componenti, cosicchè se si guasta questa unità il sistema complessivo subisce un guasto.

Naturalmente per n componenti o unità in serie l'affidabilità del sistema è:

$$R_s = R_1 \cdot R_2 \cdot R_3 \ldots R_n = \prod_{i=1}^{n} R_i \qquad (33)$$

Questa relazione è detta "legge del prodotto della affidabilità". Se tutte le affidabilità hanno andamento esponenziale, il calcolo di R_s si semplifica notevolmente :

$$R_s = \exp\left[-(\lambda_1+\lambda_2 + \ldots \lambda_n)t\right] = \exp\left[-\sum_{i=1}^{n} \lambda_i t\right] \qquad (34)$$

Va tenuto presente che il tasso di guasto dei componenti in tali calcoli è riferito ad un certo insieme di condizioni di funzionamento ben determinate.

In generale, i tassi di guasto subiscono forti variazioni al variare delle condizioni operative, questo vuol dire che in fase di progetto si può migliorare notevolmente l'affidabilità abbassando il livello di sfruttamento dei componenti, così, come nei limiti del possibile, si può ridurre il numero dei componenti. Per questa via però non sempre si ottengono le affidabilità richieste.

Ad esempio, se l'affidabilità richiesta per il sistema è molto elevata, il progettista è costretto a duplicare o triplicare alcuni componenti.

Nel caso di n componenti in parallelo si ha che l'inaffidabilità è espressa dalla relazione:

$$F_p = F_1 \cdot F_2 \cdot F_3 \ldots F_n = \prod_{i=1}^{n} F_i \qquad (35)$$

relazione che prende il nome di "legge del prodotto della inaffidabilità in parallelo".

L'affidabilità di n componenti in parallelo sarà:

$$R_p = 1 - F_p(t) = 1 - \prod_{i=1}^{n} F_i \qquad (36)$$

Poichè molto spesso i montaggi in parallelo sono realizzati con componenti identici, allora le equazioni precedenti si semplificano nel modo seguente:

$$F_p = F^n \quad ; \quad R_p = 1 - F^n \qquad (37)$$

Si è detto che per un sistema in serie, costituito da componenti ed affidabilità esponenziale, il tasso di guasto λ è costante ed uguale alla somma dei tassi di guasto di tutti i componenti; quindi un tal sistema è anch'esso ad affidabilità esponenziale ed il suo tempo medio tra i guasti è:

$$m_s = 1 \Big/ \sum_{i}^{n} \lambda_i \qquad (38)$$

Tutto ciò non vale per i sistemi in parallelo;in questo caso il tasso di guasto è una funzione variabile del tempo di impiego, benchè il tempo medio tra i guasti m_p sia ancora costante. Si può dimostrare che per n componenti uguali in parallelo è:

$$m_p = \frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{3\lambda} + \ldots \frac{1}{n\lambda} \qquad (39)$$

nel caso invece di 2 componenti in parallelo non uguali si ha:

$$m_p = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1+\lambda_2} \qquad (40)$$

Sistemi a logica maggioritaria

Si consideri un sistema composto da 3 componenti uguali in parallelo. Siano sempre R e F l'affidabilità e l'inaffidabilità di ogni componente. Si sviluppi ora il binomio

$$(R + F)^3 \quad \text{si otterrà}$$

$$(R + F)^3 = R^3 + 3R^2F + 3RF^2 + F^3 = 1 \qquad (41)$$

Il primo termine rappresenta la probabilità che tutti e tre i componenti sopravvivano:
Il secondo esprime la probabilità di due sopravvivenze e di un guasto.
Il terzo la probabilità di una sopravvivenza e di due guasti.
Il quarto la probabilità di tre guasti. Questo ultimo termine quindi definisce l'inaffidabilità del sistema-parallelo:

$$F_p = F^3 \qquad (42)$$

L'affidabilità del sistema è perciò:

$$R_p = 1 - F^3 = R^3 + 3R^2F + 3RF^2 \qquad (43)$$

Se si richiedesse la sopravvivenza di almeno 2 componenti su 3 per il buon funzionamento del sistema , il termine $3RF^2$ non contribuirebbe più alla affidabilità del sistema.L'affidabilità R_1 diverrebbe quindi:

$$R_1 = R^3 + 3\,R^2F = 3R^2 - 2R^3 \qquad (44)$$

e l'inaffidabilità:

$$F_1 = 3RF^2 + F^3 = 3F^2 - 2F^3 \qquad (45)$$

Un sistema di questo tipo ha il nome di sistema a logica maggioritaria; nell'esempio si ha quindi un sistema a logica 2 su tre.

Si può facilmente verificare che, se è $R > 1/2$, si ha $R_1 > R$; ma la situazione si inverte per $R < 1/2$.

Se l'affidabilità R ha andamento esponenziale si ottiene

$$R_1 = 3 \exp (- 2\lambda t) - 2 \exp (- 3\lambda t) \quad (46)$$

e nel caso $\lambda t << 1$:

$$R_1 = 1 - 3 \lambda^2 t^2 \quad (47)$$

Più in generale un sistema m su n, anche indicato m/n, è costituito da n elementi di cui almeno m devono essere funzionanti per garantire il funzionamento del sistema. In questi casi l'affidabilità risulta:

$$R_1 = \sum_{m}^{n} {}_k \binom{n}{k} R^k (1 - R)^{n-k} \quad (48)$$

Analoga è l'espressione della disponibilità del sistema.

Si consideri ancora un sistema a logica 2 su 3 in cui l'affidabilità dei singoli elementi siano differenti. Dette queste R_A, R_B. R_C, l'affidabilità del sistema risulta, evidentemente:

$$R_1 = R_A R_B R_C + (1 - R_A) R_B R_C +$$

$$+ (1 - R_B) R_A R_C + (1 - R_C) R_A R_B$$

Sistemi in attesa di intervento

Frequentemente non è possibile o pratico impiegare componenti od unità montati in parallelo, si adottano in tali casi i cosiddetti montaggi "in riserva", in cui un elemento principale è funzionante mentre uno o più elementi aspettano di sostituirlo appena si guasta.

Tale montaggio richiede,ovviamente, dispositivi che rilevino il guasto e che innestino nel circuito l'elemento di riserva appena è necessario. Questi dispositivi, naturalmente, non sono affidabili al 100%, ma, in prima approssimazione,si possono ritenere tali.

L'affidabilità del sistema dotato di riserva R_r si ottiene integrando la funzione densità di guasto f(t) del sistema stesso:

$$R_r = \int_t^{\infty} f(t)\, dt \qquad \text{affidabilità cumulativa}$$

Tale procedimento è valido anche se gli elementi in riserva sono diversi tra di loro.

Consideriamo due componenti di cui uno funzionante (1) ed uno in riserva (2); essi avranno tassi di guasto λ_1 e λ_2. Supponendo che il componente in riserva entri in funzione al tempo t_1 (guasto del primo), esso funzionerà quindi per un tempo $t_2 = t - t_1$ (essendo t_2 il tempo di funzionamento del componente in riserva).

Ricordando che la funzione densità di guasto è:

$f(t) = \lambda\, e^{-\lambda t}$ si avranno:

per il primo componente $\quad f_1(t_1) = \lambda_1\, e^{-\lambda_1 t_1}$

e per il secondo $\quad f_2(t_2) = \lambda_2\, e^{-\lambda_2 (t-t_1)}$

In un intervallo di tempo dt, affinchè si abbia il guasto nel sistema è necessario il guasto di entrambi i componenti,per cui la probabilità di guasto del sistema è data dal prodotto:

$$f_1(t_1)\cdot f_2(t_2) = \lambda_1\cdot\lambda_2 \quad e^{-\lambda_1 t_1} \cdot e^{-\lambda_2 (t-t_1)}$$

In questo prodotto le variabili sono t e t_1, integrando rispetto a t_1 si ottiene la funzione densità di guasto dell'intero sistema dotato di riserva, espressa in funzione di t:

$$f_r(t) = \int_{t_1=0}^{t} f_1(t_1).f_2(t_2)dt_1 = \lambda_1\lambda_2\left[\frac{\exp(-\lambda_1 t)}{\lambda_2-\lambda_1} + \frac{\exp(-\lambda_2 t)}{\lambda_1-\lambda_2}\right]$$

Poichè $R_r = \int_t^{\infty} f_r(t)dt$, si ottiene l'affidabilità per un tempo di missione t:

$$R_r(t) = \int_t^{\infty} f_r(t)dt = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_2-\lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right) \quad (49)$$

Il tempo medio fra i guasti è:

$$m_r = m_1 + m_2 = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} \quad (50)$$

Considerando che i dispositivi di commutazione non hanno un'affidabilità del 100%, ma, ad esempio, abbiano un valore $R_c(t)$, allora la relazione (49) si modifica nel seguente modo:

$$R_r(t) = e^{-\lambda_1 t} + R_c\,\frac{\lambda_1}{\lambda_2-\lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right) \quad (51)$$

Nei sistemi con riserva esaminati non si è tenuto conto del fatto che anche i componenti "in ozio" han

no un tasso di guasto. Sia questo, per l'esempio precedente, λ_3 . In questo caso allora, tenendo conto che il tempo di integrazione delle funzioni di densità di guasto si estende ai periodi di attesa del componente di riserva, si ottiene:

$$R_r(t) = e^{-\lambda_1 t} + R_c \cdot \frac{\lambda_1}{\lambda_2 + (\lambda_1 + \lambda_3)} \left(e^{-(\lambda_1+\lambda_3)t} - e^{-\lambda_2 t}\right) \quad (52)$$

BIBLIOGRAFIA

1. L.S.Fryer e R.F. Griffiths, Report SRD-R, UKAEA, London, 1979.

2. V.C.Marshall, "How lethal are explosions and toxic escape?" n. 373, 573, The chemical Engineer (1977).

3. A.Lovati, "linee orientative alla valutazione probabilistica del rischio di incidente rilevante", CLUP, Milano, 1983.

4. A.Lovati, "L'affidabilità per la sicurezza - Introduzione al tema", Chim. Ind. (Milan), 60, 843 (1978).

5. W.Wohlleben and F.Vahrenholt, "Precautions Against Accidents in Chemical Facilities", J. Haz. mat., 5, 41 (1981).

6. T.Van de Putte, "the Safety Report Legislation and its Application in the Netherlands", J. Haz. Mat., 7, 131 (1983).

7. First (1976) and Second (1979) Report of the Advisory Committee on Major Hazards, HMSO, London.

8. France, Public Law No. 76/663 of the 19 July 1976 and No. No. 77/1134 of the 21 September 1977.

9. Council of European Communities, Directive No. 82/501 of the 5 August 1982.

10. G.C.Bello, "La valutazione quantitativa del rischio", ENI-Sicurezza nell'ambiente di lavoro - Documenti n.1-2 (1978).

11. A.Lovati, Chim. Ind. (Milano), "Il rischio tecnologico", 60, 938 (1978).

12. A.Lovati, "La riduzione dei rischi nelle industrie di processo", Le Scienze, 151, (3), 88 (1981).

13. A.Lovati e A.Lovati, "L'analisi del rischio", EPC, Roma, 1984.

14. A.E.Green, A.J.Bourne, "Reliability technology", Wiley J. and Sons, London, 1972.

15. U.S.Nuclear Regulatory Commission, "Reactor safety study", Wash-1400, 1975.

16. E.R.Snaith, "Can reliability predictions be validated?", Proceedings Second National Reliability Conference, Birmingham, march 1979.

17. E.P.Lees, "loss Prevention in the process Industries", 2 voll., Butterworths, London, (1981).

18. American Institute of Chemical Engineers, "loss Prevention", A.C.E.P. Technical Manual, New York, 1979.

19. R.L.Browing, "The loss Rate Concept in Safety Engineering", M. Dekker, Inc. New York, 1980.

20. G.L.Wells, "Safety in process Plant Design", G. Godwin Ltd., London, 1980.

21. E.J.Henley and H.Kumamoto, "Reliability Engineering and Risk Assessment", Prenitice-Hall Inc., Englewood Cliffs, 1981.

22. N.Piccinini, Hazard Prevention, "Design of Highly dangerous plant", 20, (1), 11 (1984).

23. C.Iannuzzi, "L'affidabilità per la sicurezza - La fase iniziale di indagine", Chim. Ind. (Milan), 60, 1021 (1978).

24. R.Piattoli, "Analisi di affidabilità e sicurezza nella progettazione di impianti chimici", in "Sicurezza e prevenzione degli infortuni nell'industria chimica", N.Piccinini, Ed. levrotto & Bella, Torino, 1979.

25. N.Piccinini e G.Levy, "Process Safety analysis for better reactor cooling system design in the Ethylene oxide reactor", Can. J. Chem. Eng., 62, 541 (1984).

26. H.G.Lawley, "operability studies and hazards analysis", Chem. Eng. Progr., 70 (4), 45 (1974).

27. Chem. Ind. Safety and Health Council of the Chem. Ind. Ass., " A guide to Hazard and Operability Studies", Alembic House, London, 1977.

28. R.E.Knowlton, "Hazard and Operability Studies", Chemetics International Ltd., Vancouver B.C., 1981.

29. R.Labozzetta, "Identificazione delle anomalie di un impianto", Chim. Ind. (Roma), 61, 46 (1979).

30) G.C. Bello, "L'affidabilità per la sicurezza - I dati numerici per l'analisi quantitativa del rischio", Chim. Ind. (Milan), 62, I48 (I980).

3I) 4th Euredata Conf., Venice 23-25 March, I983.

32) A. Lovati, "L'affidabilità per la sicurezza - Stima della frequenza verificarsi di un evento", Chim. Ind. (Milan), 62, 247 (I980).

33) J.S. Arendt and J.B. Fussel, "System Reliability Engineering Methodology for Industrial Application", Loss Prev., I4, I8 (I98I).

34) P.A. Carson, C.J. Mumford,"Journal of Occupational Accidents", 2, I (I978); 2, 85 (I979).

35) G. Ooms, A.P. Mahieu, F. Zelis, "Loss Prevention and safety promotion in the process industries", Elsevier, Amsterdam I974.

36) C. Grelecki, "Fundamentals of fire and explosion - Hazard evaluation", Am. Inst. Chem. Eng.s, Today Series, I976.

37) N.Piccinini, U.Anatra, G.Malandrino and D.Barone, "Safety Analysis for an Allyl Chloride Plant", Plant/Operations Progress, I, 69 (I982).

38) I. Ciarambino, S. Messina: "Il diagramma causa/conseguence". Chim. Ind. (Roma), 61, p. 123 (1979).

39) L. Farris, A. Mazzocchi: "Il diagramma conseguenza/cause". Chim. Ind. (Roma), 61, p. 216 (1979).

40) A. Lovati: "Metodi matematici di analisi". Chim. Ind. (Roma), 61, p. 584 (1979).

41) D. Barone: "Le formule fondamentali per componenti e sistemi". Chim. Ind. (Roma), 61, p. 753 (1979).

42) W. Dosi, E. Gramellini: "La magnitudo delle conseguenze di un incidente". Chim. Ind. (Roma), 62, p. 335 (1980).

L'autore desidera ringraciare vivamente il Dr. A. Lovati, curatore della serie di articoli "L'affidabilità per la sicurezza", apparsi su "La Chimica e l'Industria" tra il 1978 e il 1980, nonchè l'editore per avergli concesso l'utilizzo di parte dei detti articoli.

I N D I C E

Sezione III

PRINCIPI E METODI DELL'AFFIDABILITA'

ACABAT D'IMPRIMIR
A ROMARGRAF, S.A.,
DE L'HOSPITALET DE LLOBREGAT
EL DIA 5 DE MARÇ DE 1985


SOCIETAT CATALANA CIÈNCIES
INSTITVT D'ESTVDIS CATALANS


SOCIETAT CATALANA CIÈNCIES
INSTITVT D'ESTVDIS CATALANS